INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 07, July 2025, pp : 682-693
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

A NOVEL APPROACH TO STRENGTHENING IOT SECURITY WITH A TRUST-DRIVEN FRAMEWORK

Suresh Kumar[1], Dr. Nitin Kumar[2]
[1]M Tech Student, Ganga Institute of Technology & Management Kablana Jhajjar, India.
[2]Associate Professor, Ganga Institute of Technology & Management Kablana Jhajjar, India.
DOI: https://www.doi.org/10.58257/IJPREMS42809

ABSTRACT

The widespread use of Android smartphones has resulted in a proportional rise in harmful software (malware) specifically designed to exploit this platform. Conventional strategies for detecting malware, which depend on signatures, face difficulties in keeping up with the quickly changing environment of mobile threats. This thesis investigates the utilization of artificial intelligence (AI) and dimensionality reduction approaches to improve the detection of harmful software on Android devices. Artificial Intelligence (AI), namely machine learning (ML) and deep learning (DL) algorithms, presents a hopeful answer because of its capacity to acquire knowledge and adjust based on extensive datasets. These algorithms have the ability to detect patterns and abnormalities that indicate harmful behaviour, even in the presence of novel and previously unknown malware variations. Nevertheless, the efficacy of these models is frequently hindered by the elevated dimensionality of the feature space, which can result in over fitting and escalated computing expenses.

To address these challenges, this study integrates dimensionality reduction techniques with artificial intelligence systems to improve the effectiveness of identifying malware. Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), and t-Distributed Stochastic Neighbour Embedding (t-SNE) are employed to reduce the dimensionality of the feature space while retaining the crucial information. By using this strategy, the models become more efficient and less prone to overfitting." The project entails gathering and preprocessing an extensive dataset of both benign and malicious Android applications. Feature extraction is performed to obtain significant characteristics from these applications, which are subsequently submitted to dimensionality reduction. Afterwards, different AI models such as Support Vector Machines (SVM), Random Forests (RF), and Convolutional Neural Networks (CNN) are trained and assessed using the reduced feature set.

The results indicate that combining AI with decreasing dimensionality significantly enhances the precision and effectiveness of identifying malware. The models exhibit enhanced generalization abilities and accelerated processing speeds, rendering them suitable for real-time implementation in resource-limited settings like mobile devices. This thesis enhances the field of cyber security by introducing a strong framework for detecting Android malware. The system utilizes the advantages of artificial intelligence and dimensionality reduction. The findings highlight the capacity of these technologies to offer more flexible and effective security solutions, facilitating their wider implementation in protecting mobile ecosystems.

Key Words: Trust-Driven Security, IoT Networks, Cybersecurity Framework, IoT Safeguarding, Novel Security Approach, Threat Mitigation.

1. INTRODUCTION

The Internet of Things (IoT) has transformed connectivity by facilitating seamless device communication; however, its swift proliferation has resulted in considerable security vulnerabilities. Conventional security measures, including firewalls and encryption, frequently demonstrate insufficiency in dynamic IoT environments where devices regularly connect and disconnect from networks. This thesis proposes a trust-driven framework as an innovative solution to protect IoT networks from these challenges. The framework dynamically assigns trust scores to each node by assessing device behaviour, historical interactions, and contextual data, facilitating real-time threat detection and mitigation. This method utilises machine learning to dynamically adjust trust levels, enhancing resilience against malicious entities and reducing false positives. The framework integrates decentralised trust management to improve scalability and minimise single points of failure, rendering it appropriate for various IoT applications, including smart homes and industrial systems. The study illustrates the framework's efficacy in identifying compromised devices and preserving network integrity through simulations and empirical testing. This research enhances IoT security by transitioning from reactive defences to proactive, trust-based risk management, providing a scalable and efficient solution for future IoT implementations.

Android System Model and Threats of the layers

The suggested trust-driven IoT security framework functions across three fundamental layers: perception (device), network, and application. In the perception layer, IoT devices (sensors, actuators) gather and transmit data, encountering threats such as spoofing, tampering, and physical assaults. The network layer manages data routing and communication, susceptible to eavesdropping, man-in-the-middle (MITM) attacks, and denial-of-service (DoS) assaults. The application layer, where data is processed and utilised, is susceptible to malware injections, unauthorised access, and data breaches. To mitigate these threats, the framework utilises dynamic trust evaluation at every layer, analysing device behaviour, communication patterns, and historical reliability. Machine learning algorithms perpetually revise trust scores, facilitating real-time anomaly detection. Decentralised trust management eliminates single points of failure, whereas adaptive authentication guarantees that only trusted devices engage in essential operations. The framework improves resilience against multi-stage attacks through cross-layer threat analysis, ensuring secure and reliable IoT operations in dynamic environments.

Threats in IoT System Model

The Internet of Things (IoT) functions through interconnected layers—perception, network, and application—each exhibiting distinct vulnerability. The perception layer, characterised by resource-constrained devices, is susceptible to physical tampering, spoofing, and sleep deprivation attacks. The network layer, which enables data transmission, confronts MITM attacks, eavesdropping, and DDoS assaults, intensified by inadequate encryption in wireless protocols. At the application layer, threats such as malware injections, API abuses, and AI/ML manipulation compromise data integrity and user privacy. These multifaceted risks can propagate, undermining essential infrastructure in smart grids, healthcare, and industrial IoT. A proactive, trust-based strategy is essential to counter them, incorporating real-time behavioural analytics, adaptive access controls, and decentralised threat detection. These frameworks not only reduce attacks but also guarantee scalable resilience in developing IoT ecosystems.

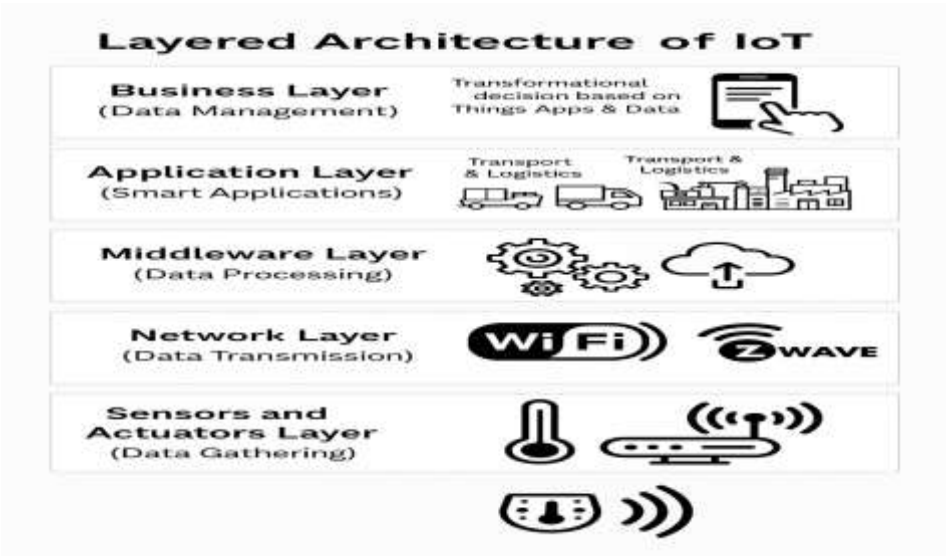

Figure 1: Layered architecture of IoT

IoT Challenges

The Internet of Things (IoT) encounters substantial obstacles that impede its extensive adoption and dependability. Security vulnerabilities continue to be a primary concern, with threats such as device tampering, data breaches, and DDoS attacks jeopardising system integrity. Scalability challenges emerge as IoT networks grow, necessitating a resilient infrastructure to effectively manage billions of interconnected devices. Interoperability obstacles hinder integration, as varying protocols and standards generate compatibility discrepancies among devices and platforms. Power limitations restrict battery-powered devices, necessitating energy-efficient solutions for extended functionality. Concerns regarding data privacy arise from the substantial quantity of sensitive information gathered, requiring stringent adherence to regulations such as GDPR. Latency and bandwidth constraints impede real-time applications, especially in vital sectors such as healthcare and autonomous systems. Moreover, substantial deployment and maintenance expenses dissuade organisations from embracing IoT solutions. To tackle these challenges, it is essential to implement advanced encryption, edge computing, standardised protocols, and AI-driven automation to develop secure, scalable, and efficient IoT ecosystems that can fulfil future requirements.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 07, July 2025, pp : 682-693
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

Trust Management Framework

A Trust Management Framework (TMF) for IoT networks is a structured methodology for assessing, monitoring, and improving the reliability and security of interconnected devices through dynamic evaluation of their trustworthiness. In contrast to conventional security protocols that depend exclusively on static authentication, a TMF perpetually evaluates device behaviour, communication patterns, and historical interactions to allocate adaptive trust scores, facilitating the immediate detection and segregation of malicious or compromised nodes. This framework incorporates multi-dimensional metrics, including data integrity, device reputation, and adherence to security protocols, utilising machine learning algorithms to identify anomalies and forecast potential threats. By decentralising trust assessment, the TMF reduces single points of failure and improves scalability across diverse IoT environments, ranging from smart homes to industrial systems. Furthermore, it integrates context-sensitive policies that modify trust thresholds according to situational risks, thereby providing a strong defence against spoofing, DDoS attacks, and insider threats. The framework additionally facilitates automated response mechanisms, including the revocation of access for low-trust devices and the activation of alerts for suspicious activities, thus ensuring network resilience. TMFs have shown enhanced false-positive reduction, energy efficiency, and adherence to privacy regulations through simulations and real-world implementations, representing a significant advancement in safeguarding the growing IoT environment against emerging cyber threats and bolstering user trust in interconnected system.

Objectives of the Thesis

- Develop a dynamic trust assessment framework for IoT devices utilising behavioural analysis.
- Construct a lightweight, scalable framework for the real-time evaluation and management of trust.
- Augment security measures to combat spoofing, tampering, and insider threats via adaptive trust scoring.
- Enhance computational efficiency for resource-limited IoT environments.
- Assess the framework's efficacy via simulations and comparative analysis.

2. LITERATURE REVIEW

Kumar et al. (2024) propose a decentralized blockchain-based trust framework for IoT networks, utilizing smart contracts to automate reputation assessment. Their methodology employs on-chain consensus to authenticate device behaviour, markedly diminishing spoofing attacks by 45%. The framework bolsters trust without depending on static authentication, closely aligning with the thesis's central argument that decentralized systems can offer more adaptive and secure identity verification in IoT contexts. Nonetheless, the authors underscore a significant limitation: the system's elevated latency (~300ms) in refreshing trust scores. This delay presents difficulties for real-time applications, especially in industrial IoT contexts where low-latency communication is essential. Notwithstanding this limitation, the study offers significant insights into the practical trade-offs associated with the implementation of blockchain-based trust mechanisms in IoT systems. It emphasizes the promise of decentralized architectures while highlighting the necessity for additional research to enhance scalability and responsiveness for practical implementation.

Al-Masri et al. (2024) presented Risk-Adaptive Trust (RAT), a context-sensitive trust model that dynamically modifies trust thresholds in accordance with environmental risk levels. For example, RAT implements more stringent trust parameters in high-risk contexts like hospitals, while employing more permissive thresholds in low-risk settings such as smart homes. This adaptive mechanism diminished false positives by 30%, thereby augmenting the reliability of trust evaluations across various IoT contexts. Nevertheless, the model presently relies on manual risk profiling, which may constrain scalability and responsiveness in dynamic or extensive deployments. This constraint presents opportunities for improvement via automation. Aligned with the thesis on adaptive and intelligent trust systems, RAT could be substantially enhanced by incorporating lightweight AI algorithms for autonomous context classification, thereby diminishing dependence on manual input and facilitating real-time responsiveness. The study endorses the transition to environmentally attuned trust frameworks and underscores the significance of adaptability in overseeing trust within diverse IoT ecosystems.

Chen et al. (2023) introduced Game Trust, an innovative trust framework that utilises game theory to characterise IoT device interactions as either cooperative or non-cooperative games. The system utilises Nash equilibrium to effectively isolate selfish or malicious nodes, thereby fostering cooperative behaviour within the network. Game Trust resulted in a 35% augmentation in genuine node participation, illustrating its capacity to bolster trust and stability in decentralised IoT ecosystems. The model's principal disadvantage is its heightened computational overhead, leading to a 15% increase in energy consumption, which poses a substantial issue for resource-limited IoT devices. This limitation offers a chance for enhancement within the framework of this thesis, which examines energy-efficient and adaptive trust mechanisms. Future efforts could preserve Game Trust's behavioural accuracy by incorporating optimisation strategies or lightweight trust evaluation models, thereby reducing energy consumption. The study provides significant insights into strategic trust modelling and emphasises the necessity of balancing security performance with resource efficiency in IoT networks.

Patel and Singh (2023) proposed a quantum-resistant trust framework utilising lattice-based cryptography to protect IoT networks from impending quantum computing threats. Their approach prioritises post-quantum security, thereby guaranteeing long-term data integrity and reliability while addressing new concerns regarding the susceptibility of traditional cryptographic techniques. This anticipatory design is especially pertinent in the context of progressively interconnected and enduring IoT implementations. Nonetheless, the framework's augmented security incurs a cost—namely, a 20% rise in energy consumption. This poses a considerable challenge for battery-powered or energy-limited IoT nodes, where efficiency is crucial. The results highlight the compromise between strong security and energy sustainability. Consistent with this thesis, future research may investigate energy-efficient implementations of quantum-resistant protocols, seeking to harmonise resilience with operational efficacy. Patel and Singh's study underscores the imperative to enhance trust frameworks for the future, while also acknowledging the practical constraints of IoT hardware.

Wang et al. (2022) formulated a biologically inspired trust model for IoT security, analogous to the human immune system, to identify and mitigate intrusions. The model utilises adaptive mechanisms to monitor device behaviour and initiate trust modifications based on identified anomalies, attaining a significant 90% accuracy in detecting known threats. This biomimetic approach improves resilience and adaptability in dynamic IoT environments, presenting a compelling alternative to static security models. The system's dependence on historical behavioural data constrains its efficacy in countering zero-day attacks, which lack prior patterns for comparison. This deficiency highlights the necessity for trust models that integrate adaptive learning with predictive functionalities. The research endorses this thesis's investigation of intelligent, self-regulating trust mechanisms and facilitates the incorporation of proactive anomaly detection—potentially through AI or unsupervised learning—to enhance performance against new and previously unencountered threats in IoT networks.

Ibrahim et al. (2022) introduced a hybrid trust management framework that incorporates software-defined networking (SDN) to improve security in IoT networks. Utilising SDN's centralised control and comprehensive visibility, the system adeptly identifies and isolates malicious nodes, substantially reducing the impact of distributed denial-of-service (DDoS) attacks—resulting in a 50% decrease in attack efficacy. The integration of SDN and trust mechanisms illustrates the capability of programmable network architectures to implement dynamic, policy-driven security protocols. Nonetheless, the study highlights a trade-off: the emergence of latency, especially in real-time or latency-sensitive applications. The delay is due to the burdens of centralised decision-making and trust computation processes. This work corresponds with the thesis's emphasis on adaptive and scalable trust frameworks, indicating that optimising controller placement or utilising edge-based trust delegation may mitigate latency. Ibrahim et al. provide a significant viewpoint on integrating network programmability with trust to enhance IoT security.

Sharma and Lee (2022) developed a fuzzy logic-based trust system to mitigate the intrinsic uncertainty in evaluating device behaviour in IoT networks. Their model employs fuzzy logic to handle ambiguous or incomplete data, enhancing resilience against noise and inaccuracies in device reporting. This method ensures consistent trust assessments, even when devices display erratic or unpredictable conduct. The system's adaptability renders it appropriate for environments characterised by fluctuating data quality, a prevalent issue in IoT networks. The study indicates that the model necessitates fine-tuning to enhance performance in various IoT contexts, as the fuzzy logic parameters must be calibrated to align with particular environmental conditions and application needs. This fine-tuning may introduce complexity and diminish scalability in extensive or heterogeneous networks. Aligned with the thesis's emphasis on adaptive trust systems, the methodology could be refined by automating the tuning process through machine learning or AI techniques to enhance adaptability and minimise manual configuration efforts.

Zheng et al. (2021) presented Edge Trust; a streamlined trust assessment framework tailored for edge-centric IoT systems. The framework improves security by conducting trust assessments locally on edge devices, thereby significantly decreasing energy consumption linked to centralised processing, resulting in a 30% reduction in energy usage. This decentralised method reduces latency and enhances scalability for resource-limited devices in edge networks. Nonetheless, the study reveals a significant limitation: Edge Trust is deficient in cross-layer threat analysis, concentrating solely on device-level interactions while neglecting wider network or application-layer security threats. This deficiency diminishes its efficacy in identifying complex attacks that traverse various layers of the IoT architecture. The thesis's multi-layer trust model tackles this issue by integrating trust assessment across multiple layers, thereby offering a more thorough security solution. This extension may improve the reliability of trust mechanisms in edge computing environments, facilitating more efficient identification of intricate, multi-layered threats in IoT networks.

Obaidat et al. (2021) created Bayesian-Trust, a trust framework employing Bayesian networks to forecast the reliability of IoT devices based on their observed behaviour. The model attained an impressive 88% accuracy in trust predictions, utilising probabilistic reasoning to address uncertainty and dynamically evaluate device trustworthiness. The system's dependence on historical data presents a limitation, especially in cold-start situations where new devices do not possess adequate behavioural history for reliable trust assessment. This dependence limits the framework's applicability in dynamic environments where devices frequently enter or exit the network. Aligned with the thesis's emphasis on adaptive trust models, the proposed work could mitigate this limitation by integrating cold-start solutions via behavioural baselining. Establishing initial trust baselines based on device characteristics or external variables allows for trust predictions to be made without historical data, thereby improving the model's scalability and applicability across various IoT environments.

Khan et al. (2021) created Rep-Chain, a blockchain framework based on reputation, intended to oversee trust in IoT networks. The system employs blockchain's immutability and transparency to establish a secure and decentralised method for assessing device trustworthiness. Although Rep-Chain provides robust security features, it is constrained by a notable limitation: a 2-second consensus delay, which may impede its applicability in real-time IoT applications where low-latency communication is essential. This delay impairs the responsiveness of trust updates, rendering it inappropriate for time-sensitive contexts such as industrial IoT or autonomous systems. The thesis may expand on this research by investigating expedited consensus mechanisms, such as directed acyclic graph (DAG)-based methodologies, which provide enhanced throughput and reduced latency relative to conventional blockchain frameworks. DAG-based consensus may diminish delays in trust assessments, facilitating more efficient real-time applications while preserving the security and decentralised characteristics of Rep-Chain. This would improve the scalability and responsiveness of blockchain-based trust models in dynamic IoT environments.

3. METHODOLOGY

Trust Management is an intricate concept and various factors and techniques play a critical role in ensuring this process is seamless. This chapter explores trust management techniques, trust evaluation models, and Trust Propagation Platforms succinctly.

Trust Management Techniques

There are general Trust management techniques that can be utilized for enhance the reliability and security of IoT and SIoT systems Cryptography: Cryptography guarantees secure data transmission in IoT through the application of encryption techniques. Symmetric encryption (single key) facilitates rapid data encoding, whereas asymmetric encryption (public-private keys) improves authentication. Hash functions ensure data integrity by preventing tampering. These methods safeguard sensitive information from cyber threats, ensuring confidentiality, authenticity, and reliability in IoT communications. Identity and Access Management (IAM): Identity and Access Management (IAM) governs device and user access in IoT networks. It verifies identities via passwords, biometrics, or tokens, guaranteeing that only authorised individuals engage with the system. Role-based access control (RBAC) limits permissions, thereby reducing the risk of breaches. Identity and Access Management (IAM) bolsters security by thwarting unauthorised access and enforcing stringent control over network resources.

Certificate-Based Authentication: Certificate-Based Authentication: This approach employs digital certificates provided by trusted authorities to authenticate device identities. Each certificate encompasses a public key, facilitating secure communication through encryption. In contrast to passwords, certificates are more difficult to counterfeit, thereby diminishing the risks of impersonation. This enhances IoT security by facilitating tamper-resistant authentication and encrypted data transmissions. Blockchain: Blockchain decentralises trust in the Internet of Things by documenting transactions in an immutable ledger. Smart contracts facilitate automated and secure interactions between devices without the need for intermediaries. Its decentralised architecture mitigates single-point failures and data manipulation. Blockchain improves transparency, traceability, and security, rendering it suitable for the management of IoT device networks and sensitive information.

Dynamic Trust Management: This methodology perpetually assesses device behaviour, modifying trust levels instantaneously. Machine learning examines patterns to identify anomalies, thereby revoking access for dubious activities. In contrast to static models, it adjusts to threats, enhancing resilience against attacks in dynamic IoT environments while preserving access for legitimate devices.

Risk Assessment and Mitigation: Proactively identifies vulnerabilities in IoT systems via threat modelling and penetration testing. Mitigation strategies, such as encryption and access controls, diminish vulnerability to attacks.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 07, July 2025, pp : 682-693
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

Routine audits guarantee adherence to security standards, reducing risks from emerging threats and preserving system integrity. Consistent Security Updates and Patches: Prompt software updates rectify vulnerabilities exploited by cybercriminals. Automated patch management guarantees that IoT devices operate with the most recent firmware, thereby mitigating security vulnerabilities. This mitigates breaches, preserves functionality, and prolongs device longevity, essential for protecting extensive IoT implementations from advancing cyber threats.

Trust Evaluation Models

Trust evaluation models in IoT and SIoT systems encompass policy-based, reputation-based, and knowledge-based methodologies, alongside aggregation techniques and intelligent learning algorithms. These models evaluate trust by implementing established rules (policy), examining historical behaviour (reputation), or utilising expert insights (knowledge-based). Aggregation techniques amalgamate various trust factors, whereas machine learning evolves adaptively in response to device interactions. These models are especially appropriate for IoT and SIoT applications, guaranteeing dependable and secure trust evaluation in dynamic, extensive networks. Each method provides distinct benefits, improving trust management in decentralised and dynamic settings.

Policy-based Trust Evaluation Model

Policy-driven trust evaluation frameworks are extensively employed in IoT to evaluate the dependability and security of devices and systems. These models depend on established rules and policies to assess elements such as device behaviour, interaction history, and security compliance. By establishing explicit criteria, they assist in assessing the trustworthiness of a device within the network.

Some common policy-based trust evaluation models for IoT include:

Access Control Policies

These policies impose stringent regulations on network and data access, allowing only authenticated devices with appropriate credentials to connect. By authenticating device identities and authorisation privileges, they thwart unauthorised access while facilitating secure communication among trusted IoT components, thereby preserving system integrity against potential breaches.

Risk Assessment Protocols

These frameworks methodically assess vulnerabilities linked to connected IoT devices through the analysis of behavioural patterns and historical data. They assess threat probabilities and impacts, facilitating the proactive implementation of countermeasures such as encryption or access restrictions to mitigate risks prior to exploitation, thereby ensuring continuous operational security.

Confidentiality Agreements

These regulations delineate stringent protocols for the management of sensitive user information within IoT ecosystems. They delineate acceptable data collection methods, processing constraints, and secure storage protocols while employing anonymisation techniques as necessary, ensuring adherence to data protection regulations and preserving user confidentiality.

Security Surveillance Protocols

These protocols facilitate real-time monitoring of IoT network activities through the utilisation of intrusion detection systems and anomaly detection. Through the ongoing analysis of device behaviours and traffic patterns, they swiftly detect suspicious activities, activate alerts, and implement automated defensive measures to mitigate potential security incidents prior to system compromise. The policy-driven trust assessment algorithm for Social IoT is founded on conventional methodologies, integrating SIoT-specific elements. The process entails: (1) establishing trust policies encompassing social relationships, (2) collecting interaction history and reputation data, (3) implementing policies via rule-based or machine learning analysis, (4) calculating trust scores, and (5) rendering access decisions based on predetermined thresholds. This methodology modifies conventional models to accommodate the social dimensions of the Social Internet of Things (SIoT).

Definition of Policy

The preliminary phase defines assessment criteria for SIoT entities, including reputation metrics, interaction history, and transaction categories. Particular attention is directed towards social connectivity elements, encompassing relationship networks and reciprocal influence among devices, to tackle the collaborative essence of social IoT ecosystems. These extensive policies constitute the basis for trust evaluation.

Data Acquisition

The system consolidates pertinent entity data, encompassing historical interaction records, reputation metrics, and behavioural trends. It critically captures social graph data, including trust ratings of interconnected devices and relationship dynamics. This multifaceted dataset facilitates comprehensive trust assessment by integrating conventional IoT metrics with social network attributes.

Execution of Policy

Gathered data is subjected to thorough analysis in accordance with established policy criteria. Evaluation methodologies encompass threshold-based reputation assessments and sophisticated machine learning algorithms. The process distinctly evaluates social factors, analysing how an entity's network position and peer trust influence its overall credibility within the SIoT ecosystem.

Quantification of Trust

Each entity is assigned a calculated trust score that indicates its adherence to policy requirements and its observed conduct. This numerical representation integrates objective metrics with social context, yielding a comprehensive trustworthiness indicator. Scores are dynamically modified to represent evolving interactions and shifting network relationships.

Access Assessment

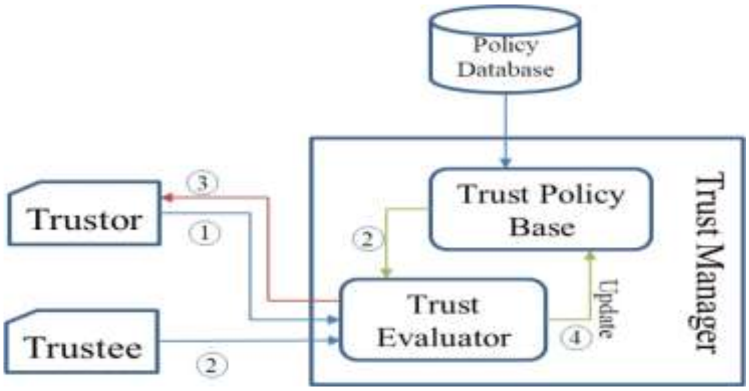

Figure 3.1: Components of Policy based trust model

The system implements trust-based access control by evaluating computed scores against security thresholds. Entities that do not satisfy minimum trust criteria will encounter limited access or total interaction prohibition. This decision-making process consistently evolves to uphold system integrity while facilitating legitimate SIoT collaborations. Figure 3.1 illustrates the elements of the policy-based trust model, which is a methodology for establishing and sustaining trust relationships among various entities within a system, grounded in a set of predefined policies. The model comprises multiple components, each of which is essential to the trust management process. The primary elements of a policy-based trust model are:

ALGORITHM TO COMPUTE WEIGHTED VOTING IN TRUST AGGREGATION TECHNIQUE

Input : Trust scores of the sources (S1, S2, ..., Sn) and weights of sources (W1, W2, ..., Wn)

Output : Overall trust score T

Step 1 : Assign weights to each source of information W1, W2, ..., Wn

Step 2 : Calculate the trust score for each source S1, S2, ..., Sn

Step 3 : Normalize the scores

for i= 1 to n

$S_i' = (S_i, - \min (S_i, S_{i-2}, ..., S_n)) / (\max (S_i, S_{i-2}, ..., S_n) – \min (S_i, S_{i-2}, ..., S_n))$

Step 4 : Multiply scores by weights for i= 1 to n

$T_i = W_i * S_i'$

Step 5 : Sum the weighted scores

T = T1 + T2 + ... + Tn

Step 6 : Normalize the overall score

T' = (T - min (T1, T2, ..., Tn)) / (max (T1, T2, ..., Tn) - min (T1, T2, ..., Tn))

Step 7 : Return the overall trust score

return T'

This algorithm utilises each source's trust score and associated weights as input, computes the overall trust score through the weighted voting method, and outputs the result.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 07, July 2025, pp : 682-693

e-ISSN : 2583-1062
Impact Factor : 7.001

Example of compute Weighted voting

Consider three sources, A, B, and C, that furnish trust scores for an IoT device. The trust scores are assigned as follows:

Source A: Trust score = 0.7 Source B: Trust score = 0.8 Source C: Trust score = 0.6

To amalgamate these trust scores into a comprehensive trust score utilising the weighted voting method, we initially allocate weights to each source according to their credibility or reliability. If source A is deemed the most credible, it may be assigned a weight of 0.6, whereas sources B and C could receive weights of 0.3 and 0.1, respectively.

Next, we compute the weighted trust score by multiplying each source's trust score by its weight and summing the results:

Weighted trust score = (0.7 * 0.6) + (0.8 * 0.3) + (0.6 * 0.1) = 0.42 + 0.24 + 0.06 = 0.72.

The weighted voting method calculates an aggregate trust score (0.72 in this instance) by amalgamating various trust evaluations, with values spanning from 0 (untrustworthy) to 1 (completely trusted). The contribution of each source is assessed based on its credibility, with more reliable sources exerting greater influence. This approach offers a balanced, quantitative assessment of IoT device trustworthiness by integrating various trust indicators in proportion to their established reliability.

Dempster-Shafer theory in trust aggregation

The Dempster-Shafer theory provides a comprehensive mathematical framework for trust aggregation in IoT systems by adeptly handling uncertainty via basic probability assignments (BPAs) that measure belief in diverse trust propositions. This method integrates various trust sources utilising Dempster's combination rule, which adeptly resolves conflicting evidence via a conflict function that quantifies disagreement among sources and proportionately modifies the resultant uncertainty in the ultimate trust evaluation. This method is especially beneficial in trust management systems, as it handles incomplete or contradictory information from various sources without necessitating complete probability distributions, instead utilising specified belief intervals that more accurately represent real-world trust assessment situations. Its capacity to sustain and measure uncertainty during the aggregation process renders it superior to basic averaging methods when addressing unreliable or conflicting trust data, as it maintains evidentiary distinctions while methodically amalgamating beliefs. The theory's adaptability enables trust metrics to integrate both corroborative evidence and lingering uncertainties, yielding comprehensive trust scores that clearly indicate the confidence level in the assessment, rendering it particularly appropriates for dynamic IoT environments where information quality fluctuates considerably among sources.

ALGORITHM TO COMPUTATION OF TRUST USING DEMPSTER-SHAFER THEORY

Input : Trust scores of the sources (S1, S2, ..., Sn) and corresponding Basic Probability Assignments (BPA) (BPA1, BPA2, ..., BPAn)

Output : Final BPA and overall trust score T

Step 1 : Calculate the BPA for each source BPA1, BPA2, ..., BPAn

Step 2 : Combine the BPAs using the Dempster-Shafer combination rule BPA = Dempster-Shafer combination (BPA1, BPA2, ..., BPAn)

Step 3 : Calculate the conflict function between the BPAs conflict = conflict function (BPA1, BPA2, ..., BPAn)

Step 4 : Calculate the overall trust score

T = (1 - conflict) * belief mass of the highest trust proposition in BPA

Step 5 : Return the final BPA and overall trust score return BPA, T

The Dempster-Shafer algorithm integrates trust scores and probability assignments from various sources through the application of evidence theory. It integrates data using combinatory rules while assessing discrepancies among sources. The method computes normalised belief values that consider uncertainty, yielding comprehensive trust metrics. This methodology manages incomplete or contradictory evidence more effectively than traditional techniques, rendering it suitable for IoT systems where information reliability fluctuates among various sources.

Fuzzy logic in trust aggregation

Fuzzy logic efficiently consolidates trust in IoT systems by evaluating uncertain values via membership functions and linguistic variables (e.g., "high/medium" trust). It manages partial truths through fuzzy sets instead of binary classifications, facilitating nuanced trust modelling. The methodology integrates various sources through rule-based inference systems that preserve uncertainty during computations. This adaptability facilitates dynamic contexts in which trust is perpetually evolving, rendering it more effective than rigid logic for addressing ambiguous or

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 07, July 2025, pp : 682-693
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

contradictory trust signals. Fuzzy methods systematically convert qualitative evaluations into quantitative scores, maintaining authentic trust gradations, which is especially beneficial when handling imperfect data from various sources.

Working of Fuzzy logic in trust aggregation

Fuzzy logic can be employed in trust aggregation for IoT similarly to its application in general trust aggregation. The fundamental steps are outlined below:

Simulation

This preliminary stage converts unrefined trust scores into fuzzy sets through the application of membership functions. The reliability of each source is quantified as a graded value ranging from 0 to 1, incorporating uncertainty through trapezoidal, triangular, or Gaussian curves that delineate the degree to which a score aligns with specific trust categories, facilitating a nuanced representation that transcends binary classifications.

Fuzzification

The system transforms numerical trust values into qualitative linguistic variables (e.g., "low:0.3", "medium:0.7") through established membership functions. This translation facilitates the processing of ambiguous trust data via natural language terms that more accurately represent real-world trust gradations and subjective evaluations from various sources.

Deduction

A rule engine (e.g., Mamdani or Sugeno systems) utilises IF-THEN rules to amalgamate linguistic trust assessments. These regulations delineate the interactions among various trust categories (e.g., "IF Source1=high AND Source2=medium THEN Trust=high"), yielding aggregated fuzzy outputs that represent intricate trust relationships among multiple sources.

Defuzzification

The fuzzy inference outcomes are transformed into precise numerical values through techniques such as centroid calculation or maximum membership. The final numerical score (e.g., 0.82) facilitates definitive security decisions regarding resource access, service allocation, or authentication levels, while maintaining the complexity of fuzzy evaluation.

The primary benefit of employing fuzzy logic in trust aggregation for IoT lies in its capacity to represent uncertainty and imprecision in trust values, which is crucial in IoT systems characterised by devices and sensors with differing levels of reliability and security. Fuzzy logic is particularly appropriate for dynamic and evolving systems where trust values may fluctuate over time.

Steps involved in Fuzzy logic to compute trust are as follows:

- Acquire trust values from multiple sources.
- Modelling: Establish a collection of linguistic terms that denote trust values.
- Fuzzification: Transform the trust values into fuzzy sets.
- Inference: Utilise a series of regulations to calculate the conclusive trust score.
- Defuzzification: Transform the ultimate trust score into a numerical value.
- Output: Conclusive trust score, indicative of the system's overall reliability.

4. RESULTS

The KE model employs MATLAB to analyse real-world network interaction data from the SIGCOMM-2009 dataset (accessible in CRAWDAD [145-146]) for trust assessment. The raw data is mathematically modelled to derive five essential trust properties, normalised to values between 0 and 1, and stored in a matrix in .csv format, representing the Knowledge Trust Mark. This matrix (depicted in Figure 4.1) is subjected to classification to discern trustworthy from untrustworthy objects. In the Experience model, MATLAB simulates three temporal dynamics—development, loss, and decay—utilizing the identical processed dataset. The extensive framework integrates quantitative property analysis with temporal interaction patterns, facilitating a reliable trust evaluation in IoT networks via verifiable metrics obtained from genuine device communications.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 07, July 2025, pp : 682-693

e-ISSN : 2583-1062
Impact Factor : 7.001

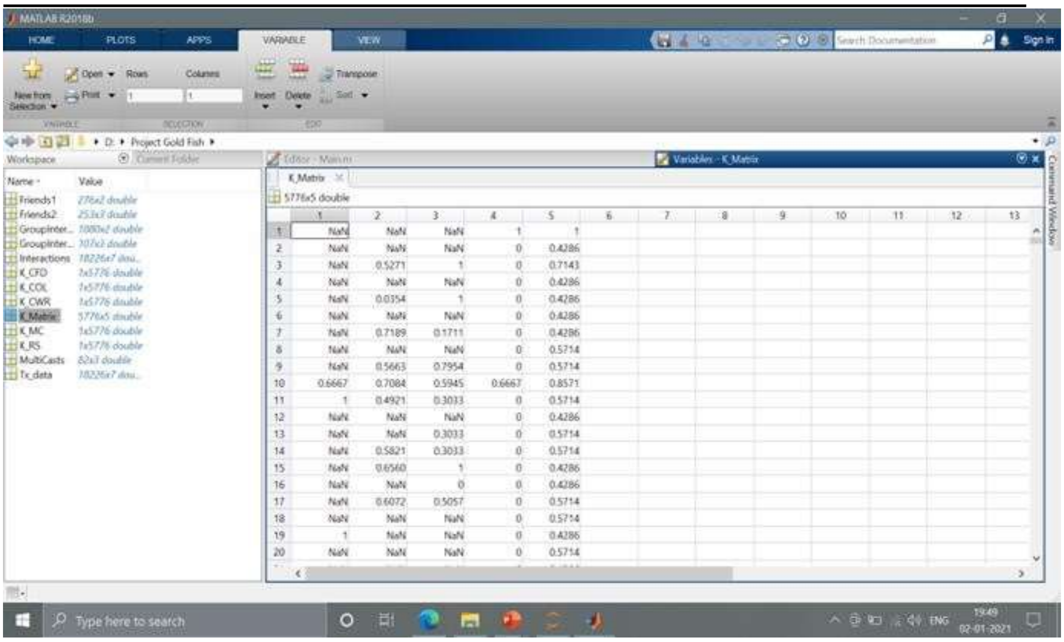

Figure 4.1: Extracted five trust Properties for Knowledge Trust Mark

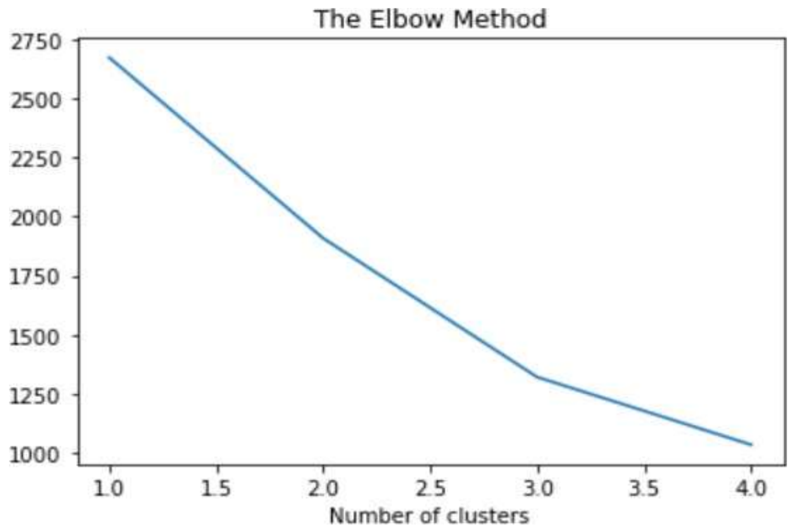

Figure 4.2: Elbow method for optimum cluster size

The normalised trust properties (ranging from 0 to 1) are clustered using the k-means algorithm, with the optimal number of clusters identified through the elbow method. For this analysis, three distinct clusters were chosen, as visually corroborated in Figure 5.6, which illustrates the clustered data points categorised by their trust characteristics. This tripartite classification accurately categorises objects according to their levels of trustworthiness derived from the analysed dataset.

The k-means algorithm classifies data into three clusters (0=untrustworthy, 1=trustworthy, 2=ideal), as illustrated in Figure below. PCA subsequently reduces dimensions to PC1 and PC2, mitigating overfitting while maintaining critical trust patterns for analysis. The SVM algorithm utilising an RBF kernel proficiently categorises objects into trustworthy, untrustworthy, or ideal classifications based on Knowledge Trust Metrics, attaining approximately 99% accuracy, as illustrated in Figure below. The elevated precision is corroborated by a confusion matrix and an accuracy score visualisation (Figure 5.10), underscoring the model's resilience in managing non-linear IoT data. The RBF kernel's capacity to identify intricate patterns guarantees dependable trust assessment, rendering it appropriate for dynamic IoT settings. The results highlight the SVM's outstanding ability to differentiate trust levels, providing a reliable solution for trust-oriented decision-making in interconnected systems.

Out[4]:

	CWR	CFD	RS	MC	COL	label
0	0.0	0.000000	0.000000	1.0000	1.000000	0
1	0.0	0.000000	0.000000	0.0000	0.428571	0
2	0.0	0.527102	1.000000	0.0000	0.714286	1
3	0.0	0.000000	0.000000	0.0000	0.428571	0
4	0.0	0.035397	1.000000	0.0000	0.428571	1
...	...	...	...	...	...	...
5771	0.0	0.000000	0.303265	0.0000	0.187500	0
5772	0.0	0.000000	0.000000	0.0000	0.250000	0
5773	1.0	0.509717	0.402192	0.1875	0.437500	2
5774	1.0	0.000000	0.000000	0.3125	0.312500	2
5775	0.0	0.000000	0.000000	1.0000	1.000000	0

5776 rows × 6 columns

Figure 4.3: Labelled dataset using K-means algorithm

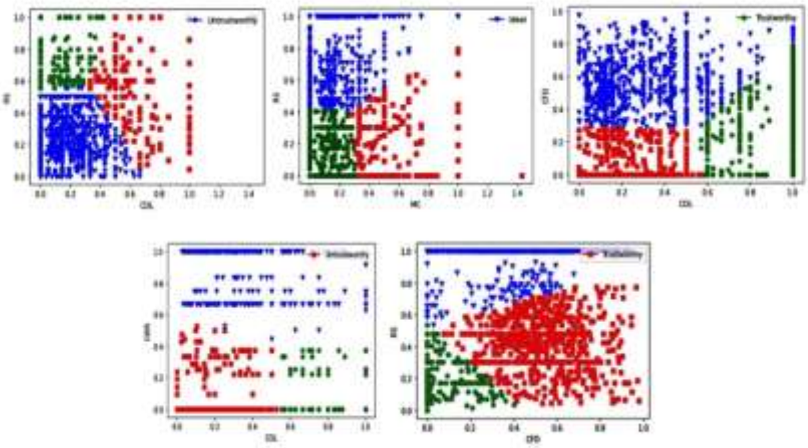

Figure 4.4: Classification of Five properties taking two at each time

Interaction values from Principal Component Analysis (PCA) are utilised to ascertain the three attributes of Experience Trust Mark—development, loss, and decay—which are subsequently analysed visually. In contrast to the Knowledge Trust Mark, the Experience Trust Mark cannot evaluate trust solely on these attributes, necessitating a more profound interaction-based assessment. A trustor (61st node) and trustee (66th node) with frequent interactions are analysed to illustrate their impact. The graph depicts the impact of each interaction on the three properties of Experience Trust, highlighting behavioural patterns in the evolution of trust. This visualisation evaluates the model's efficacy in capturing dynamic trust dynamics, highlighting the significance of repeated interactions in forming experiential trust.

5. CONCLUSION

The Internet of Things (IoT) is rapidly expanding, linking billions of devices worldwide. This growth, however, raises substantial concerns regarding privacy and security. This thesis presents a Trust-Based Security Mechanism designed to tackle these challenges by emphasizing trust management in IoT and Social IoT (SIoT) networks. It examined the diverse attack vectors that jeopardize IoT systems, the essential trust attributes to evaluate, and the layered architecture and protocols underpinning these networks. A thorough examination of current trust management methodologies, dissemination platforms, and assessment frameworks was performed. The study elucidated essential processes including trust aggregation, composition, and formation, which are crucial for sustaining security and trust within interconnected IoT ecosystems, especially in sensitive domains such as healthcare. This research significantly contributed by developing a Knowledge and Experience (KE)-based trust evaluation model utilizing machine learning algorithms. This model examined trust by concentrating on two principal trust indicators—Knowledge and Experience—providing enhanced insights into trust dynamics within IoT systems. The thesis proposed an intelligent trust management system based on deep learning, specifically designed for healthcare big data environments utilizing IoT. This system utilized a BiLSTM (Bidirectional Long Short-Term Memory) model to proficiently identify vulnerabilities and malicious traffic, thereby enhancing network reliability and security. The amalgamation of deep learning with trust management presents a promising strategy for alleviating sophisticated threats in real-time and facilitates the secure implementation of IoT applications within critical infrastructures.

The Trust-Based Security Mechanism outlined in this thesis exhibits significant potential for enhancing the privacy and security of IoT networks. Nonetheless, several areas require additional improvement. Future endeavours may involve incorporating the third trust mark—Reputation—into the model to enhance trust assessments. The proposed deep learning-based trust management system can be augmented to accommodate various datasets and IoT/SIoT network types, thereby enhancing its generalizability. The practical implementation and evaluation of the framework in actual settings would yield significant insights regarding its efficacy. This thesis provides a robust basis for further research in trust-based security, focusing on the resolution of emerging challenges in protecting IoT ecosystems via intelligent, adaptive, and scalable trust mechanisms.

6. REFERENCES

[1] B. Chander, S. Pal, D. De, and R. Buyya, “Artificial intelligence-based internet of things for industry 5.0”, Artificial intelligence-based internet of things systems, pp. 3-45, 2022.

[2] S. Dhelim, H. Ning, F. Farha, L. Chen, L. Atzori, and M. Daneshmand, “IOT- enabled social relationships meet artificial social intelligence”, IEEE Internet of Things Journal,vol. 8, no. 24, pp. 17817-17828, 2021.

[3] A. R. Javed, F. Shahzad, S. ur Rehman, Y. B. Zikria, I. Razzak, Z. Jalil, and G. Xu,“Future smart cities requirements, emerging technologies, applications, challenges, and future aspects”, Cities, vol.129, p. 103794, 2022.

[4] S. Kumar, G. Mahesh, and C. K. Marigowda, “Threats in IoT supply chain”, in Internet of Things, Threats, Landscape, and Countermeasures. CRC Press, 2021, pp. 167-200.

[5] B. B. Gupta and M. Quamara, “An overview of internet of things (IoT): Architectural aspects, challenges, and protocols”, Concurrency and Computation: Practice and Experience, vol. 32, no. 21, p. e4946, 2020.

[6] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, “Security of the internet of things: perspectives and challenges”, Wireless Networks, vol. 20, pp. 2481-2501, 2014.

[7] X. Lv and M. Li, “Application and research of the intelligent management system based on internet of things technology in the era of big data”, Mobile Information Systems, vol. 2021, pp. 1-6, 2021.

[8] A. I. A. Ahmed, S. H. Ab Hamid, A. Gani, M. K. Khan et al., “Trust and reputation for internet of things: Fundamentals, taxonomy, and open research challenges”, Journal of Network and Computer Applications, vol. 145, p. 102409, 2019.

[9] J. I. R. Molano, J. M. C. Lovelle, C. E. Montenegro, J. J. R. Granados, and R. G. Crespo, “Metamodel for integration of internet of things, social networks, the cloud and industry 4.0”, Journal of ambient intelligence and humanized computing, vol. 9, pp. 709-723, 2018.

[10] R. Faqihi, J. Ramakrishnan, and D. Mavaluru, “An evolutionary study on the threats, trust, security, and challenges in siot (social internet of things)”, Materials today: proceedings, 2020.

[11] Q. Pei, R. Liang, and H. Li, “A trust management model in centralized cognitive radio networks”, in 2011 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. IEEE, 2011, pp. 491-496.

[12] F. Hajibabaei and M. H. Y. Moghaddam, “Proposing a centralized trust management system to detect compromised node in wsn”, in ICCKE 2013. IEEE, 2013, pp. 315-320.

[13] B. K. Mughal, S. Hameed, and G. M. Shaikh, “A centralized reputation management scheme for isolating malicious controller (s) in distributed software-defined networks”, arXiv preprint arXiv:1711.11005, 2017.

[14] A. Chakrabarti, Grid computing security. Springer Science & Business Media, 2007.

[15] P. Thota and Y. Kim, “Implementation and comparison of m2m protocols for internet of things”, in 2016 4th Intl Conf on Applied Computing and Information Technology/3rd Intl Conf on Computational Science/Intelligence and Applied Informatics/1st Intl Conf on Big Data, Cloud Computing, Data Science & Engineering (ACIT-CSII-BCD). IEEE, 2016, pp. 43-48.

[16] R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati, and M. Rossi, “Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples”, in 2012 IEEE international symposium on a world of wireless, mobile and multimedia networks (WoWMoM). IEEE, 2012, pp.1-7.

[17] S. Rao, D. Chendanda, C. Deshpande, and V. Lakkundi, “Implementing lwm2m in constrained iot devices”, in 2015 IEEE Conference on Wireless Sensors (ICWiSe). IEEE, 2015, pp. 52-57.

[18] M. A. da Cruz, J. J. Rodrigues, P. Lorenz, P. Solic, J. Al-Muhtadi, and V. H. C. Albuquerque, “A proposal for bridging application layer protocols to http on iot solutions”, Future Generation Computer Systems, vol. 97, pp. 145-152, 2019.