I.J. Information Engineering and Electronic Business, **2024, 4, 28-46**
Published Online on August 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2024.04.03

Security Framework for Social Internet of Things: A Relativity Strength Approach

K. S. Santhosh Kumar
Department of Studies in Computer Science, University of Mysore, Manasagangothri campus, Mysuru-570006, Karnataka, India
E-mail: santhosh@compsci-uni.mysore.ac.in
ORCID iD: https://orcid.org/0000-0003-4792-8503

Hanumanthappa J.
Department of Studies in Computer Science, University of Mysore, Manasagangothri campus, Mysuru-570006, Karnataka, India
E-mail: hanumsj@yahoo.com
ORCID iD: https://orcid.org/0000-0002-6031-6993

S. P. Shiva Prakash*
Department of Information Science and Engineering, JSS Science and Technology University, Mysuru-570006, Karnataka, India
E-mail: shivasp@jssstuniv.in
ORCID iD: https://orcid.org/0000-0003-3490-6292
*Corresponding Author

Kirill Krinkin
School of Computer Science and Engineering, Constructor University, Bremen, Germany
E-mail: kirill@krinkin.com
ORCID iD: https://orcid.org/0000-0001-5949-7830

Received: 30 December, 2023; Revised: 20 February, 2024; Accepted: 07 March, 2024; Published: 08 August, 2024

Abstract: The evolution of the Internet of Things (IoT) into the Social Internet of Things (SIoT) involves the integration of social networking features into smart devices. In this paradigm, smart devices emulate human social behavior by forming social relationships with other devices within the network. These relationships are leveraged for service discovery, emphasizing the need for robust security to foster collaboration and cooperation among devices. Security is paramount in the SIoT landscape, as malicious messages from devices can disrupt service functionality, impacting service quality and reliability. These challenges are particularly pronounced in social networks, introducing unique considerations such as heterogeneity and navigability. This study introduces a Security Framework for the Social Internet of Things, adopting a Relativity Strength Approach to enhance the security and reliability of IoT devices within social network contexts. The framework incorporates a relativity-based security model, utilizes Q-learning for efficient device navigation, and employs decision tree classification for assessing service availability. By optimizing hop counts and considering the strength of relationships between devices, the framework enhances security, resource utilization, and service reliability. The proposed security framework introduces a" Relationship key" derived from device-to-device relationships as a central element. This key, coupled with a standard 256-bit Advanced Encryption Standard (AES) algorithm, is employed for encryption and decryption processes. The relationship key technique ensures data protection during transmission, guaranteeing confidentiality and service integrity during network navigation. The system demonstrates an overall security effectiveness of 88.75%, showcasing its robustness in thwarting attacks and preventing unauthorized access. With an impressive overall communication efficiency of 91.75%, the framework minimizes errors and delays, facilitating optimal information trans- mission in smart environments. Furthermore, its 97.5% overall service availability assures a continuous and reliable user experience, establishing the framework's capability to deliver secure, efficient, and highly accessible smart services.

Index Terms: Security, Relative strength, Social Internet of Things, Decision Tree, Reinforcement Learning, Attacks

1. Introduction

The social Internet of Things is a new field of investigation in the growing technology sphere. The merging of the worlds of the” Internet of Things” and” Social Networks” is gaining popularity. This is due to a rising realization that the Artificial Intelligence Security (AIS) paradigm would have many good implications for a future society populated by intelligent items employed in human daily lives. According to which devices are capable of establishing social relationships concerning their owners in a completely self-governing manner, with the benefits of improving network scalability in information and service discovery. In which devices in the network interact freely based on a predefined connection. Artificial intelligence (AI) is utilized to instill strong trust in intelligence security framework. To ensure that authenticated devices survive and are safer in the network and environment, they are evaluated bilaterally between the requesting device and the response device in a SIoT network of intelligence security framework for devices. When socially Connected Devices do not have social relationships, problems such as loss of privacy, safety, security, access, and information manipulation by unauthorized items occur. Devices may launch harmful attacks depending on how they interact with other Devices. As a result, determining their service for the SIoT to identify the proper interaction between the request and response devices. Because each item has its own vulnerability and attack vector, confidentiality is one of the most serious issues. The Advanced Encryption Standard (AES) versions, including key size, security level, performance, and whether they are authorised by the National Institute of Standards and Technology (NIST). AES-128, with a key size of 128 bits, provides great security and efficient performance, making it suited for common protocols such as TLS and general-purpose encryption. In cases demanding additional security, AES-192 with a 192-bit key gives a larger security margin. AES-256, with a 256-bit key, provides the maximum degree of protection and is suitable for rigorous security needs and data with a long-term security focus. In addition to the typical AES methods, A relationship-based security model employs a 256-bit key to provide excellent security and efficiency, making it ideal for safeguarding data in the Social Internet of Things (SIoT). A fundamental method employed is encryption, which plays a pivotal role in securing data during transmission. Data is transformed into encrypted text using a specific model before being sent from the source object to the destination object provided the guaranteed service. The process ensures that sensitive information remains confidential and secure during its journey through the network. Subsequently, decryption is implied upon reaching the destination, enabling the intended recipient to retrieve and comprehend the original data. Additionally, the identification of an attacker is a key aspect of the method, where machine learning approaches are utilized to an attacker due to the failure of these checks. This underscores the significance of combining encryption techniques with advanced machine-learning methodologies for comprehensive security in network communication. The pivotal method revolves around establishing and deciphering relationships between objects within the network. The essence lies in the identification of relationships through machine learning approaches, treating these relationships as a key aspect of security. By deciphering the intricate connections between entities, the system ensures a secure exchange of information. Highlight the critical role of relationship-based analysis in detecting potential threats within the network. In essence, the method intertwines encryption, decryption, and the insightful understanding of relationships to fortify the integrity of the communication channels and safeguard against malicious activities.

1.1 Smart world: Need security in Smart world Real Applications

Real-world applications of the Smart World concept include smart cities, healthcare, agriculture, transportation, energy management, environmental monitoring, retail, education, emergency services, manufacturing, and wearable technology, enhancing efficiency and connectivity for the applications like Weather, Street light, Waste management, traffic, parking, bus, cinema, crowded applications.

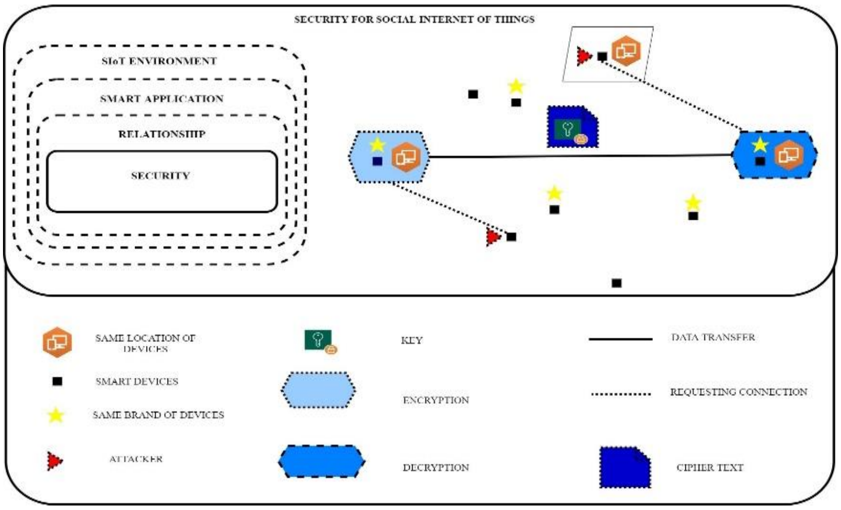


Fig. 1. Security for Smart world Real Applications

Security Steps in the Smart World: Authenticate users and devices, encrypt data, enforce access controls, update regularly, scan for vulnerabilities, protect privacy, manage devices centrally, educate users, prepare for incidents, segment networks, prioritize secure development, safeguard physically, assess third-party providers, minimize data, and monitor continuously.

Table 1. AES Variants with SIoT Perspective

Algorithm	Key Size	Security Level	Performance
AES-128	128 bits	High	Efficient
AES-192	192 bits	Higher	Moderate
AES-256	256 bits	Highest	Moderate to High

1.2 Background of study

Social Internet of Things is a new area of exploration in the technology domain is trending. With the convergence of the IoT and the Social network momentum is gained by the whole world. This is due to the fast-growing awareness that a Social Internet of Things paradigm would carry many desirable implications for a future world population by intelligent devices that are used in the everyday life of human beings. According to which devices are capable of establishing social relationships autonomously concerning their owners with the benefits of improving the network stability in information/services. Where the idea in the network interacts independently according to a certain relationship formed between each other. AI technique is used for imparting robust trust between SIoT devices. Trustworthiness is evaluated bilaterally between the trustee and trustor. The SIoT devices for making authenticated devices survive and be safe in the environment. The performance of the trust evaluation scheme is analyzed for a dynamic environment for distinguishing malicious behaviour of SIoT devices using AI algorithms and the major factors are as follows Secrecy (confidentiality), Integrity, and Availability (e.g., resilience to denial-of-service attacks). Table 1 summarises the major elements of AES Variants with SIoT Perspective.

1.3 Challenges and motivations

1.3.1 Challenges

The proposed work encountered various challenges, outlined as follows:

Heterogeneous Device Ecosystem: The diverse range of IoT devices in a social network introduces challenges in managing their security and interactions. Ensuring compatibility and security across different device types can be complex.

Dynamic Network Topology: Social IoT networks are dynamic, with devices constantly joining, leaving, or moving within the network. This dynamic topology makes it challenging to maintain consistent security and service availability.

Reliability and Availability: Guaranteeing the reliability and availability of services on SIoT devices is challenging, especially when dealing with varying network conditions and service demand.

Data Security: The security of data exchanged between SIoT devices is a critical concern. Ensuring that sensitive data remains protected is a challenge, particularly in a social network context where data may be shared between devices.

Scalability: As SIoT networks grow, ensuring the scalability of security measures and service availability assessments becomes a complex task.

1.3.2 Motivation

The development of the Security Framework for the Social Internet of Things was motivated by several factors like Growing Significance of IoT, The unique challenges posed by social IoT networks, where devices interact and collaborate, Enhanced Security Requirements, Efficient Device Navigation, Service Availability Assurance and also this work is motivated by the desire to contribute to the field of IoT research by introducing innovative methods and approaches to address the challenges of security and service availability in social IoT environments.

1.4 Key Contributions

The following are the key contributions of this work:

- **Social Relationship Integration:** The Proposed Framework pioneers the integration of social relationships into the IoT landscape. By imitating human-like connections among devices, it introduces a new layer of security that leverages the strength of relationships, enhancing the overall robustness of the system.
- **Predictive Service Availability with Decision Trees:** The incorporation of decision tree models for predicting service availability represents a significant contribution. This predictive modeling enhances the assessment of each device’s capability to provide services, contributing to overall reliability and performance in the SIoT environment.

- **Adaptive Navigation with Q-learning:** Utilizing Q-learning, the algorithm enables devices to adaptively navigate the network by optimizing hop counts. This adaptive navigation enhances communication efficiency, allowing devices to dynamically adjust their interactions based on past experiences and relationship strengths.

The Organization of the paper is as follows: Section 1 Introduces the concept, in Section 2 discusses related works and state of the art. In Section 3 with the Problem statement, System model, and proposed solutions in Section 4 discusses about Relativity Strength Approach framework for SIoT. Continue with the algorithm in Section 5 used to solve the work with greater efficiency to secure the System, in Section 6 provides results and discussion including simulation environment setup, user-defined parameters, data set model evaluation, and result analysis of the proposed. Finally, Section 7 concludes the work.

2. Related Work

Chen, Ing-Ray et al. [1] investigate adaptive trust management for social IoT networks, in which device owners' social ties change over time. The authors provide a protocol layout that strikes a compromise between trust convergence and fluctuation and enables applications to select the best trust parameter values in response to shifting social circumstances. This method maximizes the efficiency of the programme while guaranteeing accurate trust evaluations. Additionally, the author suggests a dynamic table-lookup mechanism to show how the suggested scheme might be implemented in practical social IoT service composition applications. The Author Jadhav, et al. [2] Provides a secure authentication system based on social networking sites such as Facebook that remotely monitors end users' physical home environments. This solution addresses the difficulties of security and usability in traditional and wireless home automation techniques. The system enables customers to remotely control and provide home security. The researcher Han, et al. [3] presents a dynamic routing-based source location protection system for the Social Internet of Things (SIoT). By randomly selecting an initial node from the network's boundary, the protocol maximises data transmission pathways. Packages follow a predetermined path before arriving at the wash basin. The suggested technique protects source location privacy and defeats privacy disclosure threats without reducing network lifetime, according to theoretical and experimental results. G. Ruggeri and O. Briante, [4] discusses how the Social Internet of Things (SIoT) might be used to integrate and develop e-health systems, particularly for the older population in developed countries. The World Health Organisation emphasizes the importance of ongoing medical monitoring and assistance for the elderly, implying that IoT-based e-health solutions can improve their quality of life. A novel Devices search mechanism is proposed by Roopa, et al. [5], to improve search performance in the Social Internet of Things (SIoT) paradigm based on the physical location, proximity, and social context of users in social communities, resulting in an enhancement in average path length. A new algorithm for analyzing service performance in the Social Internet of Things (SIoT) domains is proposed by Amin, et al. [6], with an emphasis on clustering coefficients, path lengths, and large components. Experiments show that it is effective at shortening paths and increasing grouping coefficients. The Internet of Things (IoT), which is gaining popularity due to its adaptability, is facing issues due to the exponential increase of heterogeneous devices. Simulation results show improved accuracy. Despite the fact that IoT applications are frequently inefficient in sharing data and knowledge. Bhavsar, et al. [7], introduces the notion of social IoT for effective data sharing, showing its potential architecture, components, levels, and procedures. Patnaik, et al. [8], propose a similarity-based Devices search mechanism that dynamically manages relationships based on physical location, proximity, and social context, outperforming existing search techniques in the overpopulation of IoT devices and finding the shortest path to service providers. In a decentralized SIoT network, Azad, Muhammad Ajmal et al. [9] proposes a novel framework for calculating and maintaining trustworthiness that does not rely on reliable outside sources. To safeguard participant privacy, homomorphic encryption is used, and each device's trust score is updated in response to votes from the network and its prior score. When more network members are added, the system's performance is assessed and it is shown that computing and communication overheads rise linearly. Under a malevolent adversarial paradigm, its security, privacy, and accuracy are demonstrated. Using the" no pain, no gain" tenet, Wang, Bowen et al. [10] investigate the security of A2G communications in unpredictable location data. In worst-case situations, it suggests combining trajectory design, power control, and channel allocation optimization challenges to optimize the average secrecy rate of UAVs. These issues are solved by sequential convex optimization techniques using block coordinate descent. It is suggested that two distributed algorithms be used to keep popular matching under dynamics. Popularity, convergence, and computing complexity are examined in the study, and simulation results demonstrate the method's better performance metrics. In order to improve IoT security, Kalyani, et al. [11] propose techniques based on cryptography. Sensitive IoT data is secured using Optimal Homomorphic Encryption (OHE), which is categorized using a Deep Learning Neural Network (DNN) structure. To ensure privacy-preserving data and maximize key breaking time, the encryption procedure entails authenticating the key and choosing the best key using the Step Size Fire Fly (SFF) optimization method. The study explores the security threats of the Social Internet of Things (SIoT) in higher education by Mawgoud, et al. [12] including identity and information leakage, device manipulation, record falsification, server and network attacks, and application platform effects. The lack of existing literature and proposed solutions contributes to a lack of comprehensive understanding of data protection and privacy in the IoT. Rehman, et al. [13]. Introduce the Smart Social Agent (SSA) to seek out acceptable friendships and user services on the Social Internet of Things without human intervention. Because of the exponential rise of IoTs, the SSA can be any Device in SIoTs, overcoming issues in identifying particular services or devices among billions of devices. Maddali et al. [15] presents a novel method for Internet of Things (IoT) security that leverages conflict resolution and knowledge-based rules (LOCSKS). To assess node activity based on location, context, and social goals, the system employs Bayesian decision theory. Exclusive and affordable keys are used by LOCSKS to guarantee location privacy and trust. Comparing the proposed LOCSKS approach to current schemes, simulations demonstrate that it successfully identifies node activity, lowers key violations, and improves location privacy. Using a comprehensive literature review methodology, Farhadi, et al. [16]. Investigate the selection and administration of social friendships in the Social Internet of Things (SIoT). It divides studies into five categories: structure-based, community-based, ontology-based, recommendation-based, and others. The report also addresses new problems and future research directions, emphasizing the importance of conducting more systematic research on this topic. The researcher Hussain, et al. [18] investigates the integration of smart IoT and machine learning in social IoT, highlighting both the potential benefits and the challenges of location privacy. The Analytic Hierarchal Process (AHP) is used to suggest a hybrid phantom technique that combines a phantom node and a multi-path route. This strategy minimizes energy consumption, boosts network lifetime, and improves safety periods, emphasizing the importance of addressing these difficulties in the field of social IoT. DSL-STM, a dynamic, scalable trust model developed for SIoT contexts, is introduced by Abdelghani, et al. [19]. It employs multidimensional metrics to define and collect SIoT entity behaviors, classify users, and identify and counteract threats yes. To distribute trust values while consuming as few resources as possible, a hybrid propagation mechanism is proposed. The model's goal is to mitigate trust attacks and provide dependable exchanges on the social Internet of Things. Sagar, Subhash et al. [20] offers a comprehensive analysis of trustworthiness management in the field of information and communication technology (IoT), classifying trust management schemes into four groups according to their features, components, strengths, and performance across a range of trust evaluation metrics. It also suggests future research areas. Dhillon, et al. [21], presents a separation architecture for social IoT (S-IoT) to manage trust between devices and services. It uses ontology architecture, the k-means algorithm, fuzzy logic inference engines, and genetic algorithms. A general reference model and optimization decision theory is used to optimize friend selection by Vaibhava Lakshmi, et al. [22]. The social Internet of Things (SIoT) is a potential technique for item discovery and service search that focuses on trust management and buddy selection. Storage space and battery life limitations, on the other hand, need steps to maximize device lifetime and durability. An intelligent friend selection strategy that takes Device attributes, typology, and functionality into account is necessary to exclude untrustworthy components. The Social Internet of Things is changing how we deliver personalized information. GNNs are used to replicate social diffusion processes; however, they frequently struggle to model user preferences and social influence. To address this, Bin Wu, et al. [23] introduced an efficient adaptive graph convolutional network (EAGCN) that surpasses strong baseline techniques in model efficacy and training efficiency. The author Maniveena, et al. [24] discusses security and privacy concerns in the Social Internet of Things (SIoT), highlighting the lack of developed protocols, device weaknesses, limited resources, and heterogeneous technology. It highlights the need for businesses to implement encryption, authentication, authorization, and access control systems to protect personal data privacy. To identify and distinguish malicious nodes from the Social Internet of Things, a new multi-hop convolutional neural network (MH-CNN-AM) is developed by Mohan Das, et al. [25]. The suggested model contrasts existing approaches with performance measurements. The issue is to improve data privacy while still providing high-quality services in IoT networks. Despite several models attempting to categorize safe nodes, none have been able to identify fake nodes or differentiate between different types of assault. The suggested methodology enhances classification, emphasizing the importance of trust in the IoT ecosystem. An intelligent friend selection technique by Mustafa, et al. [26] and considering Devices' qualities, typology, and functionality is needed to eliminate untrustworthy components. The social Internet of Things (SIoT) is a promising strategy for trust management and friend selection in Devices discovery and service search. However, storage space and battery life limits need to be addressed to maximize device lifetime and durability. Various security models exist in the literature, but none of them prevent attack occurrences. Artificial intelligence will be used to create a simulation environment for the Social Internet of Things, where social connections between the gadgets will be made, such as friendships, ownership, and communities. Using various machine learning techniques to identify anonymity, if a device is an attacker or not and determine whether communication devices have relativity, in order to manage relationships data is exchanged securely by encrypting it at the sender and decrypting it at the receiver end after the devices have established a connection.

2.1 State of the Art

The State of the art for work carried to the Security framework for the Social Internet of Things includes crucial Security management on the Social Internet of Things (SIoT) to ensure reliable data exchange and maintain service quality.

Table 2. State of the Art

Author	SIoT Relationship	Relativity Approach	High Data Security	Guaranteed Services
[14]	Yes	No	No	Yes
[17]	Yes	Yes	No	No
[28]	Yes	No	Yes	Yes
[29]	Yes	Yes	No	Yes

Secure relationships between the Sender and the requester are formed based on mutual benefits and are affected by various parameters. Confidentiality is also important in Security management. Each device has its vulnerabilities and attacks, so the system must prevent unauthorized access to data and information exchange. Smart devices can establish relationships using encryption and decryption mechanisms, and AI algorithms can be deployed to generate data and establish relation- ships. The process includes relationship security, data security, Evaluation metrics, existing tools, security analysis, and AI security mechanisms.

3. Problem Statement

In the rapidly evolving landscape of the Internet of Things (IoT), the integration of social networking into smart devices has opened new dimensions with the emergence of the Social Internet of Things (SIoT). While these devices simulate human social behavior and establish connections with each other, ensuring robust security within this interconnected ecosystem poses significant challenges. The current state of SIoT faces vulnerabilities, especially in the context of heterogeneity, navigability, and security threats. Devices, imitating social relationships, are susceptible to malicious activities that can disrupt service functionality, compromise the reliability of interactions, and undermine the quality of services provided. Existing security frameworks within IoT environments often fall short of addressing the unique characteristics and challenges introduced by social interactions among devices. The need for a comprehensive Security Framework for SIoT is evident, one that considers the strength of relationships optimizes communication efficiency, and ensures reliable service availability in the face of evolving security threats. Hence, there is a critical need for an algorithmic solution that not only addresses the security concerns inherent in SIoT but also contributes to the optimization of communication, considering the heterogeneity of devices and the dynamics of social relationships.

4. System Model

Let *D* be the set of devices in the SIoT networks, and let R_{ij} represent the strength of the relationship between devices *i* and *j*. The system model includes the security state S_i of device *i*, the hop count H_{ij} between devices *i* and *j*, and the service availability A_i of device *i*. The Set of all services requested within the network.

- S (i, m): A binary variable indicating whether service m is available on device i.
- R (i, j): A binary variable representing the relationship between devices i and j.
- Rel (i, j): The calculated relativity metric between devices i and j.
- Hop (i, j): The calculated hop count between devices i and j.

Objective Function

The objective is to maximize the overall security, minimize hop counts, and maximize service availability. The objective function (F) can be expressed as a weighted sum:

$$F = \sum_{i \in D} \alpha_i . S_i + \beta_i \left(\sum_{j \in D,\, j \neq i} R_{i,j} . H_{i,j} \right) + \gamma_i . A_i \tag{1}$$

Where, *αi, βi, γi* are weights reflecting the importance of security, hop count optimization, and service availability for device i.

Proposed Solutions

4.1 Devicesive Function

The Devicesive function for our proposed solution aims to balance service availability assessment (classification) and network exploration (hop count calculation):

$$Maximize: \sum_{i,j \in D} S(i,\ m) Rel(i,\ j)\ for\ Service\ Availability\ Assessment - \sum_{i,j \in D} R(i,\ j) Hop(i,\ j)\ forNetworkExploration \tag{2}$$

The Devicesive function combines two components: maximizing the product of service availability and relativity strength and minimizing the product of relationships and hop count.

4.1.1 Service Availability Assessment

The service availability assessment component can be represented as a binary classification problem using a decision tree. In this context, we can define a classification loss function L classification, such as cross entropy:

$$L_{classification} = -\sum_{i \in D, m \in M} [S(i,\ m)log(P(i,\ m)) + (1 - S(i,\ m))log(1 - P(i,\ m))] \tag{3}$$

Where, P (i, m) represents the predicted probability of service m being available on the device i based on the decision tree classification.

4.1.2 Network Exploration (Reinforcement Learning)

The network exploration component involves Q-learning to find the hop count between devices:

$$Q(i,\ j) = (1-\alpha)Q(i,\ j) + \alpha(R(i,\ j)\ + \gamma min(Q(k,\ j)\, fork \in D)) \tag{4}$$

Where, Q (i, j) is the Q-value representing the expected cumulative reward for moving from device i to device j, $\boldsymbol{\alpha}$ is the learning rate, $\boldsymbol{\gamma}$ is the discount factor, R (i, j) is the reward for moving from device i to device j (reward could be negative to discourage excessive hopping).

4.1.3 Combined Devicesive Function

The overall Devicesive function can be defined as the sum of the classification loss and the exploration Q-values:

$$Maximize : L_{classification} - \sum_{i,j \in N} Q(i,\ j) \tag{5}$$

This combines the Devicesive of optimizing service availability assessment and minimizing the hop count in the network.

4.2 Relativity Strength Based Security Approach

Relativity Strength Based Security can be defined as,

$$S_i = \sum_{j \in D, j \neq i} Rij \tag{6}$$

The security state S_i for a device is determined by the cumulative strength of its relationships with other devices.

4.3 Q-learning for Efficient Device Navigation

Q-learning for Efficient Device Navigation represented as,

$$H_{ij}(t+\ 1)\ =\ (1-\eta)H_{ij}(t)\ + \eta\left(R_{ij} - \min_{k \in D, k \neq i} R_{ik}\right) \tag{7}$$

Q-learning updates the hop count based on the relationship strength, with η as the learning rate.

4.4 Decision Tree Classification for Service Availability Assessment

Decision Tree Classification for Service Availability Assessment for Service availability by,

$$A_i = DecisionTree(X_i) \tag{8}$$

A decision tree model is trained on features X_i of device i to predict its service availability.

4.5 Optimizing Hop Counts

Optimizing Hop Counts efficiency is calculated using,

$$Minimize \sum_{i \in D} \sum_{j \in D, j \neq i} R_{ij}\ H_{ij} \tag{9}$$

5. Proposed Relative Strength Security (RSS) Framework

Figure 2 shows the proposed framework. A structured procedural approach defines a security framework in the dynamic world of the SIoT where networked objects actively seek services. Beginning with device profiling, the distinct characteristics of each device are rigorously defined, spanning a varied range of 9 smart applications, 16 guaranteed services, and with the help of 10 SIoT relationships. This thorough characterization serves as the foundation for the following phases. The methodology begins with a complex service availability evaluation as service requests ripple through the SIoT environment. Beyond the immediate answering device, this examination probes the availability of the requested service not only from the responding device but also from connecting devices associated with it in an environment having the guaranteed service. This all-encompassing strategy promotes flexibility within the SIoT network. By incorporating Q-Learning, the framework dynamically traverses the network by using the strength of existing linkages and previous data. Through the ability for devices to customize their interactions depending on relationship dynamics and prior experiences, this adaptive navigation mechanism improves communication efficiency. In post-service availability evaluations, the framework introduces the Relativity Strength Approach, a perceptive system that categorizes connections as strong, medium, or weak based on their effect on service availability. This better classification allows for more targeted and responsive handling of the complex social fabric in the SIoT context.

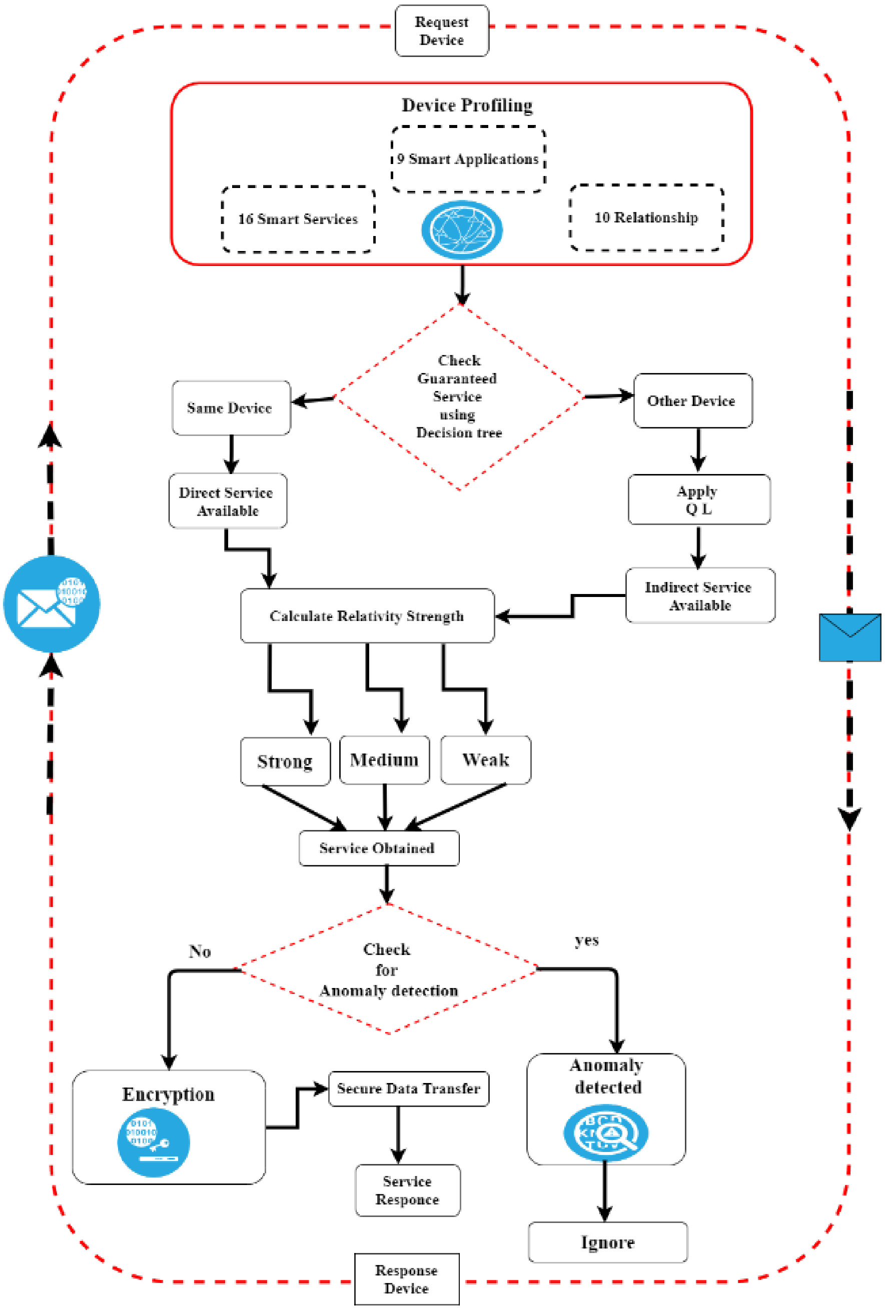


Fig. 2. SIoT Security Framework

The essential step in the procedure is anomaly detection, in which service requests are carefully examined for anomalies or possible security risks. By preventing unauthorized requests, this preventive action strengthens the SIoT environment's defenses against attacks.

The final step employs sophisticated encryption techniques, with the classified relationship strengths acting as encryption using Relationship as keys. This protects the transfer of service data, reducing the possibility of unauthorized access or manipulation during communication. The framework's proactive approach in the face of recognized abnormalities is a remarkable feature. The discovered abnormality is ignored, any security concerns are mitigated, and the integrity and dependability of the SIoT network are preserved. In essence, this Security Framework for SIoT emerges as a dynamic and adaptive strategy, fusing device profiling, service availability assessment, reinforcement learning, relationship strength categorization, anomaly detection, and encryption into a strong defense against the multifaceted security challenges of the Social Internet of Things. Recognizing a potential vulnerability in existing SIoT data, the model aims to secure device-generated data by emphasizing encryption and decryption based on object relationships, utilizing a 256-bit AES algorithm with keys generated through a transposition method reversing relationship types. The model successfully addresses SIoT data security concerns, as evidenced by its implementation and testing on an SIoT dataset, affirming the security of encrypted and decrypted data.

6. Algorithm

Algorithm 1 shows the proposed algorithm. The algorithm for the Security Framework for the Social Internet of Things (SIoT) begins by initializing the set of devices, relationship strength matrix, and relevant security parameters. Subsequently, it computes the security states based on the relativity of relationships and employs Q-learning to adaptively optimize device navigation by adjusting hop counts. Further, a decision tree model is trained to predict service availabilities for each device. The algorithm concludes by optimizing hop counts to minimize the cumulative product of relationship strengths and hop counts. The entire process is encapsulated within a main algorithm that sequentially executes the initialization, security modeling, navigation optimization, service availability prediction, and hop count optimization procedures.

Algorithm 1 Security Framework for SIoT

```
procedure INITIALIZE
    Initialize set of devices D
    Initialize relationship strength matrix R
    Initialize security states $S_i$, hop counts $H_{ij}$ , and service availabilities $A_i$
end procedure
procedure RELATIVITY-BASED SECURITY MODEL
    for i ∈ D do
        $S_i = \sum_{j \in D, j \neq i} Rij$
    end for
end procedure
procedure Q-LEARNING FOR DEVICE NAVIGATION
    Set learning rate $\eta$
    for $t \leftarrow 1$ to $T$ do
        for i, j ∈ D, i ≠ j do
            $H_{ij}(t+1) = (1-\eta)H_{ij}(t) + \eta\left(R_{ij} - \min_{k \in D, k \neq i} R_{ik}\right)$
        end for
    end for
end procedure
procedure DECISION TREE FOR SERVICE AVAILABILITY
    for i ∈ D do
        Train decision tree model on features $X_i$ to predict $A_i$
    end for
end procedure
procedure OPTIMIZE HOP COUNTS
    $Minimize \sum_{i \in D} \sum_{j \in D, j \neq i} R_{ij} H_{ij}$
end procedure
procedure MAIN ALGORITHM
    INITIALIZE
```

```
RELATIVITY-BASED SECURITY MODEL
Q-LEARNING FOR DEVICE NAVIGATION
DECISION TREE FOR SERVICE AVAILABILITY
OPTIMIZE HOP COUNTS
end procedure
```

7. Result and Discussion

Relationships between devices are established based on the data assigned during the profiling phase. There are ten different types of relationships, such as. On the basis of their trustworthiness, these connections are divided into a further 3 classifications as follows, before forming a relationship with a Devices, a number of criteria must be considered. Establishing trust between the devices is the fundamental difficulty in a secure simulator, and this is done by taking into consideration factors like transitivity and composability.

7.1 Simulation Environment and user-defined parameters

The environment outlined requires the following components: Python, a high-level programming language for simplicity and rapid prototyping; PyQt5 for building graphical user interfaces; Scikit-learn, a robust AI library; Pandas for data analysis and manipulation; NumPy for array operations. The system should run on Windows 7 or later, MacOS, with an Intel Core i5 processor and a minimum of 4GB of RAM.

Table 3. Relationship Categories and Strength Values

Relationship	Category	Strength
Owner Object Relationship	Strong	1.0
Social Object Relationship	Strong	0.9
Guest Object Relationship	Strong	0.8
Sibling Object Relationship	Medium	0.7
Guardian Object Relationship	Medium	0.7
Parent Object Relationship	Medium	0.6
Service Object Relationship	Medium	0.6
Co-Location Object Relationship	Medium	0.5
Co-Work Object Relationship	Weak	0.4
Stranger Object Relationship	Weak	0.3

7.2 Data set

7.2.1 Devices Profiling dataset details

When the user chooses devices, their profiling details are saved in daily-created relationship files. These files encompass information such as Device ID, Device brand, Device owner, Device location, and more. Connections are formed among these devices, and corresponding details are recorded.

Table 4. Devices Profiling

NAME	DESCRIPTION
Devices ID	Unique number to identify devices
Devices Types	Shows type of Devices
Devices Brand	Depicts Devices brand
Devices Location	Depicts devices X and Y location
Mobility	Shows as Mobile or Static
Owner ID	Shows the owner of the Devices
Service	Depicts the type of service offered by Devices

It includes information on the profiles of the items introduced to the simulation environment. Each Devices added to the environment is uniquely identified with an alphanumeric ID called Devices ID; the type of Devices added also becomes a necessary parameter when determining the relationship between the devices; the Devices brand is also configured along with its owner ID; and the mobility of the Devices is classified as" static" or" mobile" based on its type.

7.2.2 Relationship dataset details

Includes information on the dataset created during the simulation environment's development of relationships between trustworthy items. A connection must be formed between a minimum of two items, so the alphanumeric IDs of those two devices are recorded together with their positions, as establishing a relationship also requires consideration of distance. Relationship is a derived feature that is established by taking into account several characteristics of the profile information, including owner ID, item type, Devices brand, location, and so forth.

Table 5. Devices Relationship Information

NAME	DESCRIPTION
Devices1 ID	Identifies one of the 2 devices in relation
Devices2 ID	Identifies one of the 2 devices in relation
Devices1 Location	Depicts devices X and Y location of the first Devices
Devices2 Location	Depicts devices X and Y location of the second Devices
Relationship	Depicts the relationship between the devices

Table 6. Attacker Identification Information

NAME	DESCRIPTION
Device ID 1	Unique number to identify one of the 2 devices
Device ID 2	Unique number to identify one of the 2 devices
Device Type 1	Depicts the type of Devices 1
Device Type 2	Depicts the type of Devices 2
Device Brand 1	Depicts the brand of Devices 1
Device Brand 2	Depicts the brand of Devices 2
Device Owner 1	Shows the owner of Devices 1
Device Owner 2	Shows the owner of Devices 2
Relationship	Depicts the relationship between 2 devices
Relativity	Depicts the service availability strength between 2 devices
Anonymity	Depicts the service unavailability between 2 devices
Attack	Output feature

Table 7. Data Transfer Identification Information

NAME	DESCRIPTION
Source Device	ID of the source Devices
Destination Device	ID of the destination Devices
Relationship Count Type 1	Counts type1 relationships in the path
Relationship Count Type 2	Counts type2 relationships in the path
Output Relationship Category	Determines the output relation class

7.2.3 Attacker identification dataset

Provides the characteristics required to recognize a device as an attacker before initiating contact with it. Before creating an association with an item, its trustworthiness is tested as soon as it is introduced. The categorization of the newer item as an attacker or a regular Device is done depending on the sort of relationship it anticipates, and the transitivity and composability trust criteria are also examined. Here, the attacker uses ANN to build the output feature from the dataset.

7.2.4 Data Transfer Relation identification dataset

The shortest path between the two desired items is first determined, and then it is determined whether there is a direct link between the devices before data is sent between the trusted devices. If a direct link exists between the items, the encryption process is started using "relationship" as the key; otherwise, the relationship between the two devices is established using a decision tree classifier. Based on the number of relationships between the items included in the shortest path to the goal, the classifier will deliver the output in the form of 0 or 1, indicating to which class the determined relationship belongs.

7.3 Model Evaluation

1. ***Security Effectiveness**:* Security Effectiveness measures the effectiveness of systems and measures in protecting against unauthorized access and responding to potential threats, including prevention, detection, response, adaptability, and compliance.

Security effectiveness is evaluated using a Security Score, which is derived using a set of security metrics. The method used for measuring the Security Score is as follows:

$$Security\ Score = \frac{1}{N}\sum_{i=1}^{N} Security\ Metric_i \tag{10}$$

$$Overall\ Security\ Effectiveness = Security\ Score \tag{11}$$

Here, N represents the total number of security metrics considered, and Security Metric is considered as i. Each security metric is shown in figure 3. The obtained security score is then used to calculate the total security effectiveness. This approaches the aggregate effect of multiple security parameters on overall security performance. A higher security score indicates more effective security, demonstrating the effectiveness of the deployed security measures across a variety of metrics.

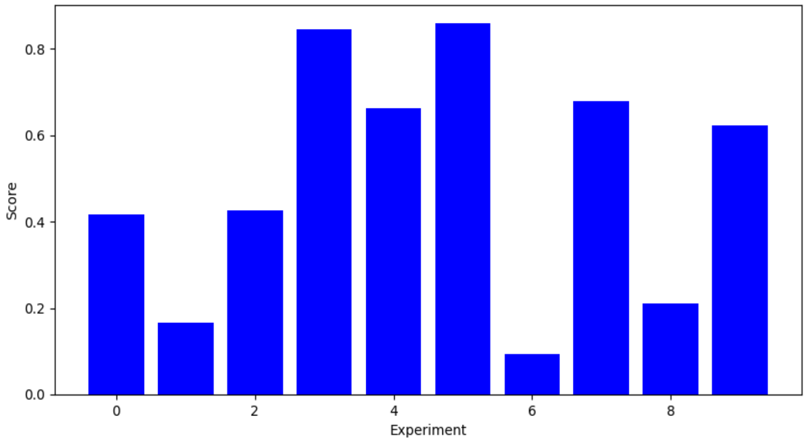


Fig. 3. Security Effectiveness.

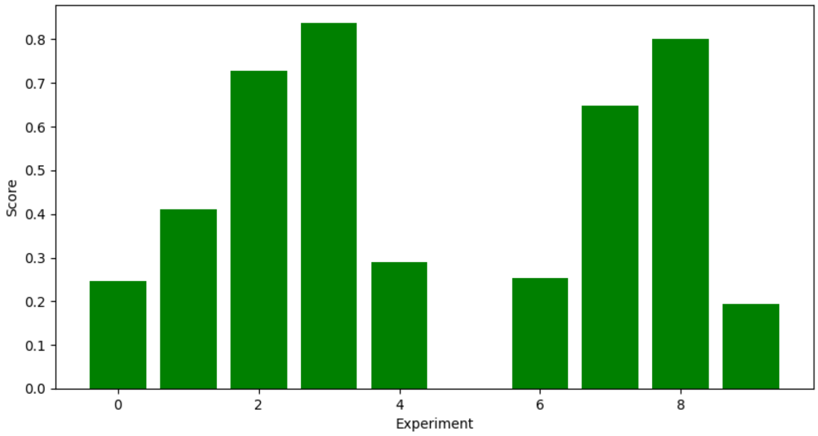


Fig. 4. Communication Efficiency

2. ***Communication Efficiency**:* Communication efficiency evaluates the efficiency of information transmission and reception within a system, aiming to minimize delays and errors for optimal information exchange. To calculate the communication score and overall communication efficiency, the system's performance is evaluated across various communication metrics. The average of every communication measure for each of the N metrics that are being considered has to be ascertained. The resulting figure, referred to as the Communication Score, represents the overall efficacy of the system's communication and is as shown in figure.

$$\textit{Communication Score} = \frac{1}{N}\sum_{i=1}^{N}\textit{Communication Metric}_i \tag{12}$$

$$\textit{Overall Communication Efficiency} = \textit{Communication Score} \tag{13}$$

A higher score denotes superior communication efficiency across the wide range of indicators taken into consideration. As a consequence, the communication score and the overall communication efficiency are in line.

3. ***Service Availability:*** The capacity to access and utilize a service in a smart environment without any interruptions is known as service availability. High availability improves system dependability and the user experience by guaranteeing that users may access and utilize the service when needed.

To guarantee service availability, tactics like monitoring, maintenance, and redundancy are used. Availability is frequently stated as a percentage is as shown in the figure 5.

$$\text{Availability Score} = \frac{1}{N}\sum_{i=1}^{N}\text{Availability Metric}_i \tag{14}$$

$$\textit{Overall Service Availability} = \textit{Availability Score} \tag{15}$$

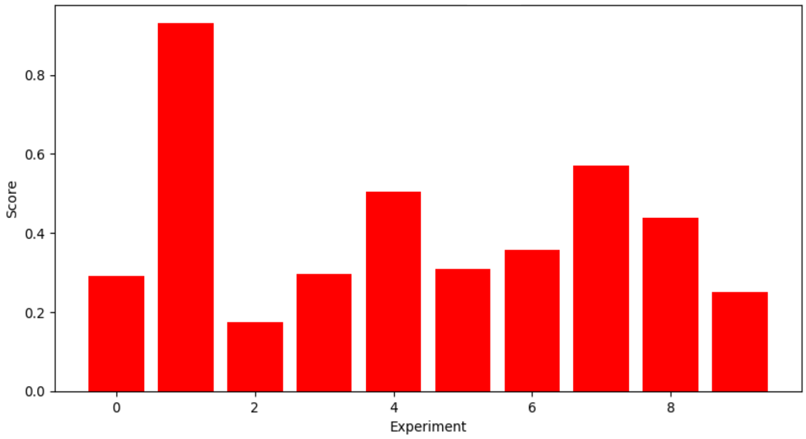


Fig. 5. Service Availability.

a) Result Analysis

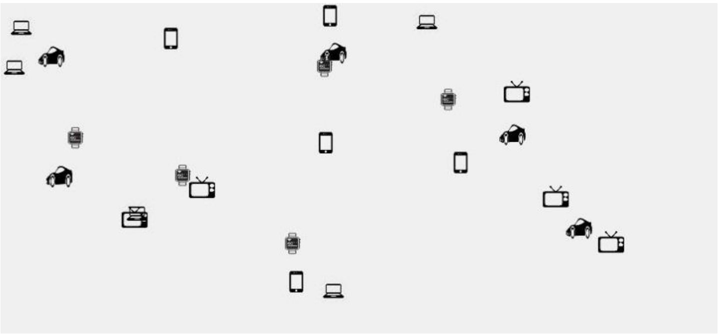


Fig. 6. Number Device in a smart environment application

The number of devices in a smart environment is represented in figure 6, which is based on the 9 smart applications available. The development of gadgets like cars, laptops, smartwatches, mobile devices, and smart TVs is notably facilitated by the smart environment. The dynamic movement of devices as they interact to create an environment.

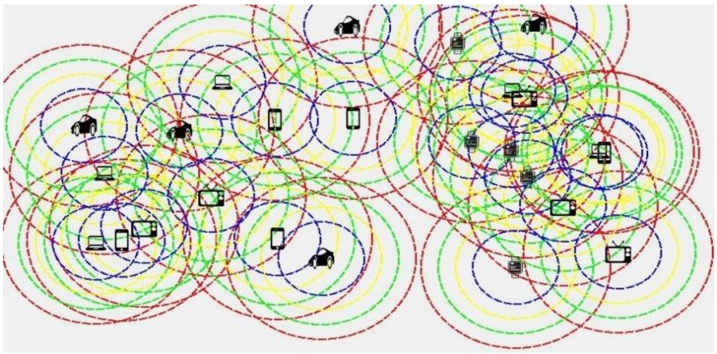


Fig. 7. Devices are establishing the relationship by searching

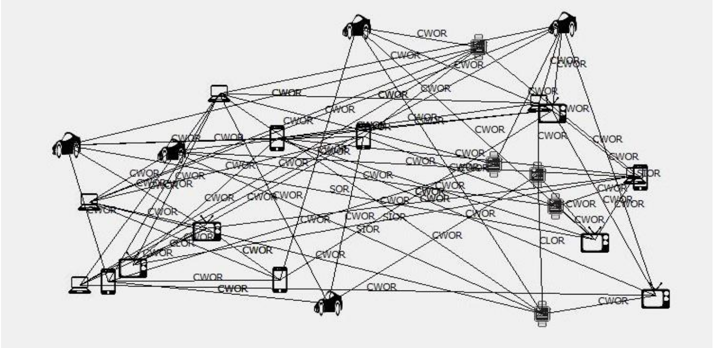


Fig. 8. Devices are Establishing Connection with the Previous Relationship

In the ever-changing world of technological growth, as represented in Figure 7, gadgets actively adapt, applying analytics to find and establish prospective equivalents. This dynamic procedure shows the agility required to create optimal cooperation for increased performance and service in the Social Internet of Things (SIoT) through the formation of 10 relationships and proactive searching. Figure 8 shows devices actively connecting with previous relationships.

This continual process demonstrates device flexibility and continuity, emphasizing the necessity of maintaining and expanding on established relationships for long-term connectivity and performance.

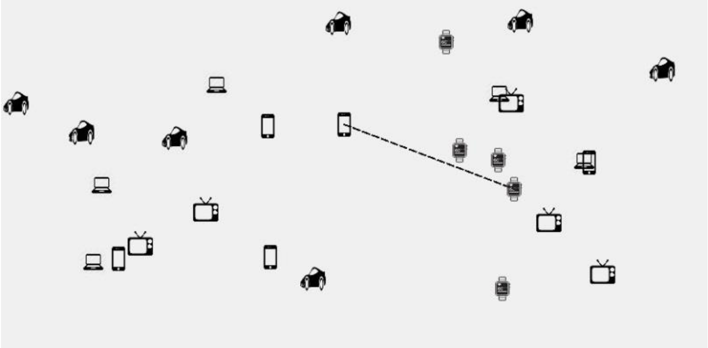


Fig. 9. Established new connection from Service available device using Direct approach

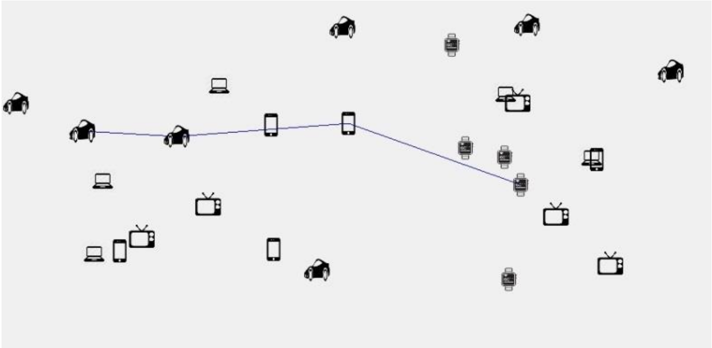


Fig. 10. Established new connection from Service available device using Indirect Approach

Figure 9 depicts the formation of a new connection from a service-available device utilizing a direct approach. This graphic depiction emphasizes the process within the proposed security architecture, highlighting the importance of direct connections in improving service availability and the general resilience of the Social Internet of Things.

An alternate method for creating a new connection from a device having services accessible is shown in Figure10. In the context of the Social Internet of Things, this figure highlights an important feature of the suggested security framework: the need for indirect connections to optimize service availability.

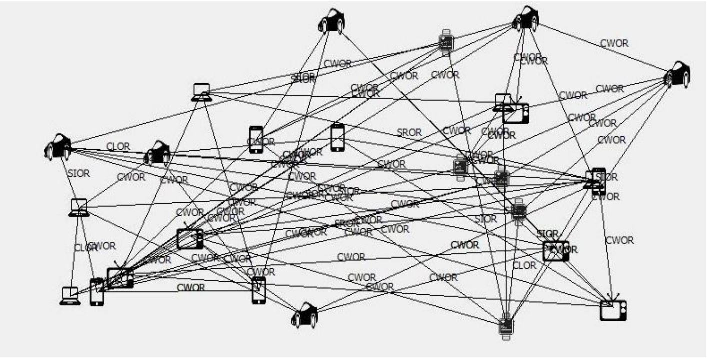


Fig. 11. Devices are Established connection with the new grouped relationship

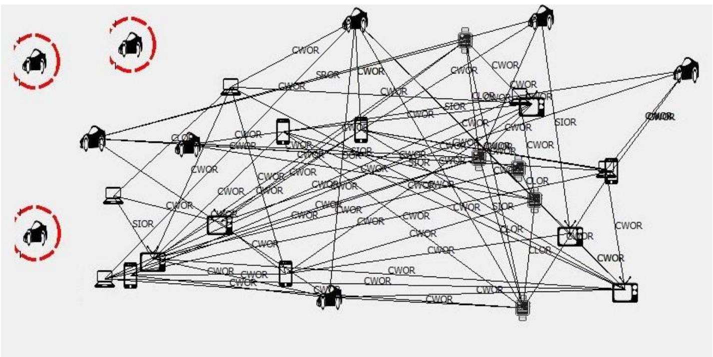
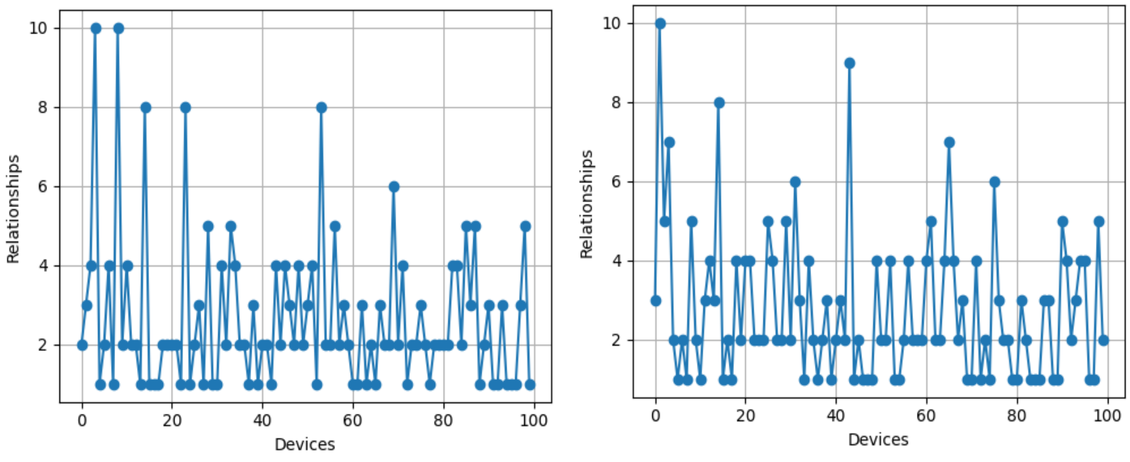


Fig. 12. Devices with the relationship and Intruder devices in an environment

Devices connecting inside a newly created grouped relationship are shown in Figure11 This graphic representation highlights the flexibility and dynamic character of device connections in the Social Internet of Things (SIoT) and represents a turning point in the proposed security framework. The formation of links inside this cluster relationship enhances the linked environment's security and communication effectiveness. An essential tool for addressing security concerns is the Security Framework for the Social Internet of Things (SIoT), as seen in Figure12. Through the detection and prevention of possible risks as well as the facilitation of meaningful interactions between devices, the framework is aimed at protecting the reliability and security of the connected smart environment.



(a)

(b)

Fig. 13 (a). Hop Count Calculation in Reinforcement Learning-Based Network Exploration for Efficient Service Provisioning in SIoT Environment. (b) Link count Calculation in Reinforcement Learning-Based Network Exploration for Efficient Service Provisioning in SIoT Environment.

Figure 13(a) (b) show how insights from the reinforcement learning algorithm are used to determine relationship links and hop counts among devices requesting services. This improves simple system investigation for effective service delivery in SIoT environments. The Relativity Strength Approach is used to form strategic partnerships in the Social.

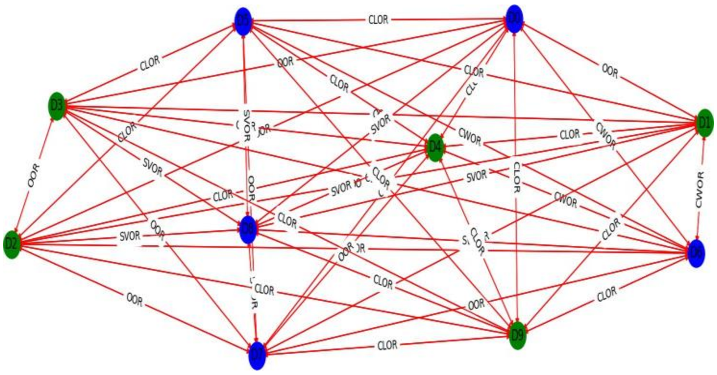
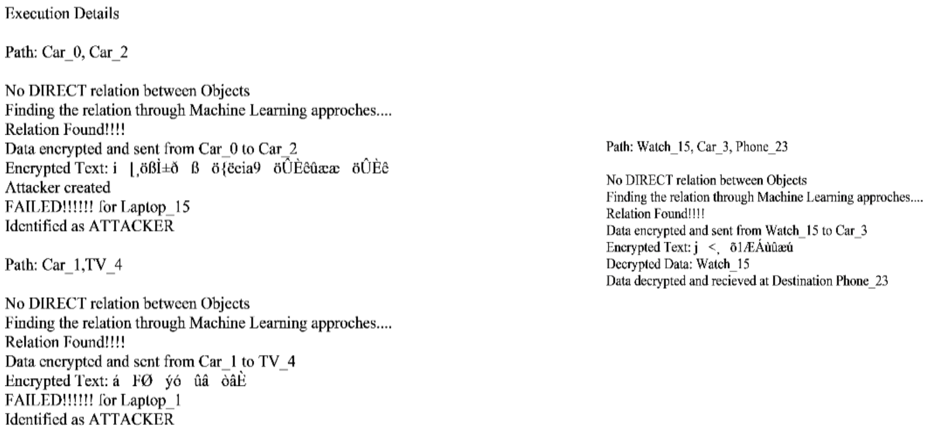


Fig. 14. SIoT environment with the new are relationship established for service availability between a device with Relativity Strength Approach.

Internet of Things (SIoT) environment, hence improving network robustness and security. This proactive method provides effective communication and consistent service availability while dealing with security risks and device heterogeneity. This proactive strategy helps to make the SIoT architecture more durable and efficient as shown in figure 14.

To establish a smart environment, a variety of smart devices, including cars, TVs, computers, watches, and smartphones, were created. Two distinct paths were uncovered, one leading from Car 0 to Car 1, and the other from Car 0 to Car 2. Despite the absence of direct relationships between the devices, the system ūtilizes māchine learning techniques to identify connections. An important discovery was made when data, as described in [27], was encrypted and transmitted from Car 0 to Car 2, resulting in the exposure of the encrypted text for that service. This revelation led to the identification of an attacker during the operational phase of the service.

Another investigative path was pursued, extending from Car 1 to TV 4, without a direct connection between the objects. Using machine learning approaches, a relationship was dīscerned, allowing access to the encrypted data of the service from Car 1 to TV 4. The service availability checks for Laptop 15 once again failed, leading to its identification as an attacker or anomaly, as illustrated in Figure 16. Despite the lack of a direct link, the system found a considerable route from Watch 15 to Car 3 and Phone 23. Data encryption and transmission were prompted by the important as- sociation that machine learning techniques showed. After reaching Phone 23, the encrypted data is decoded, exposing Watch 15 as the original data source. This shows how the system can understand relationships and maintain secure communication in a smart environment.



```
Execution Details

Path: Car_0, Car_2

No DIRECT relation between Objects
Finding the relation through Machine Learning approches....
Relation Found!!!!
Data encrypted and sent from Car_0 to Car_2
Encrypted Text: i   ˌ,ößİ±ð   ß   ö{ëcia9   öÛÈêûææ   öÛÈê
Attacker created
FAILED!!!!!! for Laptop_15
Identified as ATTACKER

Path: Car_1,TV_4

No DIRECT relation between Objects
Finding the relation through Machine Learning approches....
Relation Found!!!!
Data encrypted and sent from Car_1 to TV_4
Encrypted Text: á   FØ   ýó   ûâ   òâÈ
FAILED!!!!!! for Laptop_1
Identified as ATTACKER
```

```
Path: Watch_15, Car_3, Phone_23

No DIRECT relation between Objects
Finding the relation through Machine Learning approches....
Relation Found!!!!
Data encrypted and sent from Watch_15 to Car_3
Encrypted Text: j   <,   ð1ÆÁùûæú
Decrypted Data: Watch_15
Data decrypted and recieved at Destination Phone_23
```

Fig. 15. Data Encryption and Decryption for Available Guaranteed Service between request device and responded device.

8. Conclusions

This study addresses the pressing security challenges within the evolving Social Internet of Things (SIoT) landscape. By integrating social networking into smart devices, our Security Framework effectively enhances security and reliability. The emphasis on mitigating disruptions caused by malicious messages, optimizing resource utilization, and improving service reliability underscores the framework's significance in fostering trustworthy collaborations among IoT devices. The results demonstrate the framework's success in achieving its objectives. Through the application of a relativity-based security model, Q-learning for navigation, and decision tree classification for service availability, the SIoT experiences improved security measures and optimized resource usage. The consideration of relationship strength and optimizing hop counts contribute to the framework's unique approach, addressing the intricate challenges social networks pose in the SIoT environment. The framework is designed for real-world social IoT settings, focusing on security needs in SIoT environments. It uses a" Relationship key" based on device relationships, which is used in conjunction with the standard 256-bit Advanced Encryption Normal (AES) method for encryption and decryption. This approach ensures secrecy and service when accessing networks while protecting data during transfer. The system exhibits robust performance across multiple metrics, demonstrating an Overall Security Effectiveness of 88.75%, reflecting its efficiency in safeguarding against unauthorized access and responding to potential threats. Additionally, the system showcases a high Overall Communication Efficiency of 91.75%, emphasizing its effectiveness in minimizing delays and errors for optimal information exchange within the smart environment. Moreover, it achieves an impressive Overall Service Availability of 97.5%, ensuring uninterrupted access to and utilization of services, thereby enhancing system dependability and user experience. Together, these results underscore the system's capability to deliver secure, efficient, and highly available smart services.

References

[1] Chen, I.-R., Bao, F., & Guo, J. (2016). Trust-Based Service Management for Social Internet of Things Systems. *IEEE Transactions on Dependable and Secure Computing*, 13(6), 684-696. https://doi.org/10.1109/TDSC.2015.2420552.

[2] Jadhav, B. & Patil, S. C. (2016). Wireless Home monitoring using Social Internet of Things (SIoT). In *International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)*, Pune, India, 925-929. https://doi.org/10.1109/ICACDOT.2016.7877722.

[3] Han, G., Zhou, L., Wang, H., Zhang, W., & Chan, S. (2017). A source location protection protocol based on dynamic routing in WSNs for the Social Internet of Things. *Future Gener. Comput. Syst.*, 82, 689-697. https://doi.org/10.1016/j.future.2017.08.044.

[4] Ruggeri, G. & Briante, O. (2017). A framework for IoT and E-Health systems integration based on the social Internet of Things paradigm. In *International Symposium on Wireless Communication Systems (ISWCS)*, Bologna, Italy, 426- 431. https://doi.org/10.1109/ISWCS.2017.8108152.

[5] Roopa, M. S., Valla, D., Buyya, R., Venugopal, K. R., Iyengar, S. S., & Patnaik, L. M. (2018). SSSSS: Search for So- cial Similar Smart devices in SIoT. In *Fourteenth International Conference on Information Processing (ICINPRO)*, Bangalore, India, 1-6. https://doi.org/10.1109/ICINPRO43533.2018.9096686.

[6] Amin, F., Abbasi, R., Rehman, A., & Choi, G.S. (2019). An Advanced Algorithm for Higher Network Navigation in Social Internet of Things Using Small-World Networks. *Sensors (Basel, Switzerland)*, 19. https://doi.org/10.3390/s19092007.

[7] Bhavsar, S.A., Pandit, B.Y., & Modi, K.J. (2019). Social Internet of Things. In *Advances in Systems Analysis, Software Engineering, and High Performance Computing*. https://doi.org/10.4018/978-1-5225-7790-4.ch010.

[8] Patnaik, L.M., Venugopal, K.R., Iyengar, S.S., Buyya, R., & Roopam, S. (2020). DRCM: Dynamic Relationship Creation and Management in Social Internet of Things (SIoT). https://doi.org/10.1504/ijiitc.2020.10033966.

[9] Azad, M.A., Bag, S., Hao, F., & Shalaginov, A. (2020). Decentralized Self-Enforcing Trust Management System for Social Internet of Things. *IEEE Internet of Things Journal*, 7, 2690-2703. https://doi.org/10.1109/JIOT.2019.2962282.

[10] Wang, B., Sun, Y., Duong, T. Q., Nguyen, L. D., & Zhao, N. (2020). Popular Matching for Security-Enhanced Resource Allocation in Social Internet of Flying Things. *IEEE Transactions on Communications*, 68(8), 5087-5101. https://doi.org/10.1109/TCOMM.2020.2995223.

[11] Kalyani, G. & Shilpa Shashikant Chaudhari (2020). An efficient approach for enhancing security in Internet of Things using the optimum authentication key. *International Journal of Computers and Applications*, 42, 306-314. https://doi.org/10.1080/1206212X.2019.1619277.

[12] Mawgoud, A.A., Taha, M.H.N., & Khalifa, N.E.M. (2020). Security Threats of Social Internet of Things in the Higher Education Environment. In *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications. Studies in Computational Intelligence*, vol 846, Springer, Cham. https://doi.org/10.1007/978-3-030-24513-9_9.

[13] Rehman, A., Paul, A., Rehman, A. U., Amin, F., Asif, R. M., & Rahmatov, N. (2020). An Efficient Friendship Selection Mechanism for an Individual's Small World in Social Internet of Things. In *International Conference on Engineering and Emerging Technologies (ICEET)*, Lahore, Pakistan, 1-6. https://doi.org/10.1109/ICEET48479.2020.9048234.

[14] Malekshahi Rad, M., Rahmani, A.M., Sahafi, A. et al. Social Internet of Things: vision, challenges, and trends. Hum. Cent. Comput. Inf. Sci. 10, 52 (2020). https://doi.org/10.1186/s13673-020-00254-6

[15] Krishna, M. Bala & Lorenz, P. (2021). Location, Context, and Social Devicesives Using Knowledge-Based Rules and Conflict Resolution for Security in Internet of Things. *IEEE Internet of Things Journal*, 8(1), 407-417. https://doi.org/10.1109/JIOT.2020.3008771.

[16] Farhadi, B., Rahmani, A.M., Asghari, P., & Hosseinzadeh, M. (2021). Friendship selection and management in social internet of things: A systematic review. *Comput. Networks*, 201, 108568. https://doi.org/10.1016/j.comnet.2021.108568.

[17] Jose ́Ramo ́n Saura, Domingo Ribeiro-Soriano, Daniel Palacios-Marque ́s, Setting Privacy "by Default" in Social IoT: Theorizing the Challenges and Directions in Big Data Research, Big Data Research, Volume 25,2021,100245, ISSN 2214-5796. https://doi.org/10.1016/j.bdr.2021.100245.

[18] Hussain, T., Yang, B., Rahman, H.U., Iqbal, A., Ali, F., & Shah, B. (2022). Improving Source location privacy in social Internet of Things using a hybrid phantom routing technique. *Comput. Secur.*, 123, 102917. https://doi.org/10.1016/j.cose.2022.102917.

[19] Abdelghani, W., Amous, I., Zayani, C.A. et al. (2022). Dynamic and scalable multi-level trust management model for Social Internet of Things. *J Supercomput*, 78, 8137–8193. https://doi.org/10.1007/s11227-021-04205-5.

[20] Sagar, S., Mahmood, A., Sheng, Q.Z., Pabani, J.K., & Zhang, W. (2022). Understanding the Trustworthiness Management in the Social Internet of Things: A Survey. *ArXiv*, abs/2202.03624.

[21] Dhillon, P., & Singh, M. (2022). An ontology-oriented service framework for social IoT. *Comput. Secur.*, 122, 102895. https://doi.org/10.1016/j.cose.2022.102895.

[22] Vaibhava Lakshmi, R., Deepak, G., Santhanavijayan, A., & Radha, S. (2022). Search for Social Smart devices Constituting Sensor Ontology, Social IoT and Social Network Interaction. *Sixth International Conference on I- SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 60-65. https://doi.org/10.1109/I-SMAC55078.2022.9987249.

[23] Wu, B., Zhong, L., Yao, L., & Ye, Y. (2022). EAGCN: An Efficient Adaptive Graph Convolutional Network for Item Recommendation in Social Internet of Things. *IEEE Internet of Things Journal*, 9(17), 16386-16401.https://doi.org/10.1109/JIOT.2022.3151400.

[24] Maniveena & Kalaiselvi (2023). Social IoT Security and Privacy. In *Advanced Computing and Communication Technologies for High Performance Applications (ACCTHPA)*, Ernakulam, India, 1-7. https://doi.org/10.1109/ACCTHPA57160.2023.10083356.

[25] Mohan Das, R., Arun Kumar, U., Gopinath, S. et al. (2023). A novel deep learning-based approach for detecting attacks in social IoT. *Soft Comput*.https://doi.org/10.1007/s00500-023-08389-1.

[26] Mustafa, R. U., McGibney, A., & Rea, S. (2023). Trust Analysis to Identify Malicious Nodes in the Social Internet of Things. In *International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, 1-9. https://doi.org/10.1016/j.knosys.2021.107479.

[27] Santhosh Kumar, K.S., Hanumanthappa, J., Shiva Prakash, S.P., Krinkin, K. (2023). Relationship-Based AES Security Model for Social Internet of Things. In: Kulkarni, A.J., Mirjalili, S., Udgata, S.K. (eds) Intelligent Systems and Applications. Lecture Notes in Electrical Engineering, vol 959. Springer, Singapore. https://doi.org/10.1007/978-981-19-6581-4_12

[28] Akli, A., Chougdali, K. (2023). IoT Trust Management as an SIoT Enabler Overcoming Security Issues. In: Abd El-Latif, A.A., Maleh, Y., Mazurczyk, W., ELAffendi, M., I. Alkanhal, M. (eds) Advances in Cybersecurity, Cyber- crimes, and Smart Emerging Technologies. CCSET 2022. Engineering Cyber-Physical Systems and Critical Infrastructures, vol 4. Springer, Cham.https://doi.org/10.1007/978-3-031-21101-0_10.

[29] Meriem Chiraz Zouzou, Mohamed Shahawy, Elhadj Benkhelifa and Hisham Kholidy, (2023). SIoTSim: Simulator for Social Internet of Things. 10th International Conference on Internet of Things: Systems, Management and Security (IOTSMS). 149-155. https://doi.org/10.1109/IOTSMS59855.2023.10325812.

Authors' Profiles

K. S. Santhosh Kumar, presently a Research Scholar actively pursuing a Ph.D. in Computer Science and Application within the Department of Studies in Computer Science at the Manasagangothri campus of the University of Mysore, Mysuru and achieved an M. Tech. in Software Engineering from the Department of Information Science and Engineering at Sri Jayachamarajendra College of Engineering, Mysuru, Karnataka, India, in 2016. Demonstrating an impressive publication record, he has filed three Indian patent requests and authored more than 5 research papers, all of which have been accepted and published in peer-reviewed national and international journals and conferences.

Hanumanthappa J. is currently serves as a Professor in the Department of Studies in Computer Science at the Manasagangothri campus of the University of Mysore, situated in Mysuru, India. He completed his Ph.D. in Computer Science at Mangalore University, Mangalore, Karnataka, India, in 2014. His extensive research encompasses various fields, and he has authored and co-authored more than 50 papers, making significant contributions to both national and international journals and conferences. In addition to his academic accomplishments, he actively engages in collaborative research projects and has fostered a dynamic environment for intellectual exchange within the department includes the biography here.

S. P. Shiva Prakash is currently a Professor within the Department of Information Science and Engineering at JSS Science and Technology University (formerly known as Sri Jayachamarajendra College of Engineering) in Mysuru, Karnataka, India. He earned his Ph.D. in Computer Science, focusing on Wireless Mesh Networks in 2017 from the University of Mysore in Mysuru, Karnataka, India. He completed post-doctoral research at the Department of Software Engineering and Computer Applications at Saint Petersburg Electrotechnical University" LETI" in Saint Petersburg, Russia. Dr. S.P. Shiva Prakash boasts an impressive track record, having filed three Indian patents and authored over 35 research papers published in peer-reviewed national and international conferences and journals.

Kirill Krinkin is currently serving as a researcher at JetBrains Research and holds an academic position as Adjunct Professor at Constructor University in Germany. He is also giving lectures at Neapolis University Pafos in Cyprus. He earned his Ph.D. in Computer Science and has dedicated over two decades to research and development in various fields including Software Engineering, Operating Systems, Computer Networks, Autonomous Mobile Robots, and Co-evolutionary Intelligence Engineering. Dr. Krinkin authored or co-authored over 100 technical papers. He is also a lecturer in Mobile Robotics at various universities. Since 2012, he has organized the Joint Advanced Student School (JASS), an annual international project-driven initiative focusing on emerging technologies. Under his mentorship, student teams have twice won the Artificial Intelligence Driving Olympics Challenge (AIDO) at the ICRA and NeurIPS conferences.

How to cite this paper: K. S. Santhosh Kumar, Hanumanthappa J., S. P. Shiva Prakash, Kirill Krinkin, "Security Framework for Social Internet of Things: A Relativity Strength Approach", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.16, No.4, pp. 28-46, 2024. DOI:10.5815/ijieeb.2024.04.03