OSSIoT: An ontology-based Operational Security model for Social Internet of Things using Machine Learning Techniques

K S Santhosh Kumar, *IAENG, Member*, Hanumanthappa J, S P Shiva Prakash, *IAENG, Member* and Kirill Krinkin

***Abstract*—The Social Internet of Things (SIoT) is an innovative fusion of IoT and smart devices that enable them to establish dynamic relationships. Securing sensitive data in a smart environment requires a model to determine the relationships between devices through object profiling and ontological models. To address this need, we have proposed an ontology-based operational security model for the SIoT. In our approach, the interpolation method is used to establish relationships, while fiduciary relationships are employed to detect threats. Furthermore, the encryption of heterogeneous device data, coupled with the implementation of an operation-based intrusion detection system, proves highly effective in identifying potential threats.Invalid relationships are identified as intruders and validated using machine learning techniques. Encrypting heterogeneous device data, along with an operation-based intrusion detection system, efficiently identifies threats in the ever-evolving dynamic nature of the SIoT environment. the encryption of heterogeneous device data, coupled with an operation-based intrusion detection system, effectively identifies threats. Invalid relationships are promptly identified as attackers and machine learning techniques are used to validate relationships encryption and machine learning stand as indispensable tools in the endeavor to secure sensitive information within the realm of the SIoT. The suggested model outperformed the results of the current model, as evidenced by its average accuracy of 85.67%, precision of 90.37%, recall of 92.06%, and F1-score of 91.03% when compared to the existing model.**

***Index Terms*—Ontology, Operational Security, Social Internet of Things, LPI, ANN.**

I. Introduction

THE concept of the Social Internet of Things (SIoT) represents a ground-breaking advancement in technology, merging physical objects with information networks to provide humans with intelligent data services. Figure 1 depicts the SIoT architecture for the smart city application. Depending on the type of relationship, it consists of a variety of smart applications that connect with one another to provide services, such as Service Object Relationships (SVOR), to get connected socially as Social Object Relationships (SOR), both the gadgets used by the owner as Parent Object Relationships (POR), available devices in the same location as Co-Location Object Relationships (CLOR), devices that are used in the same working environment as Co-Work Object Relationships (CWOR), if the relationship device is connected to some other device as a guest for temporary communication, Guest Object Relationships (GSTOR), etc. They communicate with one another using object profiling and device protocols. The sample SIoT application of a smart city is shown in figure 2. It includes traffic, streetlights, weather status, waste status, cinemas, parking, crowds, and bus applications. These applications improve service availability within the SIoT environment. However, the SIoT also presents several challenges and issues. One of the primary challenges is the inherent heterogeneity within the IoT landscape. SIoT objects vary in terms of standards, communication protocols, and deployment features, making interoperability and seamless integration a complex task. The diverse nature of these objects poses obstacles to achieving seamless connectivity and information exchange. Another significant challenge is the discovery and identification of objects within the SIoT framework. Object discovery is a crucial process for establishing relationships and facilitating communication between various objects in an information network. Existing technologies employ various approaches to find the nearest object and connect objects. However, despite advancements in object discovery, there remains a risk of data manipulation and unauthorized access within the network. Making sure of the authenticity, confidentiality, integrity, and security of object data is a pressing concern. Furthermore, privacy and data protection issues arise in the SIoT environment. As smart objects collect and exchange vast amounts of data, ensuring the privacy of individuals becomes crucial. Safeguarding sensitive information and establishing robust data protection mechanisms are essential to maintaining user trust and confidence in the SIoT ecosystem. Thus, the integration of ontological methods and intrusion detection methods, utilizing machine learning, is effective for securing devices in a social network. Consequently, the key objective of the research is to establish an ontology-based operational security model (OSSIoT) for the Social Internet of Things. The following are the main contributions to this work:

- proposed a data-sensitive classifying approach that uses a neural network with a model called the Artificial Neural Network (ANN) method to classify the data as shareable or non-shareable.

Manuscript received October 9, 2023; revised May 27, 2024.

K S Santhosh Kumar is a Research Scholar in the Department of Studies in Computer Science, University of Mysore, Mysuru, Karnataka, India. (email: santhosh@compsci.unimysore.ac.in).

Hanumanthappa J is a Professor in the Department of Studies in Computer Science, University of Mysore, Mysuru, Karnataka, India. (email: hanums_j@yahoo.com).

S P Shiva Prakash is a Professor in the Department of Information Science and Engineering, JSS Science and Technology University, Mysuru, Karnataka, India. (email: shivasp@jssstuniv.in).

Kirill Krinkin is an Adjunct Professor in the School of Computer Science and Engineering, Constructor University, Bremen, Germany. (email: kirill@krinkin.com).

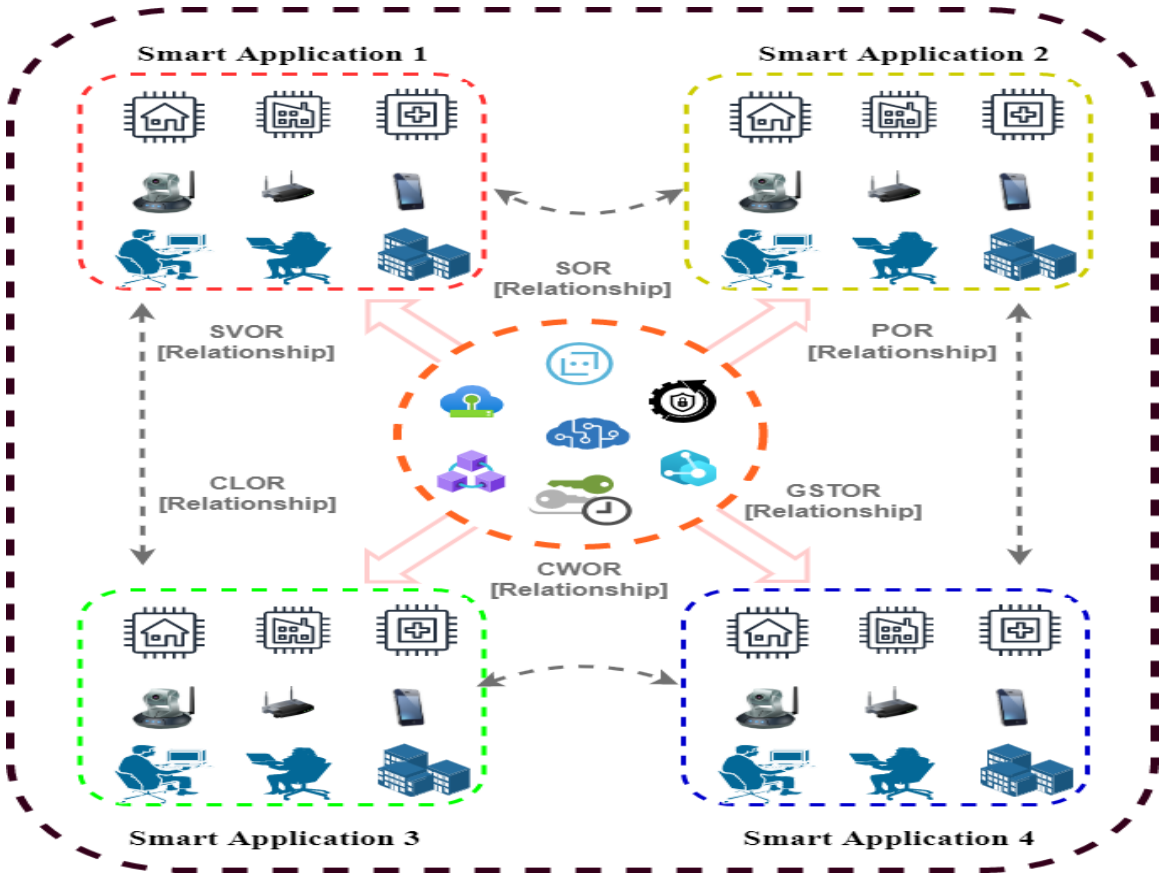

Fig. 1. An SIoT Architecture for a Smart City

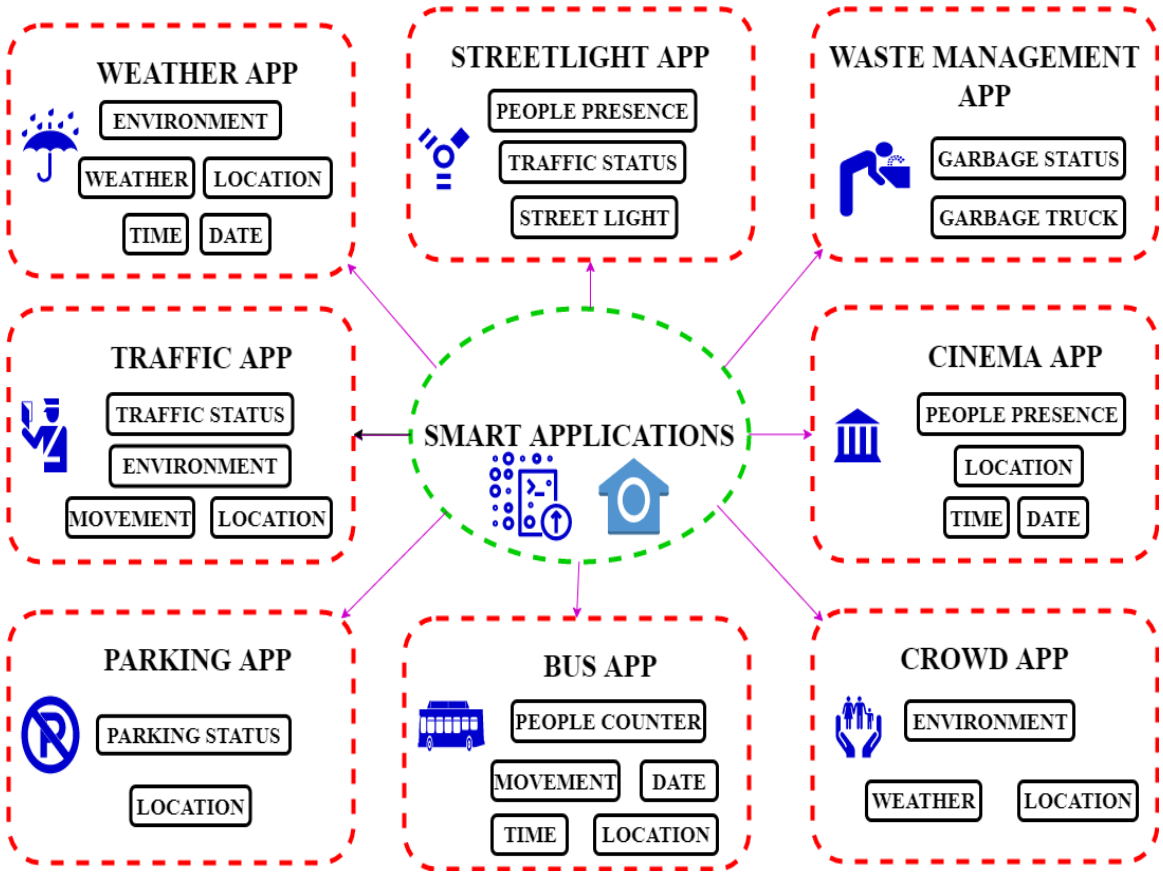

Fig. 2. Sample SIoT smart city application

- Identified intruders by using the Lagrange polynomial interpolation (LPI) method.
- The proposed Advanced Encryption Standard (AES-512) encryption technique encrypts the data before sharing it with other devices, ensuring the security of the SIoT.

The rest of the work is split into the following sections in a paper: Section 2 looks at relevant works; Section 3 outlines the issue statement; and Section 4 defines the research technique. Section 5 describes the proposed OSSIoT Framework; Section 6 suggests an OSSIoT algorithm; and Section 7 covers the results, conclusion, and next work in Section 8.

II. Related work

Security issues have been highlighted by the Social Internet of Things' diversification in the past decade. Data aggregation, intrusion detection, and other issues are covered by machine-learning-based solutions. Several studies on SIoT security are summarized. A compendium of studies in the realm of SIoT security offers profound insights into the evolving landscape. The Internet of Things, as the fundamental enabler of device-to-device communication presents an inherent array of security vulnerabilities, compounded by the absence of direct human input. In the context of SIoT, where social interactions and connectivity thrive, these security concerns become paramount. Notably, Fog computing has emerged as a scalable solution, providing a framework to address these challenges effectively. Melody Moh et al.[1], in their comprehensive research, navigate the intricate intersections of IoT, fog computing, and machine learning-based security measures. Fan Liang et al. [2] contribute significantly by shedding light on the evolutionary trajectory of IoT, emphasizing automation while delving into its associated vulnerabilities. It is worth noting that while machine learning augments these advancements, it simultaneously introduces new dimensions of vulnerability in the ever-evolving cyber threat landscape, a topic explored and further examined by Ikram Ud Din et al. [3]. In tandem with these developments, Iqbal H. Sarker et al [4]. delve into the profound impact of data science on cybersecurity, whereas Abuzar Qureshi et al.[5] explore the transformative potential of IoT and its symbiotic relationship with machine learning-based security solutions. Amit Sagu et al. [6] meticulously dissect the formidable challenges posed by IoT while spotlighting the pivotal role played by machine learning in ameliorating these concerns.Rasheed Ahmad et al. [8] presented thought-provoking inquiries into the realm of IoT security, prompting critical reflection. Umer Farooq et al. [9] survey the formidable challenges that underpin IoT security and illuminate the burgeoning landscape of machine learning-driven solutions. In a complementary vein, Iqbal H. Sarker et al. [10] proffer profound insights into the multifaceted impact of IoT on society, economy, and the pervasive security gaps that persist. Moreover, Syed Faisal Abbas Shah et al. [12] highlight the critical role that machine learning plays in the context of the Internet of Things and its easy integration into the world of smart buildings. The ever-evolving landscape of SIoT sees Mohana et al. [14] offering a complex Long Short Term Memory (LSTM) network that addresses changing dynamics in predictive modeling. Vinay Gugueoth et al. [15] lucidly articulate the imperative need for efficient models in the sphere of IoT security, concurrently exploring the transformative role played by machine learning. Yasir Ali et al. [16] undertake a meticulous review of Artificial Neural Networks (ANNs) and their far-reaching implications for bolstering IoT security. Taher M. Ghazal et al. [17] embark on a journey into the synergy between machine learning and IoT within the context of smart cities, unraveling profound insights. Nour Moustafa et al. [18] pivot towards the realm of Explainable Artificial Intelligence (XAI) and its pivotal role in the context of intrusion detection. Guowen Wu et al. [19] proposed a virus spread model specifically tailored for SIoT, paving the way for novel strategies in security. Shaozhong Zhang et al. [20] presented a trust and Quality of Service (QoS)-centric service recommendation model, significantly enhancing the reliability and functionality of SIoT. Subhash Sagar et al. [21] introduce the innovative Trust–SIoT framework, underpinned by neural networks, reshaping the foundations of trust within the SIoT ecosystem. Meanwhile, Huifen Wu et al. [22] champion an association rule-based approach for detecting network security attacks, further fortifying the SIoT security architecture. Mustafa et al. [23] advocate for trust-based friendship selection as a means to enhance navigability within SIoT, artfully merging the domains of social networking and IoT. Deng et al. [24] augment the efficiency of Message Searching and Routing (MSAR) within SIoT by leveraging social relationships and routing stages, resulting in improved latency and message delivery rates. In a concerted effort to address overarching IoT security concerns, Yadav et al. [25] proffer the innovative RSAEDSA model, effectively mitigating security and efficiency issues while outperforming traditional methods. In an era where the world increasingly embraces technology, connecting devices for seamless communication, the growing prevalence of IoT underscores the imperative of addressing its vulnerabilities. To exclude untrustworthy components by [26], an intelligent friend selection strategy that takes into account gadget quality, typology, and functionality is required. The SIoT represents a viable approach by [27], to trust management and buddy selection in device discovery and service search. However, limitations in storage capacity and battery life must be addressed to maximize device lifespan and durability. Artificial intelligence will be utilized to develop by [28] a simulation environment for the Social Internet of Things, enabling social connections between gadgets such as friendships and communities. Machine learning algorithms will detect anonymity, evaluate device vulnerability, and determine communication device relativity. Data will be sent securely by encrypting at the sender and decrypting at the recipient. The confluence of these studies and explorations collectively forms a robust tapestry of knowledge and innovation [29], illuminating the multifaceted landscape of SIoT security and the pivotal role that machine learning and other advanced technologies play in safeguarding this dynamic ecosystem. Table I presents the state-of-the-artwork that addresses the security issues in SIoT. From the state-of-the-art work, it is found that several researchers have proposed innovative methods to enhance the security of SIoT by leveraging machine learning techniques. These research investigations illustrate how machine learning is used in SIoT

TABLE I
STATE OF THE ART

Authors	Machine Learning	SIoT	Encryption	LPI
Fan Liang, et al. [2]	✓	✓	✓	×
Abuzar Qureshi et al.[5]	✓	✓	✓	×
Amit Sagu, et al. [7]	✓	×	✓	×
Santhosh Kumar K.S., et al.[13]	×	✓	✓	×

security and how it may improve network security and threat detection. However, the integration of ontology in These works remain limited, indicating a potential area for further exploration and development.

III. PROBLEM STATEMENT

The SIoT is a network of interconnected devices that exchange data. to provide users with valuable services. Fortunately, as the internet of things expands and it becomes more difficult to maintain reliable and secure communication between devices, the security of the SIoT network has become an important concern. Thus, there is a need to develop a model that enhances the security of the SIoT network by utilizing an ontology-based approach to systematically represent the system and identify data anomalies in a given set of information. The model aims to classify the sensitivity of the data using Artificial Neural Networks (ANN) to detect intruders using Lagrange polynomials. Interpolation, and encrypt data using the Advanced Encryption Standard (AES-512) if no intruder is found.

IV. RESEARCH METHOD

The proposed ontology-based security model addresses the challenges of device heterogeneity, data privacy, trust management, energy efficiency, and scalability in the SIoT network. It makes use of standard designs, methods, and communications for ensuring security and dependability. Real-world SIoT data sets may be used to test and validate the proposed model and analyze the extent to which it enhances security and dependability.

A. Ontological Model

In a Smart Environment of the smart city is represented as a virtual object that comprises nine applications as composite virtual objects from the supplied data set. These applications offer corresponding services that form associations based on the relationship, constraints defined in the ontology.The selection of data from the available data set is the first step in the process for the suggested approach. Next, the selected data is analyzed to identify the relevant smart city components and their relationships. This analysis is based on the ontological model and its associated relationship constraints. Once the components and relationships are identified, appropriate security measures are selected and implemented based on the associated risk levels. These measures include data encryption, access control, and intrusion detection. Through an assortment of simulations and tests, the proposed security framework's efficiency is determined. The results demonstrate the ability of the framework to improve security risk analysis and protect smart city components from various security threats.

V. PROPOSED OSSIOT ALGORITHM

1) Data Validation Domain Ontology: A standardized illustration of the domain framework for smart cities, including applications and services, has been provided through the ontological model. This representation offers insight into the device data associated with each service. Virtual objects are objects that exist solely in a digital context, serving as substitutes for real-world objects. Composite virtual objects are created by combining these digital objects, reflecting the analytical structure of information relevant to virtual objects and contributing to achieving specific objectives. Microservices involve the development of composite virtual objects. each functioning independently within the composite object structure. These Microservices operate as individual processes, facilitating communication with the next object in the system. Sensor data is crucial in defining the data flow. required by specific microservices and plays a significant role in gathering external information. This data flow aids in establishing relationships among devices based on the existing data within the system.In the provided domain ontology, depicted in Figure 3, 4, 5, and 6 the smart city serves as a virtual object, encompassing nine applications as a composite virtual object. These applications are derived from the data set presented in the table, each associated with corresponding microservices that establish relationships based on specific constraints.

2) Data Validation Device Ontology: The device ontology provides a framework for organizing knowledge related to different objectives, taking into account the factors influencing the domain knowledge.There are two primary phases in the process: the first is to create a representation system for every device that is connected, and the second is to analyze the different fields in the model. The hardware entities or devices in the network are interfaced with via the device ontology. It operates as an intersection in our system between social item discovery and the device repository. In a different way, the system is in charge of managing microservices and composite objects that are virtual. enabling each service that provides these composite virtual things to communicate with one another.

3) Data Validation Operational Ontology: Among the three ontologies discussed, the operation ontology stands out as particularly unique. It stores various mathematical entities used by experts. system designers in fields like robotics, sensor networking, and more. However, it goes beyond mere storage; it organizes these models to be machine-accessible. This organization is essential for our middleware to distinguish suitable models for specific cases and identify the best models for specific domains. Therefore, the operation ontology must provide each model with a well-designed set of properties and enable complex social interactions between models, devices, and physical concepts. Specifically, it encompasses:

- Identify and Sensitivity models
- Data Threat models
- Elimination of risk models

In various professional disciplines, the ontology is vital for enhancing the functionality of knowledgeable systems.

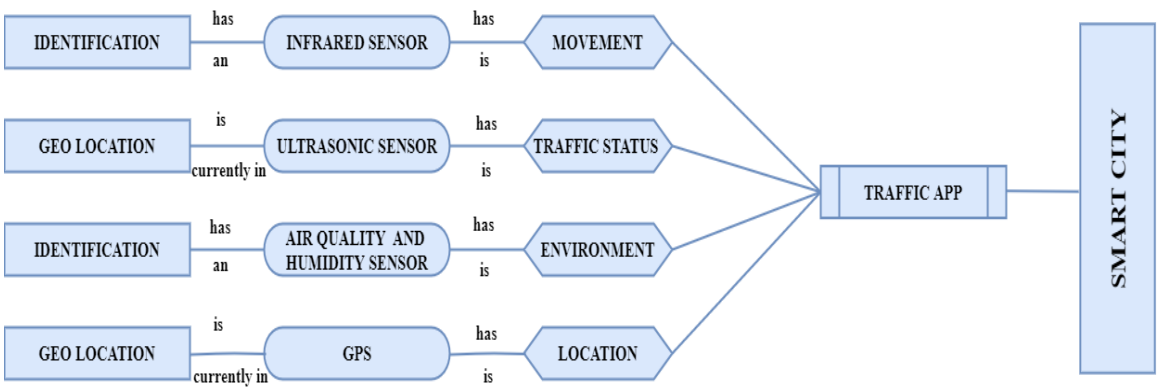

Fig. 3. Smart city ontological model for Traffic Applications

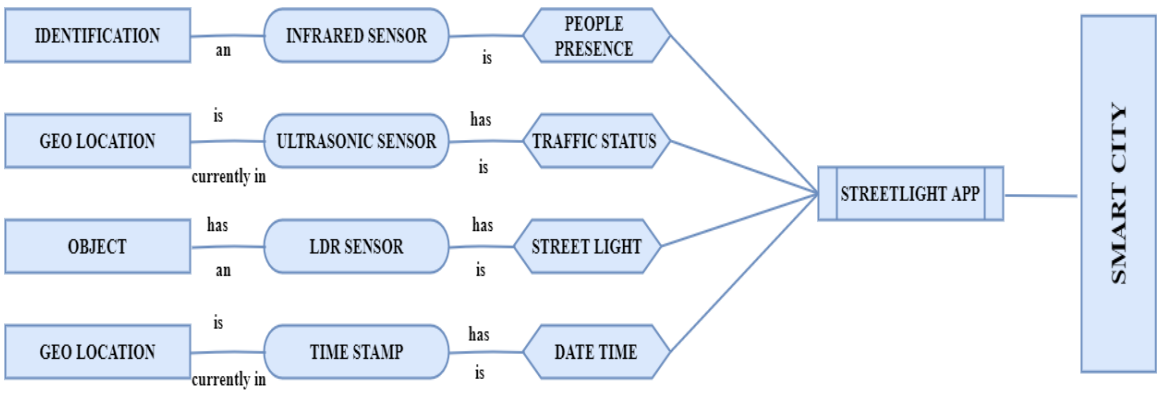

Fig. 4. Smart city ontological model for Streetlight

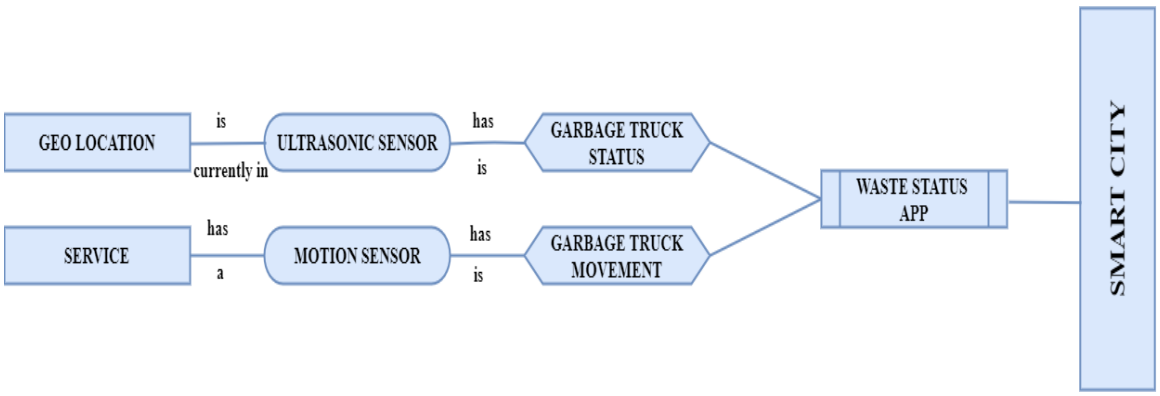

Fig. 5. Smart city ontological model for Waste Status Applications

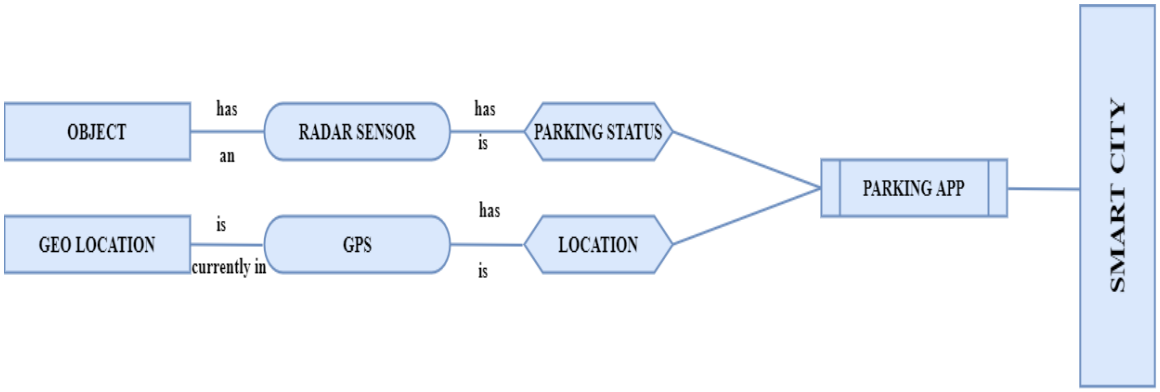

Fig. 6. Smart city ontological model for parking Applications

A. System Model

Consider smart city information, including source object ID, relationship type, destination object type, and trust factor: $D = (x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$, where x_i is the input feature vector and y_i is the output variable. Ontology model for representing the system and identifying data anomalies: $O = O_1, O_2, \ldots, O_m$, where O_i is the ith class of objects in the system. Trained Artificial Neural Network (ANN) model for classifying the sensitivity of data: $f(x) = y$, where f is the ANN model, x is the input feature vector, and y is the output variable indicating the sensitivity of data. Lagrange Polynomial Interpolation algorithm for finding intruders: $P(x) = \sum(y_i \cdot l(x_i))/\sum l(x_i)$, where P is the Lagrange Polynomial Interpolation function, x_i is the input feature vector, y_i is the output variable, and $l(x_i)$ is the Lagrange basis polynomial for x_i. Advanced Encryption Standard (AES-512) for encrypting data.

B. Problem Formulation

The overall objective function can be to maximize the security and reliability of the SIoT network by minimizing the risk of data breaches and unauthorized access. This can be achieved by combining the three components of the model (ANN, Lagrange Polynomial Interpolation, and AES-512 encryption) and optimizing them jointly. The objective function can be formulated as

$$\min \ \lambda_1 \cdot E_{\text{ANN}} + \lambda_2 \cdot E_{\text{Interpolation}} + \lambda_3 \cdot E_{\text{Encryption}} \quad (1)$$

where E_{ANN} is the error of the ANN classifier, $E_{\text{Interpolation}}$ is the interpolation error of the Lagrange Polynomial Interpolation, and $E_{\text{Encryption}}$ is the decryption error of the AES-512 encryption. The λ's are non-negative weights that can be tuned to balance the trade-off between the three components.

C. Proposed Solution

- **Artificial neural network (ANN) for classifying sensitivity of data:** The ANN is used to classify the sensitivity of data based on its features or attributes. Let x be the input vector of data features, y be the output vector of class labels (e.g., sensitive or non-sensitive), the w be the weight vector of the neural network and f is the activation function. It is represented as

  $$y = f(w^T x) \quad (2)$$

  Thus it minimizes the classification error or maximizes the classification accuracy. This is done using various optimization algorithms such as gradient descent.
- **Lagrange Polynomial Interpolation for finding intruders:** The Lagrange Polynomial Interpolation is used to find intruders in the SIoT network by estimating the values of missing or corrupted data points. Let x_i be the input vector of known data points, y_i be the output vector of observed values, and x be the input vector of missing or corrupted data points. It is defined as

  $$y = \sum_{i=1}^{n} y_i L_i(x), \quad \text{where} \quad L_i(x) = \prod_{j=1, j\neq i}^{n} \frac{(x - x_j)}{(x_i - x_j)} \quad (3)$$

  The usage of LPI minimizes the interpolation error thereby maximizing the accuracy of the estimated values.
- **AES-512 encryption for securing data:** The AES-512 encryption can be used to secure data in the SIoT network by encrypting it with a secret key. Let M be the plaintext message, K be the secret key, C be the ciphertext message, and E be the encryption function. The proposed AES-512 encryption method is obtained from the works of Santhosh Kumar K S et al. [13] and it is defined as

  $$C = E(K, M) \quad (4)$$

  The AES-512 encryption ensures the maximization of the security by encrypting the data making it difficult for unauthorized users to decrypt it without the secret key.

VI. Proposed OSSIoT framework

The smart city is represented as a virtual object that comprises nine apps as composite virtual objects from the supplied data set. The figure 7 depicts the methodology used to address the security issues of SIoT in the proposed model. The proposed model consists of three main components: data Sensitivity classification using artificial neural networks, intruder detection using Lagrange polynomial interpolation, and data encryption using AES-512 if no intruder is found. Firstly, the ANN is trained to classify the sensitivity of the data according to its importance and level of confidentiality. The workflow for the proposed system starts with the selection of data from the available data set. Next, the selected data is analyzed to identify the relevant smart city components and their relationships. Once the components and relationships are identified, Appropriate security measures are selected and implemented based on the associated risk levels. These measures include data encryption, access control, and intrusion detection. The effectiveness of the proposed security framework is evaluated through various simulations and experiments. The smart city is a vast interconnected system, like a futuristic city where various devices, Sensors, and data sources are constantly communicating and sharing information. This data can be incredibly valuable but also sensitive, just like personal information or important documents in our daily lives. The first step in this security framework is to understand which parts of the data are the most valuable, need special protection, and want to be safeguarded the most. Next, there's a system in place that keeps a vigilant eye on all the data and devices, just like a security guard or an alarm system for unauthorized access. In a smart city, this would be like having cameras and motion sensors that alert you if anything unusual happens. Now, even if everything seems safe, the framework takes an extra step to ensure data security. It's like putting your valuables in a safe. where the security system hasn't detected any intruders. In this case, the "safe" is data. encryption, a sophisticated way of locking up the data to make it incredibly hard for anyone to access, even if they manage to get past the initial security measures. Finally, the security framework is thoroughly tested to make sure it does its job effectively. It's like regularly checking your home security system to ensure it's working as expected. In the Smart City context:

this might involve running simulations and experiments to see how well the Security measures protect the data and devices. The proposed security framework for a smart city is like a multi-layered protection system. It identifies valuable data, watches for trouble, uses encryption as a last line of defense, and constantly checks to make sure everything is secure. This comprehensive approach is crucial for ensuring that the smart city functions smoothly while keeping its data safe from potential threats.

VII. Proposed OSSIoT algorithm

This section presents the algorithms used in the proposed operational security model. Algorithm 1 is used to classify the sensitivity level of the data between the devices based on the relationship between the devices. The classification helps to identify and prioritize the protection of sensitive data within the SIoT network.

Algorithm 1: Classify Sensitivity using ANN

Input : data_packet
Output: sensitivity_level

Inputs ← [data_packet.source_object_id, data _packet.destination_object_type, data_packet.trust_factor];

sensitivity_model ← `train_ann_model` (inputs, output_data)

sensitivity_level ← `predict_sensitivity_level` (inputs)

return *sensitivity_level*

Algorithm 2: Find Intruders using Interpolation

Input : data_packet
Output: intruder_detected

Inputs ← [timestamp for packet in packets]

Outputs ← [location for packet in packets]

lagrange_coefficients ← `calculate_lagrange _coefficients` (inputs, outputs)

new_time_stamp ← data_packet.timestamp

location ← `interpolate_location` (lagrange_coefficients, new_time _stamp)

if *location is within expected range* **then**
  return *False*
end
else
  `alert_security_personnel` () **return** *True*
end

Algorithm 2 describes the steps followed to identify the intruder. The Lagrange Polynomial Interpolation (LPI) algorithm is used to detect intruders attempting to access or manipulate the sensitive data within the network. The algorithm can predict the relationship type between devices and identify any anomalies in the data flow. If an intruder is detected, the system will initiate an alert to notify the administrator, and the data will not be transmitted until the issue is resolved. Algorithm 3 is used if no intruder is detected, the data is encrypted using the AES-512 encryption algorithm, which is a robust and secure encryption method. Algorithm 4 is used to Data decryption by using generation key, which is a robust and secure method. Algorithm 5 acts as the main algorithm that is used to process the data packets between any two devices in SIoT. This ensures that even if the data is intercepted, it cannot be accessed or deciphered by unauthorized users.

Algorithm 3: Encrypt Data using AES-512

Input : data_packet
Output: encrypted_data

encryption_key ← `generate_encryption_key` ()

encrypted_data ← `AES_512_encrypt` (data_packet, encryption_key)

return *encrypted_data*

Algorithm 4: Data Decryption Using key

Input : data_packet
Output: encrypted_data

decryption_key ← `generate_Decryption_key` ()

encrypted_data ← `AES_512_encrypt` (data_packet, decryption_key)

return *decrypted_data*

VIII. Result and Discussion

In this section, comprehensive information is provided regarding the dataset, the steps undertaken for data pre-

Algorithm 5: Main algorithm: process data packets

function *process_data_packets*:
  packets
end
for *data_packet in packets* **do**
  sensitivity_level ← `classify_sensitivity_using _ANN` (data _packet) intruder_detected ← `find_intruders_using _interpolation` (data _packet) **if** *intruder_detected* **then**
    continue
  end
  else
    encrypted_data ← `encrypt_data_using_AES_512` (data_packet) `send_encrypted_data` (encrypted_data)
  end
end

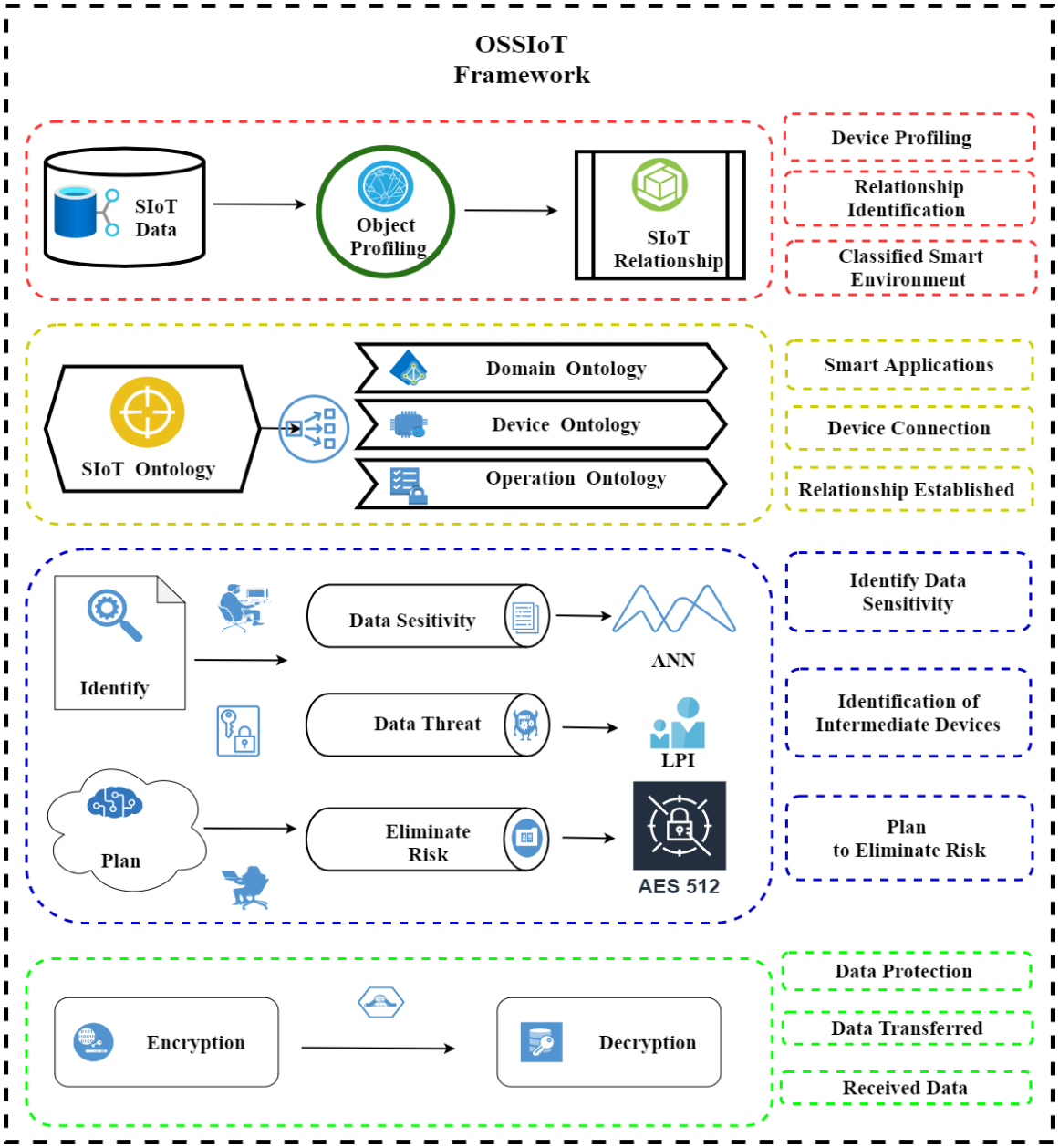

Fig. 7. A Proposed OSSIoT Framework

processing, and the simulation results specifically focused on SIoT smart city applications. The details encompass the dataset. description, the various pre-processing steps implemented, and the outcomes achieved. through the simulation process.

A. Dataset Description

The SIoT dataset includes 26 applications and 16 services, for a total of 52. features. These features include object profiles, requests for device information, and response: device information, device brand, device type, data type, connection type, and services. The dataset also contains information about the private details of smart applications, such as the device's identity, position, weather, traffic conditions, street lights, and sensor activity. Additionally, there is an encryption service ID for the relationship, source, and destination, and object ID. The relationships are of 10 different types. Mohan S.D. et al. [11] offered valuable insights into devices and their surroundings. It includes information about the device names, environmental temperature, weather conditions, road traffic levels, street light status, and device mobility. This dataset enables tracking device movements and their responses to surrounding conditions. It can be leveraged to optimize traffic. management systems, enhance driver safety and reduce travel time. The object Profiling showcases the device service IDs and their associated services. and relations. Various devices are linked to services, such as location, environment, traffic status, movement, people's presence, and more. The Relationships exist between devices and services, denoted by different acronyms. Table II gives the system ID and the system model are both included in the dataset. and each is given an ID number. the descriptions of the 16 service IDs' matching system models. The first service ID is for location, whereas the second service ID is for date and time, POI (point of interest) events are represented by the third service ID. A person's present service ID is the fourth service ID.

Environment is represented by the fifth service ID, weather by the sixth, and energy use by the seventh. Traffic status is the subject of the eighth service ID. while street light is the subject of the ninth service ID. The movement of an object is the tenth service ID. The People Counter (in the bus) is the eleventh service ID, and the Trash Pickup Status is the twelfth service ID, and the parking condition is the thirteenth service ID. Medical Information is the topic of the fourteenth service ID, while indoor information is the topic of the fifteenth service ID. Consumption and related activities in the garbage truck movement are the sixteenth service ID. The device service IDs, along with the related services and relationships, are listed in object profiling. Location, environment, traffic status, movement, people's presence, People counter, street light, actuator, garbage truck status and movement, and parking status are just a few of the services that devices 1 through 13 and 16 have available. Devices and services have several relationships, including Mohan S.D. et al. [11] Depending on the type, brand, service, and nature of the device connected, there are several types of object relationships that can be connected to different devices, such as social object relationships, parent object relationships, co-location object relationships, guest object relationships, service object relationships, co-worker object relationships, object object relationships, stranger object relationships, guardian object relationships, and sibling object relationships. Overall, 10 types of relationships have been identified. Certain gadgets have connections to a variety of services, showcasing their versatility and potential applications in smart city settings. All things considered, the graphic provides a useful overview of the many services and technologies that may be employed in a smart city.

B. Data Preprocessing

The proposed model uses an Artificial Neural Network (ANN) to classify data sensitivity, determining if data can be shared between devices based on inter-device relationships. The ANN is trained using a specific dataset and evaluated using a separate testing dataset, with varying the size of the testing dataset being a key methodology. The ANN model's performance was improved through various techniques, including balanced datasets, increased neuron size, hidden layers, optimal activation functions, extended training epochs, and graphical analysis for performance evaluation, all of which contributed to the model's accuracy and robustness. The model's accuracy in classifying data sensitivity levels was significantly improved through rigorous experimentation and comparative analysis, enhancing data sharing decisions between devices and contributing to the broader field of artificial intelligence applications in data security and privacy. From Table III the Applications' sample dataset gives a thorough understanding of numerous devices and the environment in which they operate. Information concerning the gadget's name, the surrounding environment's temperature, the current weather, the volume of traffic on the road, whether the streetlight is on or off, and whether the device is moving or not are all provided in the columns. The information in each row is particular to the device's location and its surroundings, including the weather, traffic conditions, and status of street lights. The table makes it easier to see how the gadgets move and react to their environment. The data in the table might be used to improve traffic management systems and provide drivers with real-time information. to increase safety and cut down on travel time. Table IV shows the operations that can be performed in SIoT. By implementing these operations, a social IoT network can be secured using a relationship-based key encryption method for sensitive data. To ensure the security of the Social Internet of Things (SIoT), it is recommended to verify several features for operation. These features include authentication, access control, data integrity, key generation, encryption,and decryption are verifying these security features using an ontological model-based operational security model, SIoT can ensure that the data transmitted across the network is secure and can only be accessed by authorized entities. From Table V, the sample dataset for encryption with relationship keys provides information about different objects and their relationships in four columns. The first column represents the ID of the source object, the second column represents the type of relationship, the third column represents the ID of the destination object, and the fourth column provides an example of the message exchanged between the source and destination objects. Each row in the table represents a unique relationship between two objects. The relationships are of 10 different types.

C. Simulation Environment and user-defined parameters

The work supports Windows as well as Mac OS X and includes a 2.59Hz Intel core i7 CPU and 8 GB of RAM and 64 bit operating system. It uses SciPy, Pandas, NumPy, Matplotlib, and other scientific libraries and is developed in Python 3.7. The graphical user interface is built using PyQt5 5.15.4 and libraries for artificial intelligence like Joblib, Scikit-learn, and SKO are also present.

D. Results

Figures 8, 9, 10, and 11 show the results of different train-test ratios, including 90:10, 80:20, 70:30, and 60:40, on various evaluation metrics are F1 Score, recall, precision, and accuracy and their average values. The highest accuracy score of 90.0% was achieved with the 90:10 train test. ratio, while the highest precision score of 93.84% was achieved with the 80:20 ratio. The highest recall score of 97.44% was achieved with the 60:40 ratio, and the highest F1 score of 93.83% was achieved with the 90:10 ratio. The model has demonstrated high precision, recall, and F1 score, which indicates that it is performing well in identifying positive instances in the dataset. However, the accuracy is slightly lower, indicating that the model is struggling to correctly classify negative instances.

Figure 12 depicts the results of various performance metrics. The average values of these metrics are 85.67%, 90.37%, 92.06%, and 91.03%, respectively for accuracy, precision, recall, and F1 score for the evaluated ANN model. Table 2 summarizes these metrics and demonstrates that the proposed model performed better than the previous model, primarily due to the changes made in the ANN algorithms. This suggests that the modifications made to the ANN algorithms have improved the performance of the model, as indicated by the higher values of the evaluated

TABLE II
SMART CITY APPLICATIONS, DEVICE CONNECTIONS, DEVICE SERVICE IDS, SERVICES, AND RELATIONS

Applications	Request Device	Respond Device	Device Brand	Device Type	Data Type	Connection Type	Service ID	RELATIONSHIPS
STREETLIGHTAPP	car	car	D	D	ST	PR	4,8,9	CLOR, SOR, GSTOR, POR
TRAFFICAPP	tablet	car	D	S	HY	PR	1,5,8,10	SOR, CLOR, SVOR, GSTOR
BUSAPP	tablet	smart phone	D	D	ST	RR	1,2,10,11	STGOR, GSTOR, POR,SOR SVOR, CWOR
TEMPERATUREAPP	car	tablet	D	D	ST	RR	1,5	CLOR, SVOR, POR, SOR,GOR
WEATHERAPP	car	car	D	S	HY	RR	1,2,5,6	SOR, POR, CLOR, CWOR, SVOR
WASTESTATUS	smart	car	S	S	HY	RR	12,16	CLOR, CWOR, SVOR
PARKINGAPP	tablet phone	tablet	D	S	ST	RR	1,13	STGOR, CLOR, CWOR, SVOR, SOR, POR
CROWDAPP	car	tablet	D	D	ST	RR	1,5,6	POR, SOR, OOR, CWOR,CLOR
DRIVE MONITORING	car	tablet	D	D	HY	PR	5,6,8,9,10	POR, SOR, OOR, SVOR
CINEMAAPP	tablet	smart	S	D	HY	RR	1,2,3,4	CLOR, GSTOR, SVOR, POR, OOR

***D=Different, S=Same, ST= Static, HY= Hybrid, PR=public to private, RR=private to private**

TABLE III
DEVICE DATA IN A SMART CITY IOT

Device name	Environment	Weather	Traffic Status	Street Light	Movement
Car	hot	Rainy	Lw	off	yes
Tablet	cool	Lightening	Hi	off	yes
Tablet	normal	Clear Sky	Lw	on	no
Car	hot	Sunny	Lw	off	yes
Car	cool	Partly	Hi	off	yes
Smart Phone	normal	Clear Sky	Hi	off	yes
Tablet	normal	Sunny	Lw	on	yes
Car	normal	Sunny	Lw	off	yes
Car	cool	Clear Sky	Hi	on	no
Tablet	cool	Thunder	Hi	off	yes
Tablet	hot	Windy	Hi	on	no
Tablet	hot	Lightening	Hi	off	yes
Smart Phone	hot	Clear Sky	Hi	off	yes
Smart Phone	cool	Sunny	Hi	off	no
Tablet	normal	Sunny	Lw	on	yes
Smart Phone	hot	Sunny	Lw	on	yes
Car	cool	Thunder	Hi	on	yes
Car	normal	Sunny	Hi	off	yes
Tablet	normal	Clear Sky	Hi	on	yes

***Hi=High, Lw=Low**

TABLE IV
SECURITY OPERATIONS OF SIOT

Operations	Yes	No
Authentication	✓	
Access control	✓	
Data integrity	✓	
Key generation	✓	
Key distribution		✘
Key management		✘
Encryption	✓	
Decryption	✓	

TABLE V
OBJECT RELATIONSHIPS AND MESSAGES

Source Object ID	Relationship	Destination Object ID	Sample Message
car 1	OOR	phone 2	Requesting distance
car 2	SOR	phone 1	Playing songs
car 31	POR	car 13	Keep away from me
tv 1	CLOR	laptop 1	News channel
tv 2	CLOR	laptop 2	Recharge for monthly
phone 1	OOR	house alarm 1	Set alarm
phone 2	SOR	car 2	Park the car
phone 3	CWOR	phone 5	Start charging

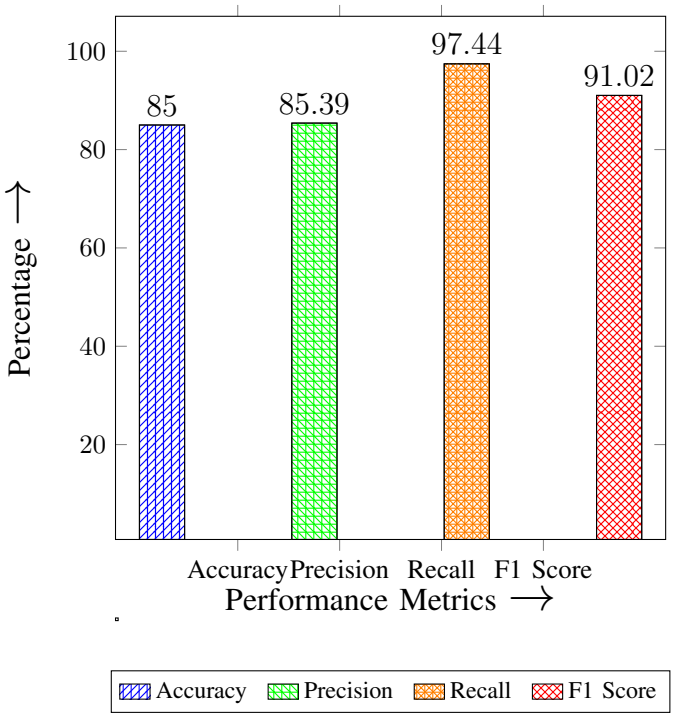

Fig. 8. Performance metrics results of the proposed model for the ratio 60:40.

metrics. To determine the intermediate device identification, Lagrange's polynomial interpolation is used. from the Figure

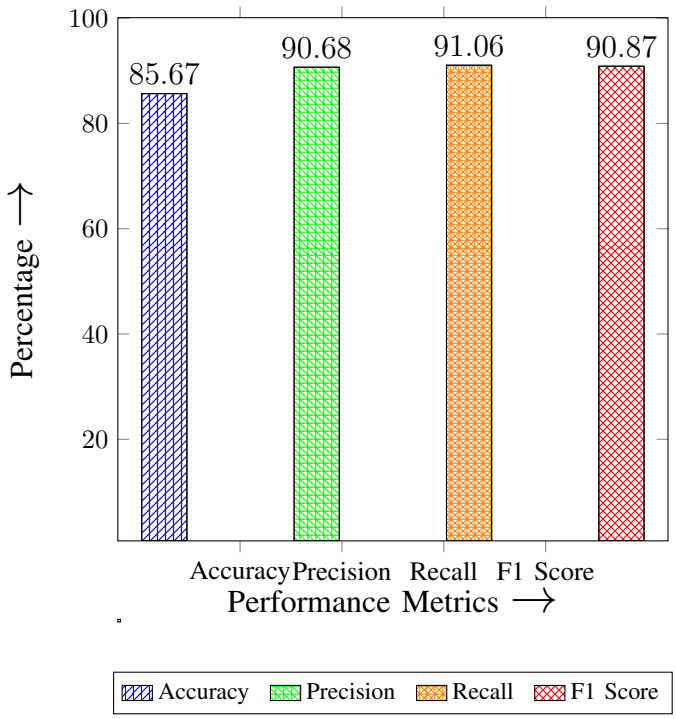

Fig. 9. Performance metrics results of the proposed model for the ratio 70:30.

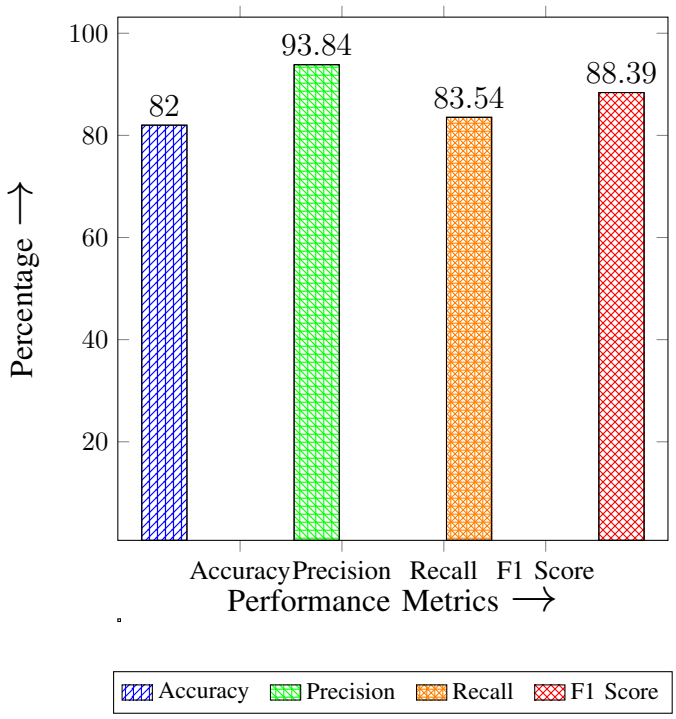

Fig. 10. Performance metrics results of the proposed model for the ratio 80:20.

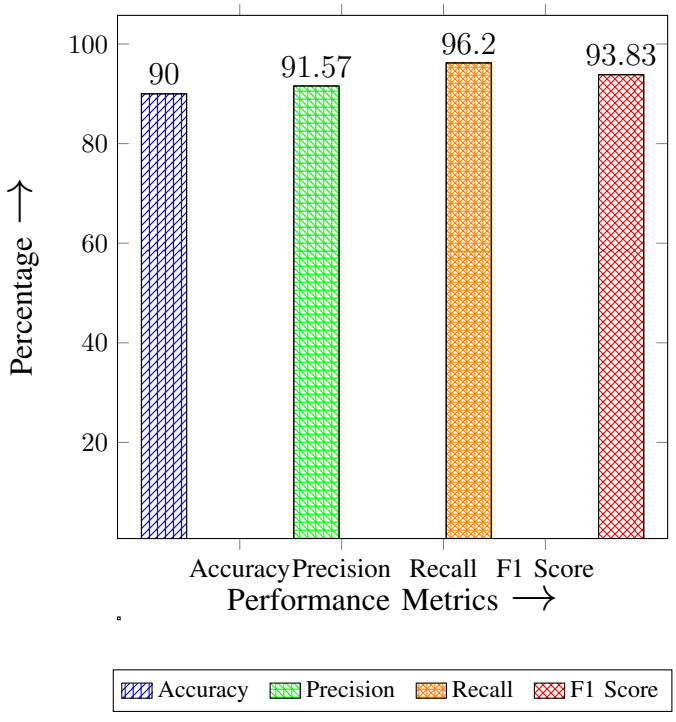

Fig. 11. Performance metrics results of the proposed model for the ratio 90:10.

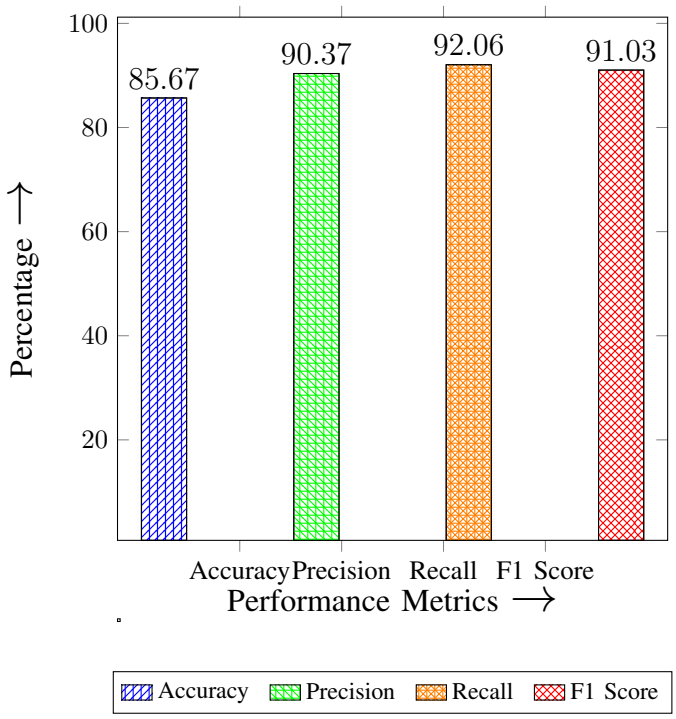

Fig. 12. Average Performance metrics result of the Proposal model

13 the Device to Device Relationship at time step '0' and Number of Devices in STREETLIGHT application, Figure 14 Device to Device Relationship at time step '10' and Number of Devices in STREETLIGHT application, Figure 15 Relationship changes Between Devices over time in STREETLIGHT application, Figure 16 Interpolation Devices for STREETLIGHT application at time step '0', Figure 17 Interpolation Devices for STREETLIGHT application at time step '10'and Figure18 Device count and Encrypted Data transferred between the devices in STREETLIGHT application.

Table VI compares the security features with and without AES. Encryption and LPI. AES encryption offers high levels of confidentiality. integrity, authenticity, and non-repudiation, but it slows down processing speed. and adds complexity due to key management. LPI also provides high security in various aspects that may impact performance. Both approaches ensure availability and scalability. Ultimately, the choice depends on specific security needs, speed, complexity,

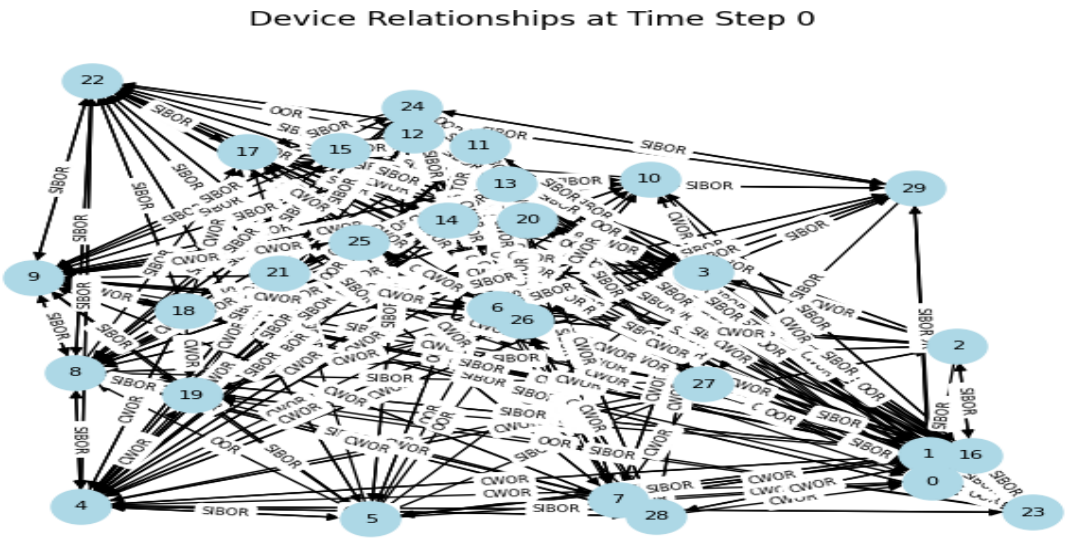

Fig. 13. Device to Device Relationship at time step ’0’ and Number of Devices in STREETLIGHT application

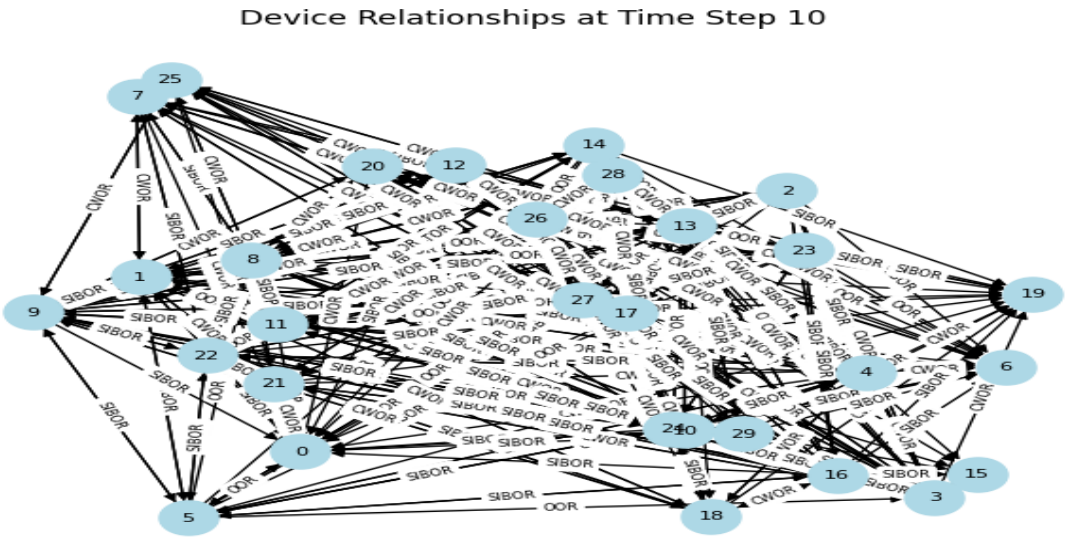

Fig. 14. Device to Device Relationship at time step ’10’ and Number of Devices in STREETLIGHT application

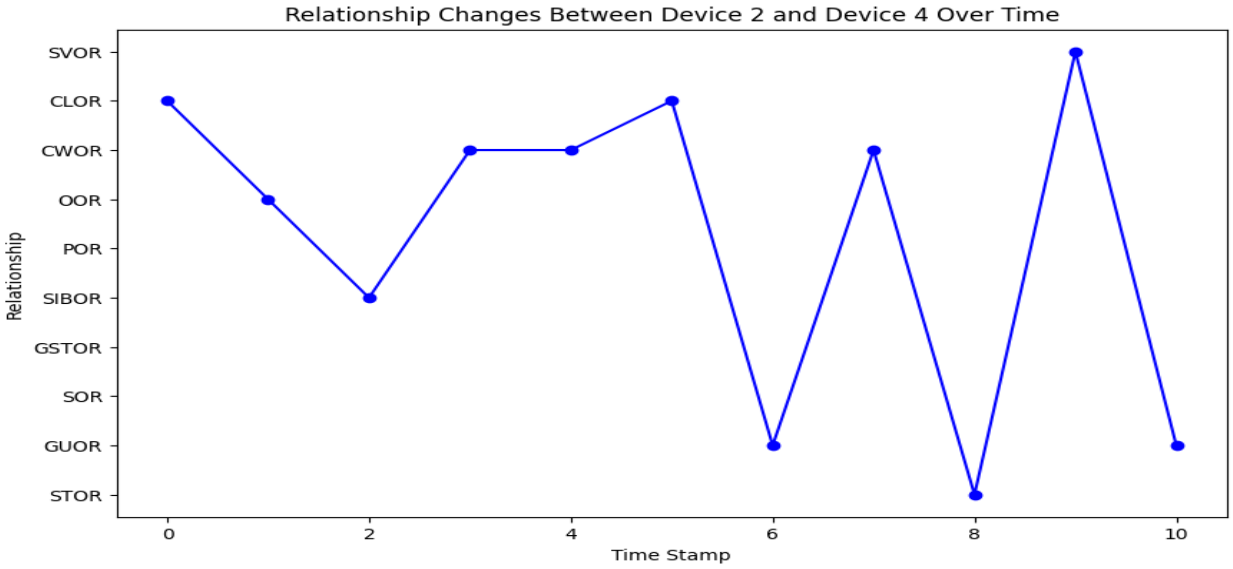

Fig. 15. Relationship changes Between Devices over time in STREETLIGHT application

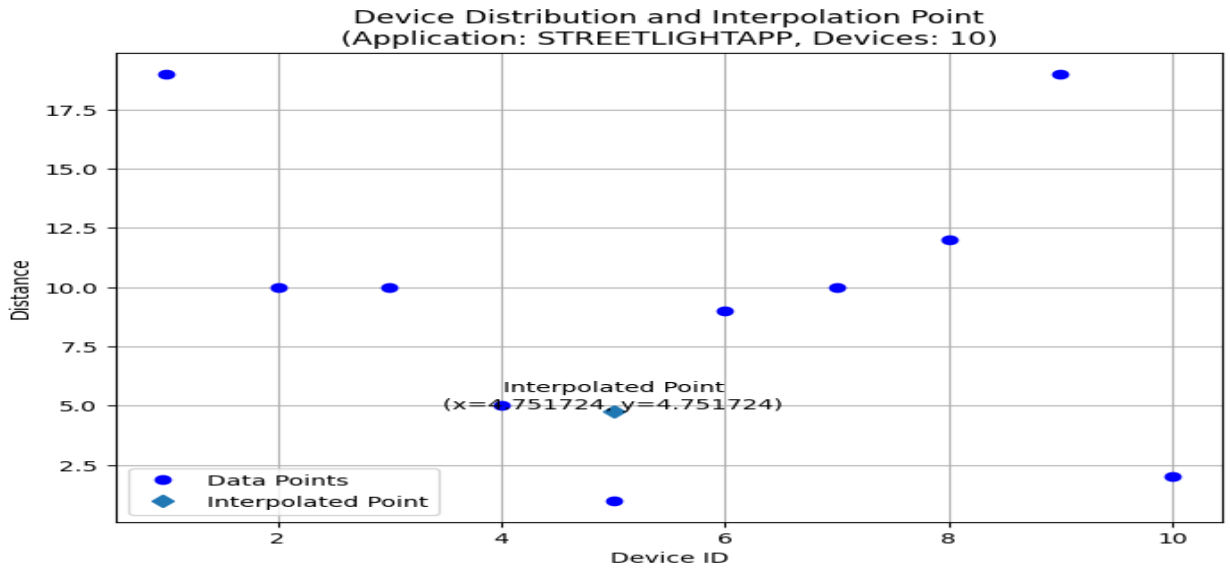

Fig. 16. Interpolation Devices for STREETLIGHT application at time step '0'

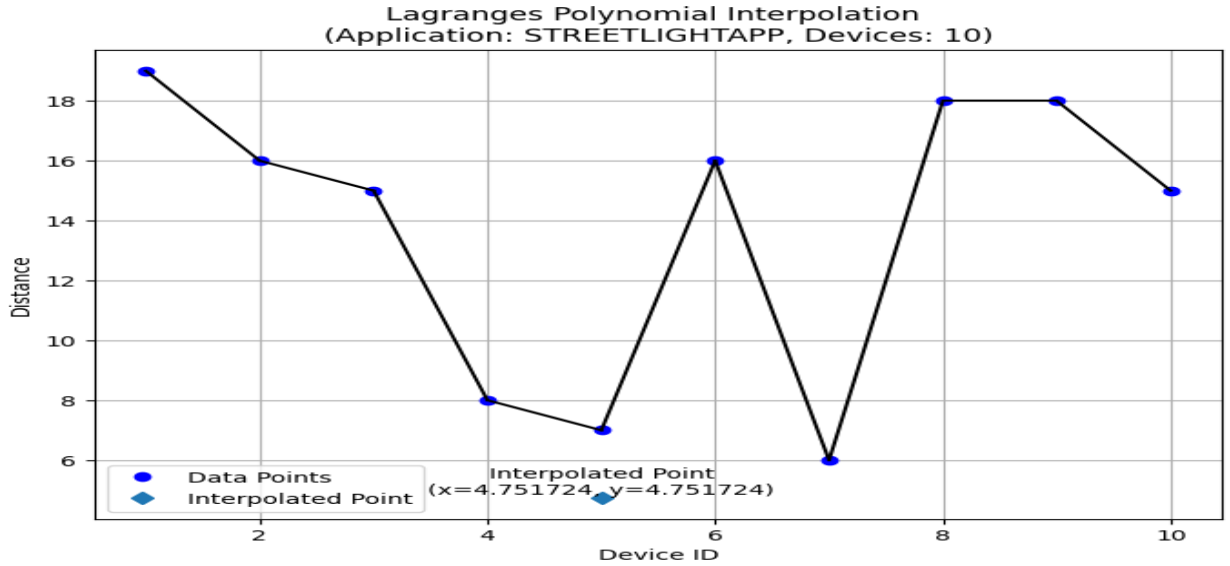

Fig. 17. Interpolation Devices for STREETLIGHT application at time step '10'

```
Enter the application name:
STREETLIGHTAPP, TRAFFICAPP, BUSAPP, TEMPERATUREAPP, WEATHERAPP,
WASTESTATUS, PARKINGAPP, CROWDAPP, DRIVE MONITORING, CINEMAAPP
STREETLIGHTAPP

================STREETLIGHTAPP=======================
The Device ID 1: 2
The Device ID 2: 4
The Number of Devices in STREETLIGHTAPP is 10
==============END OF STREETLIGHTAPP =================

======================================================
Random Relationship is: SOR
Encrypted String: b'\xdd\xe0\x0c\xb1\xec\x90G\x80\x99\x10\xb8\x1d\x18\xcd\x05\xa7'
Decrypted String: SOR
```

Fig. 18. Device count and Encrypted Data transferred between the devices in STREETLIGHT application

TABLE VI
COMPARISON OF SECURITY FEATURES WITH AES ENCRYPTION AND LPI

Security Feature	With AES Encryption	Without AES Encryption	With LPI	Without LPI
Confidentiality	H	L	H	L
Integrity	H	L	H	L
Authenticity	H	L	-	-
Non-repudiation	H	L	H	L
Key Management	E	NR	-	-
Availability	H	L	H	L
Scalability	H	L	H	L
Complexity	H	L	H	L

***H=High, L=Low, E=Essential, NR=Not required**

and key management trade-offs.

IX. CONCLUSION AND FUTURE WORK

This study focuses on addressing issues that arise from variations in the relationship between devices. A machine learning approach called OSSIoT is proposed to classify the relationship between devices by modifying the ANN model. The evaluation metrics, were measured at 85.67%, 90.37%, 92.06%, and 91.03%, respectively, for average accuracy, precision, recall, and F1 score. These improvements can be primarily attributed to advancements in the ANN. algorithms. Additionally, an innovative LPI approach is introduced to identify intruders among devices, which is the first of its kind in the domain of SIoT. This approach facilitates secure data sharing among authorized devices or users by employing a modified AES-512 algorithm for data encryption. As a result, the proposed OSSIoT framework ensures a secure data sharing for smart city applications, enhancing the overall security of inter- device communication. Future research will involve testing the model against various attacks, considering other aspects of SIoT such as device mobility and the influence of changes in device relationships. By exploring these aspects, the The proposed model provides comprehensive security solutions for SIoT in the future.

REFERENCES

[1] M. Moh and R. Raju, "Machine Learning Techniques for Security of Internet of Things (IoT) and Fog Computing Systems," *2018 International Conference on High-Performance Computing & Simulation (HPCS), Orleans, France*, 2018, pp. 709 -715,

[2] F. Liang, W. G. Hatcher, W. Liao, W. Gao and W. Yu, "Machine Learning for Security and the Internet of Things: The Good, the Bad, and the Ugly," in IEEE Access, vol. 7, pp. 158126-158147, 2019,

[3] Ikram Ud Din, Mohsen Guizani, Joel J.P.C. Rodrigues, Suhaidi Hassan, Valery V. Korotaev, "Machine learning in the Internet of Things: Designed techniques for smart cities", Future Generation Computer Systems, Volume 100,2019, Pages 826-843, ISSN 0167- 739X,

[4] Sarker, I.H., Kayes, A.S.M., Badsha, S. et al. Cybersecurity data science: an overview from machine learning perspective. J Big Data 7, 41 (2020)

[5] A. Qureshi, M. A. Qureshi, H. A. Haider and R. Khawaja, "A review on machine learning techniques for secure IoT networks," 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 2020, pp. 1-6,

[6] Sagu, Amit & Gill, Nasib & Gulia, Preeti. (2020). Artificial Neural Network for the Internet of Things Security. International Journal of Engineering Trends and Technology. 68. 129-136.

[7] Amit Sagu, Nasib Singh Gill, Preeti Gulia,"Artificial Neural Network for the Internet of Things Security" International Journal of Engineering Trends and Technology 68.11(2020):129-136.

[8] Rasheed Ahmad, Izzat Alsmadi,"Machine learning approaches to IoT security: A systematic literature review," in Internet of Things, Volume 14,2021,100365,ISSN 2542-6605.

[9] Umer Farooq, Noshina Tariq, Muhammad Asim, Thar Baker, Ahmed Al-Shamma'a,"Machine learning and the Internet of Things security: Solutions and open challenges", Journal of Parallel and Distributed Computing, Volume 162,2022, Pages 89-104, ISSN 0743-7315,.

[10] Sarker, I.H., Khan, A.I., Abushark, Y.B., "Internet of Things (IoT) Security Intelligence: A Comprehensive Overview", Machine Learning Solutions and Research Directions. Mobile Netw Appl (2022).

[11] Mohana S. D, S. P. Shiva Prakash and Kirill Krinkin, "Service Oriented R-ANN Knowledge Model for Social Internet of Things," *Big Data Cogn. Comput*, vol. 6, no. 1, p. 32, 2022.

[12] Shah, S.F.A.; Iqbal, M.; Aziz, Z.; Rana, T.A.; Khalid, A.; Cheah, Y.-N.; Arif, M. The Role of Machine Learning and the Internet of Things in Smart Buildings for Energy Efficiency. Appl. Sci. 2022, 12, 7882.

[13] Santhosh Kumar K.S, Hanumanthappa J, Shiva Prakash S.P, Krinkin K. "Relationship- Based AES Security Model for Social Internet of Things." *Intelligent Systems and Applications. Lecture Notes in Electrical Engineering*, vol. 959, Springer, Singapore.2022.

[14] Mohana, S. D., Shiva Prakash, S. P., and Krinkin, Kiril, "Relationship LSTM Network for Prediction in Social Internet of Things", booktitle="Intelligent Systems and Applications," Springer Nature Singapore, vol.19, pp.133-141, 2023.

[15] Vinay Gugueoth, Sunitha Safavat, Sachin Shetty, "Security of Internet of Things (IoT) using federated learning and deep learning: Recent advancements, issues and prospects", ICT Express,2023, ISSN 2405-9595.

[16] Ali, Y., Khan, H.U. & Khalid, M. Engineering the advances of the artificial neural networks (ANNs) for the security requirements of Internet of Things: a systematic review. J Big Data 10, 128 (2023).

[17] Ghazal, T.M., Hasan, M.K., Ahmad, M., Alzoubi, H.M., Alshurideh, M, "Machine Learning Approaches for Sustainable Cities Using Internet of Things", Studies in Computational Intelligence, vol 1056. Springer, Cham.

[18] N. Moustafa, N. Koroniotis, M. Keshk, A. Y. Zomaya and Z. Tari, "Explainable Intrusion Detection for Cyber Defences in the Internet of Things: Opportunities and Solutions," in IEEE Communications Surveys & Tutorials, vol. 25, no. 3, pp. 1775- 1807, third quarter 2023.

[19] Guowen Wu, Lanlan Xie, Hong Zhang, Jianhua Wang, Shigen Shen, Shui Yu,"STSIR: An individual-group game-based model for disclosing virus spread in Social Internet of Things", Journal of Network and Computer Applications, Volume 214,2023,103608, ISSN 1084-8045.

[20] S. Zhang, D. Zhang, Y. Wu and H. Zhong, "Service Recommendation Model based on Trust and QoS for Social Internet of Things," in IEEE Transactions on Services Computing.

[21] S. Sagar, A. Mahmood, K. Wang, Q. Z. Sheng, J. K. Pabani and W. E. Zhang, "Trust–SIoT: Toward Trustworthy Object Classification in the Social Internet of Things," in IEEE Transactions on Network and Service Management, vol. 20, no. 2, pp. 1210-1223, June 2023.

[22] Wu, H., Ye, W. & Guo, Y. "Data access control method of cloud network secure storage under Social Internet of Things environment". Int J Syst Assur Eng Manag 14, 1379–1386 (2023).

[23] R. U. Mustafa, A. McGibney and S. Rea, "Establishing Trustworthy Rational Friendships in Social Internet of Things," 2023 International Conference on Information Networking (ICOIN), Bangkok, Thailand, 2023, pp. 318- 327.

[24] Deng, Mina, Xu, Fanga; Xiong, Zengganga, Xu, Qionga, Liu, Zhena, Guo, Hairua, "Exploiting social context awareness for intelligent data forwarding in social Internet of Things", Journal of Computational Methods in Sciences and Engineering, vol. Pre-press, no. Pre-press, pp. 1-15, 2023.

[25] Yadav, S.K., Jha, S.K., Singh, S. et al. An Efficient and Secure Communication Mechanism for Internet of Things Based Connected Devices. Wireless Pers Commun (2023).

[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.(2023).

[27] Pliatsios A, Lymperis D, Goumopoulos C. S2NetM: A Semantic Social Network of Things Middleware for Developing Smart and Collaborative IoT-Based Solutions. Future Internet. 2023; 15(6):207.

[28] 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(2023).

[29] Akli, A., Chougdali, K. 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, Cybercrimes, and Smart Emerging Technologies. CCSET 2022. Engineering Cyber- Physical Systems and Critical Infrastructures, vol 4. Springer, Cham.(2023).