International Journal of Safety and Security Engineering
Vol. 14, No. 4, August, 2024, pp. 1279-1291
Journal homepage: http://iieta.org/journals/ijsse

Lightweight Cryptography Based Secured Data Transmission Model for Quality of Service in Internet of Things-A Comparative Analysis

Srilakshmi Puli*, Nulaka Srinivasu

Koneru Lakshmaiah Education Foundation, Vaddeswaram 522502, India

Corresponding Author Email: srilakshmipuli77@gmail.com

https://doi.org/10.18280/ijsse.140425

Received: 7 April 2024
Revised: 29 July 2024
Accepted: 14 August 2024
Available online: 30 August 2024

Keywords:
internet of things, routing, trust, lightweight cryptography, malicious nodes, loss, network security, quality of service

ABSTRACT

Emerging technology like Internet of Things (IoT) seeks to facilitate the linking of numerous smart devices and diverse networks. IoT enabled platform architecture heavily relies on ad hoc networks because of their efficient, adaptable, low-cost, and dynamic infrastructures. To keep Quality of Service (QoS) intact in a multi-hop transmission, these networks make good use of the resources that are available. Secure and trustworthy data transmission is crucial because malevolent relay nodes can occur in multi-hop communication. Quality of service is considered in the suggested secure communication approach for networks based on the IoT that uses a trusted route model. Routing and security are the two most important components of a wireless network. With massive networks like the Internet of Things, these instances become two times as important. The novel nature of the IoT makes its far-reaching repercussions on healthcare stand out, yet it has had an influence on many aspects of society. When coupled with mobile computing, the IoT becomes even more beneficial due to mobile computing's characteristics. The beneficial impacts of the Internet of Things on healthcare are mostly attributable to mobile health, which is enabled by mobile computing. Wearables flood Internet of Things devices with data from their many sensors, actuators, and transceivers. Data on the IoT is vulnerable to a plethora of threats, assaults, and vulnerabilities. Consequently, a strong security solution is required to resolve concerns regarding the privacy, security, and vulnerabilities of the Internet of Things. This research presents an efficient routing protocol-based architecture for the secure and scalable transfer of healthcare data in the IoT. The presence of malicious nodes makes this network vulnerable to numerous attacks. This research presents a brief comparative analysis on the proposed routing model, group key management model and malicious nodes detection model in which these models are compared with the traditional models. The comparative analysis showed that the proposed models are efficient and effective in providing Denial of Service (DoS).

1. INTRODUCTION

The IoT is a relatively new technology in the realm of intelligent communication; several institutions and businesses are joining this technology daily due to its benefits. The research allows us to envision the communication landscape of the future within the framework of the IoT. Because of these characteristics, academics are considering using new technology to build the IoT, such as the 5G network [1]. Expanding the number of supported devices beyond what is now possible is a critical component of the IoT [2]. One of the new planned uses for the IoT is the management of communication between billions of linked sensors and radio devices [3]. There will be additional security risks associated with providing a communication platform for so many devices. In such a network, victims of cyber attacks may, for instance, be unable to use devices in their homes, vehicles, or cell phones. This is why numerous studies have offered ways to make these networks more secure for communication [4]. This network still needs better security measures, and the issue is not yet resolved.

DoS assaults and other threats are becoming more common in the IoT due to the proliferation of linked devices and apps. To avoid impersonation or man-in-the-middle attacks, this network's users should employ more efficient two-way authentication than earlier generations [5]. This is why a quick, precise, and resilient security solution for secure communications in the IoT is essential. However, new research suggests that encryption techniques alone won't be enough to secure data and communications transmitted by the IoT. Security must accompany efficiency when performing one of the most fundamental tasks in communication networks routing [6]. Failing to do so results in wasted processing resources and makes it impossible to detect attackers. To ensure the safety of the IoT data routing [7], it is necessary to have a well-structured system for arranging network devices and to have a methodical strategy for detecting potential threats by analyzing massive volumes of network data [8]. The specified security processes cannot be fully assigned to things due to concerns such as heterogeneity, limited computational

capabilities, and lack of full reliability [9]. However, owing to the significant overhead, traditional centralized security systems are ill-equipped to safeguard communications across massive networks like the IoT. Because of these problems, IoT routing security solutions need to be reviewed [10]. The network structure is shown in Figure 1.

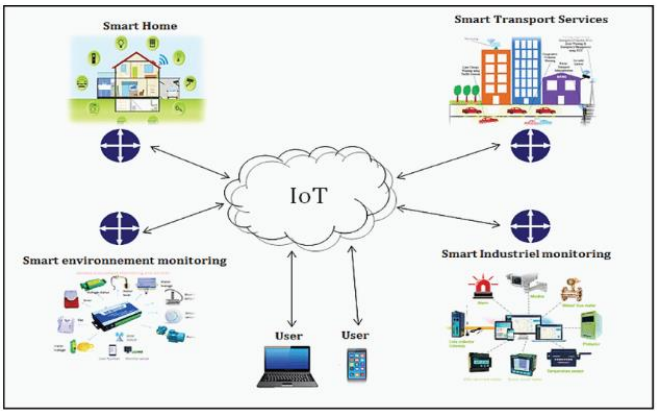

Figure 1. IoT network structure

This research impetus comes from the pressing need to develop a unified and effective approach to real-time threat detection and secure routing in the IoT. Given this background, the primary goal of this research has been to address the limitations of existing solutions by developing a thorough and efficient method for secure routing that can identify assaults in the IoT. Many parts of IoT security have progressed, such as communications, privacy, authentication [11], and trust. To prevent future assaults and ensure the data of users is properly protected, it is essential to encrypt IoT connections [12]. Because n-to-n communication, which refers to group communication, is more difficult to encrypt than one-to-one communication, developers will find it problematic. It is necessary to encrypt messages in n-to-n communication for a group of receivers [13]. Group Key Management (GKM) is an essential component of safe group chat protocols. On decentralized systems, GKM is used to handle secret keys for secure group communication and distributes them to all members of the group [14]. Signing and encrypting group communications, authenticating members and messages, and granting access to group resources and traffic are all done via the shared group key [15].

A safe method that allows for the production, distribution, and revocation of cryptographic keys is vital for the devices to accomplish this goal. The robustness of proposed scheme is dependent on the cryptographic strength of the group key and the key management protocol [16]. A big leap forward in this direction has been the creation of trustworthy cryptographic protocols that can protect the confidentiality of both data and communications [17]. In addition, there are two main categories for cryptographic security mechanisms: symmetric and asymmetric. Symmetric, asymmetric, and hybrid group key management techniques are the three main types [18]. Secure communication channels between numerous parties can be established with the help of asymmetric key techniques [19], which are more powerful but also consume more power. Because of its importance in highly-connected networks, this technology is fundamental to the IoT. Elliptical Curve Cryptography (ECC) and Advanced Encryption Systems (AES) are two examples of cryptographic primitives that have been made lighter by the reduction of processing time and cost [20]. The level of difficulty of the problem is considered when deciding whether the algorithm is more attack-resistant or not. Number theory and discrete logarithms are the foundations of current group key management techniques [21], but they are susceptible to quantum computers. There will be a meteoric rise in the number of IoT devices as well as the capability of quantum computers in the next years. These two technologies challenge the present crypto techniques [22]. The cryptography model in key pair generation is shown in Figure 2.

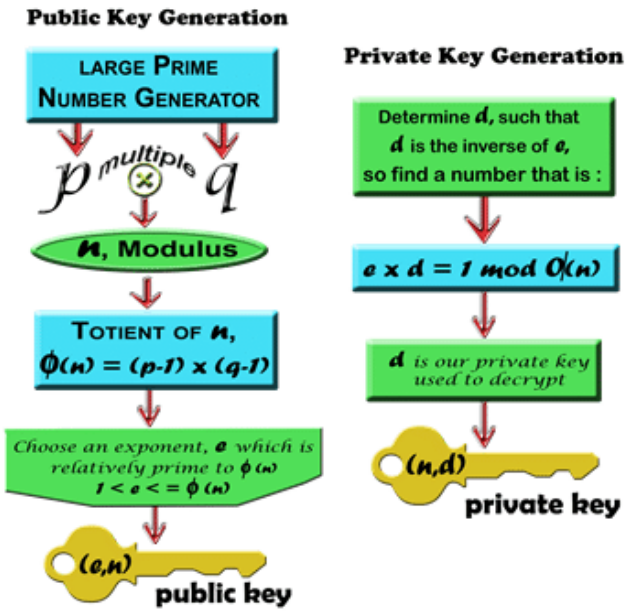

Figure 2. Cryptography model for key pair generation

Even though IoT devices pose a multitude of security vulnerabilities, the network is advancing at a rapid pace. Because IoT networks are complicated, IoT devices could be attacked in many different ways [23]. When an attacker uses a wireless control to eavesdrop on communications between nodes, it is considered a passive attack. Passive attacks are difficult to detect because they simply gather data without making any changes to the way a protocol normally operates. A attacker node breaches the security strategy and endangers the availability and integrity of the network by actively inserting fake information, deleting and modifying data packets, and negatively impacting on network protocols [24]. The source determines whether an attack is considered internal or external. In a network, an attack can be either external, coming from a node outside the network, or internal, coming from nodes inside the network, which are allowed to illegally use its resources [25]. Malicious nodes can cause significant damage to system and network operations if not eliminated, hence it is critical to find them quickly [26].

The proliferation of IoT devices has made it imperative for businesses to oversee the functioning, testing, debugging, and security of these devices in real-time. Nevertheless, there are three primary reasons why this work is challenging: First, the dispersed nature of the devices makes them hard to keep track of, and second, the diversity of the environment hinders people's ability to communicate clearly. As a last point, the job is difficult. Finally, and maybe most importantly, there is the issue of safeguarding systems and data against assaults, vulnerabilities, and other defects. They derive behavioral qualities that can be utilized to make decisions in domains

where privacy and security are still crucial by viewing machine learning via the classic Confidentiality, Integrity, Authentication (CIA) model. This research presents a brief comparative analysis on the proposed routing model, group key management model and malicious nodes detection model in which these models are compared with the traditional models. The comparative analysis showed that the proposed models are efficient and effective in providing QoS.

The introduction section 1 discussed about the cryptography models for secure data transmission models in IoT. Section 2 provides brief literature survey by analyzing numerous models using cryptography for data transmission to maintain security. Section 3 considers 3 traditional models and discussed their working model. Section 4 explains the proposed methodology considered using cryptography for secure data transmission. Section 5 provides the evaluation metrics and comparison of proposed model with traditional methods. Section 6 concludes the paper.

2. LITERATURE SURVEY

With cognitive radio (CR) capabilities, IoT devices can dynamically allocate spectrum and are finding widespread use in a variety of smart applications. Improving throughput in CR-enabled IoT communication is the primary goal in this study. In an IoT setting based on cognitive radio networks (CRNs), Malik et al. [1] suggested a routing method based on reinforcement learning (RL). To reduce EED and packet collisions, the network layer will be endowed with the decision-making power for channel selection. The author compared the network performance of our proposed RL-IoT routing mechanism to that of the recent AODV-IoT, ELD-CRN, and SpEED-IoT routing approaches, and simulated the cognitive radio cognitive network (CRCN) communication environment. This allows us to perform a thorough performance evaluation of the proposed mechanism.

While designing routing algorithms for IoT applications that employ multihop networking, conventional energy efficiency is only one of numerous distinct factors to be considered. Different security requirements, scalability, and heterogeneity are further unique factors. Zhang et al. [2] proposed a multilayer safe routing solution for IoT networks that is energy efficient. Combining clustering with a multihop routing system that is itself based on clusters helps alleviate the severe communication load associated with scaling in IoT networks, which is a natural method to save energy. When dealing with heterogeneous IoT networks that serve a varied range of IoT entities and services, it is essential to improve inter cluster routing and assign appropriate weights using genetic algorithms and a more realistic analytical hierarchy method. The trust factor on routing and clustering is estimated, and several forms of risk mitigation, including data fusion, communication trust, and data perception, are employed.

To reduce data latency and bandwidth between the cloud server and the IoT edge devices, the concept of edge computing was proposed. One of the biggest obstacles to getting reliable results from data mining is inefficient routing, which can cause transmission failure or unnecessary data (re)transmission. With link correlation in mind, Zhou et al. [3] investigated ways to improve wireless IoT infrastructure energy efficiency by combining network coding with opportunistic routing. The current routing methods are based on the assumption of link independence, yet research has shown that packet receptions on wireless networks are coupled. This assumption leads to estimation errors, which affect the accuracy of the predicted number of transmissions for forwarders. As a result, the selection of the forwarder set and the performance of the protocol are affected. An intrasession network coding mechanism was proposed by the author, with link correlation mining serving as its basis. An algorithm for selecting a set of forwarders with the optimum number of transmissions is part of a new smart routing technique, the purpose of which is to accurately estimate the quantity of transmissions required by forwarders.

The reliability of routing algorithms in wireless networks is assessed using the widely used Packet Delivery Ratio (PDR) statistic.

To put it simply, PDR is offered with the optimistic premise that the topology has been perfectly set up and that the nodes have started sending packets. Nodes still need to join the network and keep connected in order to send packets, but this remains true. The general stability of the routing protocols is critically dependent on this in mobile IoT applications due to the frequent disconnections. Unfortunately, there is a lack of appropriate criteria that could evaluate the routing systems from this perspective. Because of this, Safaei et al. [4] present attachability as a new metric to evaluate routing systems' ability to let mobile or stationary nodes establish and maintain their network connections. The author calculated the recently proposed measure using Markov chain analysis and the sample frequency-based estimate method. The author conducted extensive testing on multiple versions of the IPv6 Routing Protocol for Low-power and lossy networks (RPL) to evaluate attachability in a simulator for mobile IoT infrastructure. According to the results, attachability is significantly affected by the metrics used in routing algorithms and the strategies used for path selection.

One of the several possible applications of WSNs is in the development of more advanced IoT systems. Sensor nodes in WSNs do not allow battery replacement due to the inaccessibility or infrequency of the event being studied. Low-capacity batteries power WSNs with limited resources. Operating WSNs for extended periods of time poses challenges for Internet of Things applications due to the energy consumption of individual nodes and the overall lifetime of the network. Improving the longevity of WSNs requires the use of energy-efficient techniques, which are both necessary and challenging. Most on-demand routing methods consider hop count and other parameters when determining the best path from one node to another. Energy usage rises, IoT system lifespans drop, and route failures multiply when hop count is the only metric considered. Patel et al. [5] suggested a cross-layer variant of AODV by replacing the hop count statistic with the connection quality and collision count metrics. The proposed method retrieves connection quality data from the Physical layer and collision information from the MAC layer, and then applies the ZScore algorithm to aid the Network layer in making intelligent routing decisions. In order to create a solid and long-term routing plan, the proposed route metric considers this data.

While research on source-location-privacy (SLP) in WSNs has lately become popular, it is still in its infancy in the realm of underwater acoustic sensor networks (UASNs). Two crucial domains where SLP excels are underwater resource exploration and battle monitoring. A protocol for UASNs, LSLPR (layering and SLP-based routing), was proposed by Tian et al. [6]. To protect the SLP from passive attacks, the

LSLPR protocol makes use of multipath technology and proxy nodes; the precise location of the proxy nodes used by a source node is irrelevant when selecting a proxy node. In source-to-proxy area routing, the next-hop node is determined by the priorities of candidate nodes, which consider the node's distance and layer. This further reduces the long detour problem. In addition, a multipath routing approach based on the nodes layer and forwarding probability is proposed to avoid the void area problem and protect the SLP. When evaluating energy economy, safety period, and delay, the LSLPR protocol stands head and shoulders over 2hop-AHH-VBF, SSLP, and PP-SLPP, the Push-based probabilistic technique for source location privacy protection.

The proliferation of IoT devices that process sensitive data has prompted the development of new access control mechanisms to prevent their misuse. Particularly concerning is the fact that valid subscribers' mobility in an IoT environment with a high signaling overhead poses a significant threat to the security of data delivery. Thus, in these ever-changing contexts, GKM is the fundamental technique for managing key distribution for safe data distribution and access control. The scalability problem that arises with the proliferation of IoT devices and subscribers is too big for the centralized models utilized by the majority of current GKM-based IoT access control approaches. Also, no GKM plan that is currently in place respects members' independence. Inefficient subgroup communications occur when subscribers' behavior is highly dynamic and dependent symmetric group keys are the only means of communication. In response to these concerns, Dammak et al. [7] introduced DLGKM-AC, a novel architecture for Decentralized Lightweight Group Key Management in an Internet of Things context. In a hierarchical design with a single Key Distribution Center (KDC) and numerous Sub Key Distribution Centers (SKDCs), the proposed method enhances subscriber group management while decreasing rekeying overhead on the KDC. Furthermore, a master token—a unique method for managing the distribution of keys among a group of subscribers—is introduced. This protocol ensures that storage, processing, and communication are not overloaded during join and depart events.

Due to their massive computing overhead, existing cryptographic methods are severely insufficient for IoT scenarios, especially for terminal-embedded devices with limited resources. Even more so, the computing power of the server side is far more than that of the terminal devices in the majority of IoT environments. An approach to guaranteeing scenario security, the asymmetric computing cryptosystem is presented here. Wang et al. [8] created ACKE, an asymmetric computing key exchange protocol, by combining the Diffie-Hellman key exchange protocol with the Subset Product issue. One party's computational complexity can be significantly reduced while another party's computational complexity can be raised to an acceptable level; this is the fundamental idea underlying this build. A simulated IoT environment using the proposed protocol is constructed on a 2.2 GHz Intel i5-5200U laptop with 8G of RAM and a 1.2 GHz MTK6062 wristwatch with 512M of RAM.

The IoT has made it possible for low-resource sensors and actuators to establish Internet connections. There are a lot of security risks and attacks, so it needs defenses like encryption, message authentication codes, authentication, etc. Data transfer security between networks of devices is essential for various Internet of Things use cases. It is also important to keep the group keys used for multicasting information inside the group up-to-date because devices in dynamic IoT settings may join or exit a group at any time. A novel method based on factorial trees and the Chinese Remainder Theorem was proposed by Sudheeradh et al. [9] for efficient Group Key Management. By efficiently updating the group keys when devices join or leave a group, the proposed approach ensures forward and backward secrecy and prevents unauthorized users from obtaining group information. After testing the proposed method with precise mathematical analysis and numerical computations, the author proved that it outperforms prior work with regard to the processing and communication costs experienced by IoT devices.

It is extremely difficult to ensure the validity, integrity, and secrecy of data when it is collected and transmitted by IoT applications. Given the potential use of numerous limited devices in these applications, minimizing the communication and processing cost of security services is an important consideration. The IoT and group authentication/key management are the primary topics of this article. Asymmetric ciphers are used for calculations by the current group authentication and key management protocols in the literature, which can be expensive for the IoT. As a result, most apps use weak security measures that might be exploited by cybercriminals exploiting IoT devices. Yıldız et al. [10] presented PLGAKD, a system for lightweight group authentication and key distribution that uses physically unclonable functions (PUF), factorial trees, and the Chinese remainder theorem (CRT). To simplify group member authentication and key distribution in PLGAKD, PUF is used. Two encryptions, one decryption, four XORs, and three HMAC operations are executed by each member of the group. In contrast to the binary tree, the factorial tree and CRT allow us to decrease the amount of communication messages and keys held in nodes during the key renewal process.

When it comes to protecting group communications, group key establishment methods are a crucial building piece. Protocols for group key agreement work best in distributed settings where participants in different locations can reach a consensus on the group key. The members of a group are entrusted with important information using methods like secret sharing schemes (SSS), polynomials, and bilinear pairing. Among these methods, secret sharing schemes outperform the competition. Such key agreement protocols are essential in contexts with limited resources, which has been highlighted by the recent explosion in IoT-related applications. To achieve sufficient security with smaller key sizes, elliptic curves are commonly used in resource-constrained applications. For situations when resources are limited, Subrahmanyam et al. [11] proposed an elliptic curve secret sharing scheme (ECSSS). An alternative group key agreement protocol called Authenticated Distributed Group Key Agreement Protocol (ADGKAP) is suggested, which shares information about group keys via the Elliptic Curve Secret Sharing Scheme (ECSSS).

To keep monitoring and prevent undesirable traffic flows in the IoT network, it is vital for IoT security to identify anomalies and malicious traffic. Many academics have proposed models using ML techniques to prevent harmful traffic flows in the IoT network. Unfortunately, a number of ML models frequently misclassify traffic flows, the majority of which are malicious, because of poor feature selection. Nevertheless, a great deal of research into the best practices for feature selection in order to accurately detect fraudulent

traffic in IoT networks is still required. Shafiq et al. [12] offered a new framework model to fix the issue. A new feature selection algorithm, CorrAUC, is built and designed using the wrapper technique to accurately filter features and select effective features for the selected ML algorithm by using the area under the curve (AUC) metric. The algorithm is based on a novel feature selection metric approach, CorrAUC. Afterwards, the author validated selected features for malicious traffic identification in the IoT network using the combined TOPSIS and Shannon entropy based on a bijective soft set.

The IoT is rapidly gaining popularity and is poised to dramatically alter our daily lives. The IoT has many potential uses, such as in healthcare, smart homes, and smart industrial networks. The security of the Internet of Things devices is an ongoing concern due to the fact that these devices produce and process copious amounts of sensitive data. Many people's lives, and the entire planet, could be impacted by a security breach. In contrast, AI is being extensively investigated as a potential security solution for IoT devices, among its many other potential uses. One of the major concerns regarding the security of IoT devices is the possibility of an insider attack. While the majority of studies on Internet of Things security have focused on ways to stop hackers from getting into systems and data, nobody has yet tackled the problem of malicious insider attacks, which can be just as devastating and are often the result of internal exploitation in IoT networks. Consequently, Khan et al. [13] primary objective is to develop AI capable of detecting hostile insider attacks in an IoT setting. In resource-constrained IoT settings, this study introduced a lightweight method for identifying insider threats that may detect anomalies emanating from incoming data sensors.

With its many uses and networked smart gadgets, the IoT has changed the way we live. There are a lot of ways in which these IoT gadgets simplify life by communicating with one another automatically. Security and privacy preservation in the face of malevolent or compromised nodes in the network are two major worries brought up by the autonomy of these devices. An alternative to more conventional methods, such as cryptography, that does not require as much computing power is trust management. A solution to these problems is the FedTrust technique, which uses federated learning to detect compromised and malicious nodes is proposed by Awan et al. [14]. FedTrust uses a dataset that is provided to train edge nodes and create a global model that can detect and predict when IoT nodes are acting abnormally. An innovative trust dataset with nineteen trust parameters derived from three main sources reputation, knowledge, and experience forms the basis of the suggested method. Using the idea of communities with dedicated servers, FedTrust partitions the dataset into smaller pieces for more efficient training, thus reducing the computational strain.

IoT devices are infamously susceptible to compromise, even from very minor attacks. It is also not feasible to secure IoT installations with conventional endpoint and network security solutions due to resource limitations and the variety of IoT devices. Hafeez et al. [15] offered IoT-Keeper, a lightweight technology that encrypts IoT connectivity, to tackle this issue. IoT-Keeper analyzes traffic at edge gateways using the suggested anomaly detection method. The system analyzes network traffic and detects malicious network activity using a fuzzy interpolation approach and fuzzy C-means clustering. In the case that IoT-Keeper identifies malicious activity, it will immediately block the device's network connection so that it cannot harm other devices or services. Using a large dataset gathered from a real-world test bed that includes common IoT devices, the author had assessed IoT-Keeper.

3. COMPARATIVE ANALYSIS

3.1 Secure Routing Protocol in the IoT (SRP-IOT)

For better communication security in the IoT architecture, this traditional SRP-IOT model is considered for analysis for its working process description. With Software Defined Networks (SDN), SRP-IOT establishes a safe channel for data exchange between connected devices. Here, a collection of subnets constitutes the network architecture. Network topology communication will remain stable since members of each subnet will have very similar positions and movement patterns. Additionally, in this setup, a controller node is responsible for authenticating users and overseeing their communication within each subnet. Network traffic is also monitored by a learning model based on neural networks in addition to this communication structure. This learning model is then used by each controller node in its subnet to detect assaults and security concerns.

The working process of SRP-IOT model is:

•Network nodes exhibit non-homogeneous communication characteristics as a result of the many technologies used to manufacture radio equipment in wireless networks. Thus, the presumptive network is not homogeneous.

•The 5G network technology is the basis for the imagined network structure, thus it possesses all the traits and specifications of this communication technology.

•One way to determine how far apart two nodes are is to guess how strong of a radio signal each one received. So, even without GPS, the network nodes can still roughly gauge their distance from one another by measuring the strength of the signals received from other nodes.

•The SDN's learning models enable every controller node to capture and analyze data traffic. The purpose of this Artificial Neural Network (ANN) learning model is to detect security threats and attacks in the subnet associated with the controller node.

The following procedures are included in SRP-IOT to enhance communication security in the IoT architecture based on SDN.

•Network clustering structure formation using software-defined networking.

•Network topology formation based on hierarchical tree.

•Routing data using a pre-existing structure.

A clustering method based on the movement pattern of active nodes divides the SDN domain into numerous sub domains in the first step of SRO-IOT. Each portion of the sub domain is equipped with a controller to exchange security rules with the other parts. As part of SRP-IOT, every controller will share the list of authorized users associated with its sub domain with the others. Thus, the user's credit is accomplished by sending messages between the controllers in the event that two users need to establish communication. Data routing will be completed once both parties have been authenticated by a controller.

The Prims algorithm and minimal spanning tree are employed to manage the topology of the network. Here, the topology of the network is formed locally by each node by

building minimum-spanning trees. The next step in creating a data routing hierarchy is to level the nodes in the network and assign weights to the links between them. After that, the information is guided to its final destination by means of the hierarchical tree structure. According to the proposed architecture of this study, each subnet's controller node acts as an intermediary for all of the nodes' traffic. Consequently, in order to detect assaults, each controller node constantly analyses network traffic data using a learning model. This algorithm, which detects potential attacks in traffic using statistical data retrieved from each flow, is made of three learning models.

3.2 Group Key Management (GKM)

The WSN plays an essential role in the IoT. The processing power, memory, and battery life of sensors are often quite low. Consequently, multicast messages are more energy efficient than sending numerous copies of unicast messages to individual devices, since they are sent to a group of devices instead. One of the most important features for ensuring the confidentiality, authenticity, and integrity of messages is the creation of a secure group key [27]. Protecting a large number of devices is becoming more important as new IoT use cases depend on multicast group communication [28]. To ensure the viability of IoT services in limited contexts, specialized multicast security must be provided. Improving the efficacy of group communication through multicast is possible. This greatly simplifies the process of establishing and administering numerous devices simultaneously.

When a single source talks with multiple recipients simultaneously through a multicast session, numerous potential issues could emerge, including group privacy and key administration [29]. Protecting the session from harm is the group controller is in charge of authentication, authorization, and access control. The role of the key server is to oversee the essential key material. Models for IP multicast transmission have good scalability. The lack of protections to control access or ensure the confidentiality of group discussions is a major drawback of the strategy. With the ability to send data requests to any recipient without involving the sender, the sender has full control over the access controls for membership management. Using IP multicast applications in IoT use cases makes access control more challenging due to the broadcasting nature of the network.

Access management is a top priority for GKM when it comes to security. The encryption and control of group communication is accomplished through the use of a shared secret key, also called a group key. For privacy reasons, group key security is critical [30]. The management of important information changes while speaking to a group as opposed to an individual. It is possible to generate encryption keys during discussions using protocols such as the Diffie-Hellman key exchange protocol, or for one party to generate and provide the key to the other. When a communication fails on either end, the connection is immediately severed and the encryption key is erased, so there's no need to change the key. Making ensuring all allowed groups have the most recent keys is the primary worry, though, due to the large number of receivers in GKM. Even after a member leaves, the group's contact continues unabated, and no one can make them lose the key.

An upgrade is necessary to ensure that former members cannot access any future communication keys. A new group key needs to be generated whenever a user is added to the group. A potential new member can listen in on the group's encrypted conversations before they join. The user must temporarily join the group in order to receive the group key in order to decode the stored data. It is also recommended to replace data encryption keys on a regular basis. Cryptographers do not like it when data is encrypted with the same key for a long amount of data since it leaves the data open to cryptanalysis assaults. Generating, distributing, and updating group keys are now all part of GKM. The achievement of GKM is hindered by the resource limitation aspect of the IoT.

3.3 Detecting malicious nodes in IoT networks using machine learning and artificial neural networks (DMN-ML-ANN)

A technique for detecting malicious nodes using ANNs that could be detrimental to IoT devices is considered for analysis. The first step in the model is to create a representation of the source mote and destination mote of the network. The network is inundated with RREQ notifications when the source is moved. The starting mote determines the Routing Time (RRT) of Route Request (RREQ) and Route Reply (RREP) messages. When the RREQ flood starts, a timer is started at the source and stopped when all nodes have received the RREP; this process calculates the RRT. Each node's RREQ and RREP round journey times are stored in the source route. In order to find the best route to go, the source focuses on balancing two things. Finding the shortest and most sequence-number-maximizing route between two points is ideal. Additionally, the source mole determines the target-to-source distance by factoring in the overall number of hops.

This procedure is carried out in order to detect any malicious entities within the network. Following this, the chosen path between the two sites will be broadcasted by the source mote. When considering the total amount of time required for a data packet to go from its source to its destination, it is important to account for the amount of time it takes for the packet to arrive at each intermediate node. We compare the Round Trip Time (RTT) of the RREP messages with the time spent traveling between the nodes. Particularly among the nodes that transfer data packets with a high degree of timing sensitivity, a few of them have publicly declared themselves to be hostile. The network is protected against the hostile swarm via a multipath routing method. Consequently, the layout of the network will not take the wicked fly's flight path into account.

When developing an ML system, selecting the right features is critical. Initially, a baseline profile is created from raw data packets as they arrive, from which a set of 21 features is extracted—this forms the basis of the malicious node detection method. From these, the six most crucial characteristics are identified. The raw data packets contain an excess of information, including source and destination IP addresses, ports, and protocols, which can introduce noise or overfitting if used directly in the learning process. In the neural network, a dot product using predetermined weights is applied to the test dataset, although this method can introduce bias. Each layer, including hidden and output layers, employs an activation function. The sigmoid function, defined as $(1/(1 + \exp(-x)))$, activates all relationship-associated weights. The effectiveness of node detection depends on the activation function. The training effectiveness of the neural network is assessed using its fourth hidden layer.

4. PROPOSED MODELS

The number of people utilizing the internet has surpassed 3 billion in the past few years, as per a UN assessment. Depicting the use of wired or wireless networking technologies to establish a channel of communication among technologies and networks accessible over the Internet, the Auto-ID Center, a research organization, first used the term IoT ten years ago. There has been a flurry of proposals for routing protocols in the literature, but developing one that is both safe and energy efficient is an ongoing effort. By taking this tack, several routing protocols developed specifically for low-power wireless devices have almost reached their maximum potential [31]. The proliferation of network-enabled gadgets used in people's daily lives, along with the associated limitations on their useful lifespan, has led to the rise of the IoT. For nodes to communicate with one another, routing knowledge is crucial. By collecting and distributing local information, a node should be able to learn, conFigure, and manage itself.

Collaborative effort of dispersed mobile nodes is proportional to trust level. A degree of certainty derived from the actions of nodes is what the term trust alludes to. Based on node behavior, the trust level of the nodes is determined to guarantee secure and proper data transmission in the IoT network. Trust computation in IoT networks is challenging because to the unanticipated changes in network topology, the intricate nature of IoT networks, and the lack of established past trust relationships between nodes [32]. The suggested model has to specify the trust identity factors for all IoT nodes that are ready to transmit data, and each node is assigned a Digital Unique Identifier (DUI). Node authentication is carried out to authenticate legitimate and hostile nodes in the network using the DUI, in the suggested Swift Routing concept with Node Trust Identity Factor (SRM-NTIF) concept. When tested against more conventional approaches, the suggested model outperforms them in terms of both security and trust. The Figure 3 shows the architecture of the SRM-NTIF model.

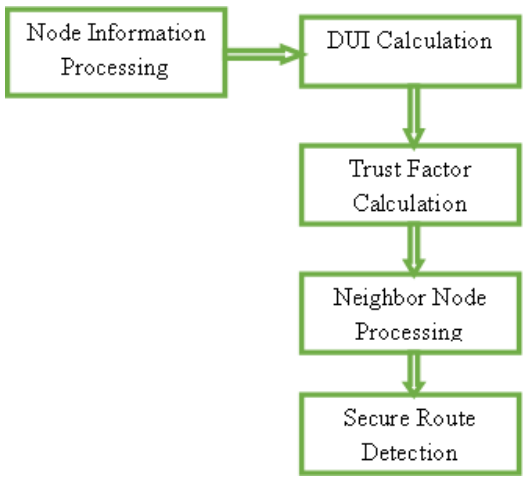

Figure 3. SRM-NTIF architecture

There are growing concerns about privacy and security in the IoT research field, despite its rapid expansion. IoT devices cannot use traditional privacy and security solutions because of their decentralized design and limited resources. The IoT and cryptography, when combined, can make data transmission safe. Every IoT device must undergo authentication before it can be integrated into the network. Encrypted group communication can take place when all devices in the multicast group authenticate with each other. Patients, providers, and payers all need to be able to share and receive information more easily, and there has to be stronger regulation, more consolidation of health practitioners, better data security, and more use of digital patient information.

Faster access to electronic health records is made possible with the help of a multi-key server strategy that distributes the workload evenly among all of the servers, and a new method for managing the keys that improves the security of healthcare information is introduced. A Priority-based Group Key Management with Cryptography Linked Approach (PbGKM-CLA) is suggested to establish a setting for safe data transmission. When it comes to cryptography, the suggested model takes care of key production and distribution. When compared with more conventional models, the results show that the new model works much better. The Figure 4 shows the PbGKM-CLA Architecture.

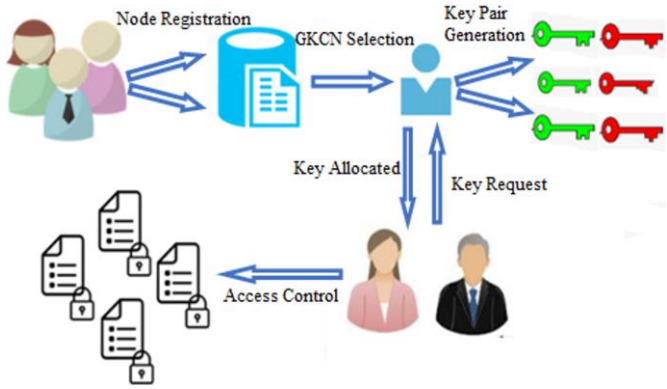

Figure 4. PbGKM-CLA architecture

There are serious security risks due to the increased connectivity brought about by Internet of Things applications. The exponential growth of or IoT, equipment is inversely proportional to the diminishing probability of catastrophic security breaches, especially when malicious signals are present in the network. Every malicious signal is unique, but most of them will change, resend, or destroy data in some manner. Reviewing the received and broadcast messages of each signal is the main focus of an effective method for detecting hazardous signals during these attacks. Obtaining messages for each signal in the network would be time-consuming and a waste of the IoT's limited resources. Efficiency, accuracy, and real-time functionality are the three most important characteristics of a system for identifying dangerous signals.

The standard detection technique is inadequate for establishing an acceptable trust assessment model or designing a trust-based verification model to detect malicious signals because it requires artificial modification in different network contexts. It is possible for malevolent signals in this system to start any number of attacks. For example, a malicious signal could launch a DoS attack by overwhelming the target signal with packets. A machine learning-based neighbor feedback system has been launched by researchers to detect these harmful signals. The suggested technique can aid in the detection of an attacker signal by continuously tracking the signal's trust factor and activating a model when it above a specific level. To accurately detect harmful signals in IoT networks, this research introduces a paradigm called Secured Trust Level Verification with Neighbor Feedback based

Malicious Signal Detection (STVNF-MND). The suggested approach outperforms the conventional model in identifying harmful signals, which in turn increases the network's data transmission rate. The STVNF-MND Architecture is shown in Figure 5.

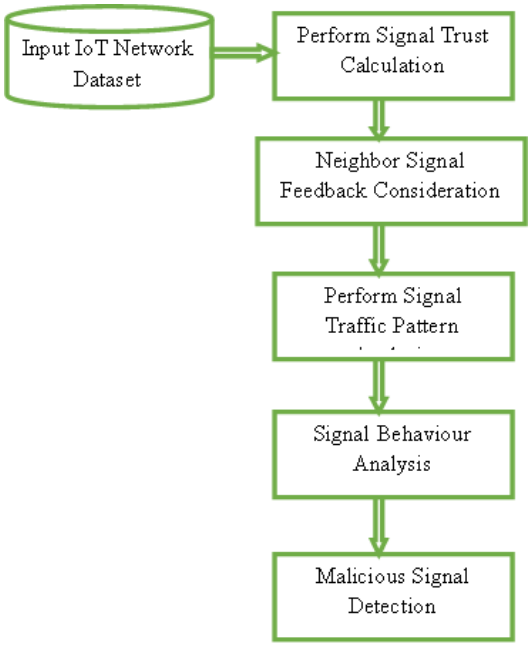

Figure 5. STVNF-MND architecture

5. RESULTS

The discovery of routes between nodes is made possible by the routing protocol, which in turn allows for communication inside the IoT network. In an IoT network, the routing protocol finds the most effective way to send messages at the correct times to different nodes. Overhead usage and bandwidth are kept to a minimum in its design. Through conversation with nearby nodes, the nodes are able to plot a course to their final destination. Weak environmental memory, little computational power, and small communication nodes make up WSN, which detects events and reports them back to a central monitoring device. The fact that the nodes are connected wirelessly opens the door to many types of attacks. Building a foundation that takes into account the security, robustness, authenticity, and authorization of wireless sensor networks is, consequently, crucial.

The IoT is a system of networked, addressable items that may share data and collaborate on larger projects. New developments in wireless communication for distributed systems have greatly altered the future of internet access, which was previously restricted to small devices but is now expanding to high-performance smart ones. Things that are fully functional as part of the IoT concept, middleware uses the information shared by sensors, actuators, and aggregators to guide the behavior of automated systems. The inherent complexity, risk, and unpredictability of the Internet of Things makes the relationships that emerge through communications between things, between humans, and between robots and humans all the more intricate than they initially appear. Due to the increased visibility of the entire IoT network conFigureuration in the public domain and the fact that all interactions are accessible to anyone—including intruders—it is challenging to identify vulnerabilities using conventional methods such as encrypted communication models, operating system security models, and identity models. The most recent, state-of-the-art models necessitate more network bandwidth, battery life, and processing power from IoT devices.

In the IoT, a dynamic distributed network offers services and builds communication protocols among the pervasive smart devices, and various automated algorithms use this data to make judgments. It will be difficult to get from the world of pervasive computing to the benefit of human existence unless specific anticipated problems in this IoT area are resolved. The dispersed and randomly generated nature of the data processed by IoT network components heightens the concerns of those involved in infrastructure security, privacy, trust, data integrity, secrecy, authentication, access control, and device safety. Every one of these contextual factors is crucial to the IoT's success. By incorporating the cryptography model into the IoT healthcare network, the security standards are raised. The suggested SRM-NTIF is compared with the traditional RL-IoT and energy-efficient multilevel SRP-IOT. The PbGKM-CLA is compared with the traditional decentralized lightweight GKM for dynamic access control in IoT environments and ACKE protocol for IoT environments. The STVNF-MND is compared with the traditional Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine-Learning Techniques (CorrAUC) and DMN-ML-ANN.

The proposed model calculates the trust factor of nodes that are used to identify the node properties. The nodes performance measures like packet delivery rate, energy consumption, computational capabilities are considered in trust factor calculation. The Trust factor calculation time levels are indicated in Table 1 and Figure 6.

Table 1. Trust factor calculation time levels

Nodes in the Network	Models Considered		
	SRM-NTIF Model	RL-IoT Model	SRP-IOTModel
50	15.1	22.1	26.1
100	15.3	22.3	26.3
150	15.5	22.5	26.5
200	15.6	22.6	26.6
250	15.8	22.8	26.8
300	16	23	27

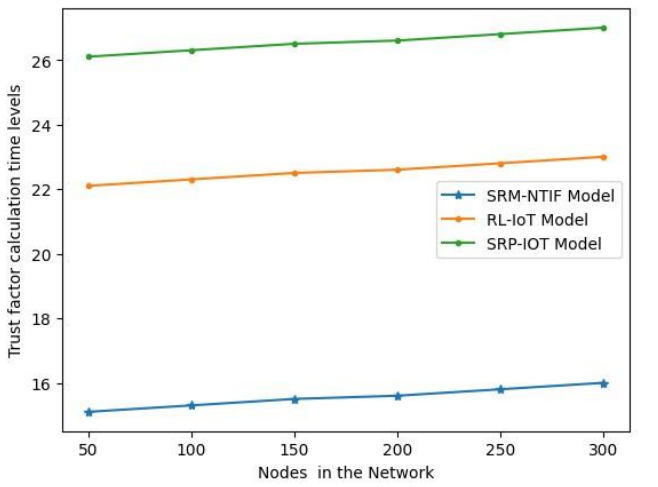

Figure 6. Trust factor calculation time levels

The proposed model performs node validation to check whether a node is a trusted node or a malicious node. The

proposed model node validation verifies the node properties by considering the nodes secret key. The node validation time levels are shown in Table 2 and Figure 7.

Table 2. Node validation time levels

Nodes in the Network	Models Considered		
	SRM-NTIF Model	RL-IoT Model	SRP-IOTModel
50	12.2	16.2	19.5
100	12.4	16.4	19.7
150	12.6	16.6	19.9
200	12.7	16.8	20.1
250	12.8	16.9	20.3
300	13	17	20.5

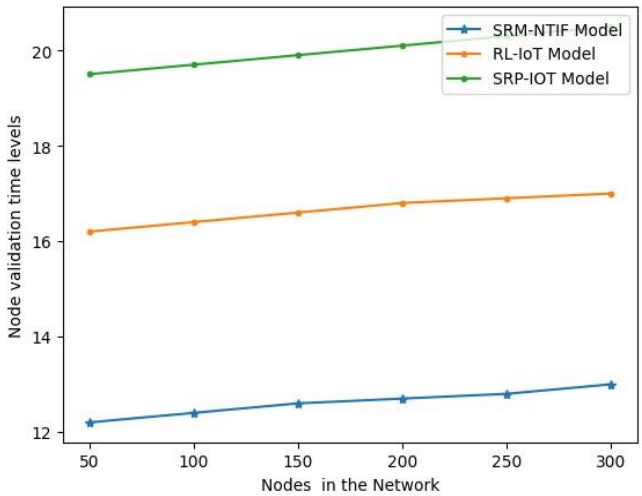

Figure 7. Node validation time levels

Table 3. Packet delivery ratio

Nodes in the Network	Models Considered		
	SRM-NTIF Model	RL-IoT Model	SRP-IOTModel
50	97.9	94.3	93.7
100	98.1	94.5	93.9
150	98.3	94.7	94.1
200	98.5	94.9	94.3
250	98.6	95.0	94.5
300	98.8	95.2	94.7

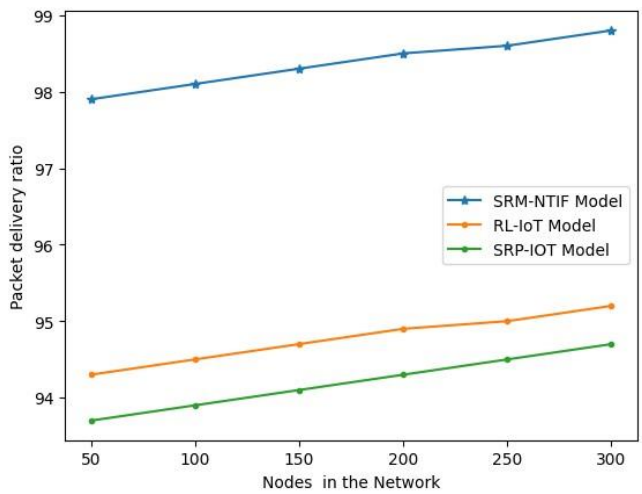

Figure 8. Packet delivery ratio

The total number of packets transmitted from the source node to the destination node in the network divided by the total number of packets delivered is known as the Packet Delivery Ratio (PDR). The maximum number of data packets should be delivered to the destination. The reliability of a network can be measured by its PDR, which is the percentage of packets that are successfully delivered out of all the packets that are sent. Ambient noise, link quality, and energy expenditure are a few of the elements that can impact PDR. The Packet Delivery Ratio are shown in Table 3 and Figure 8.

The proposed model selects the trusted nodes in the routing process. The nodes that are authenticated and are in trusted node category only is considered and updated in the routing table. The trusted route is used to securely transmit the data from sender to receiver. The routing time levels are represented in Table 4 and Figure 9.

Table 4. Routing time levels

Nodes in the Network	Models Considered		
	SRM-NTIF Model	RL-IoT Model	SRP-IOTModel
50	15.0	21.1	27.0
100	15.2	21.3	27.1
150	15.4	21.5	27.3
200	15.7	21.7	27.5
250	15.8	21.9	27.8
300	16	22	28

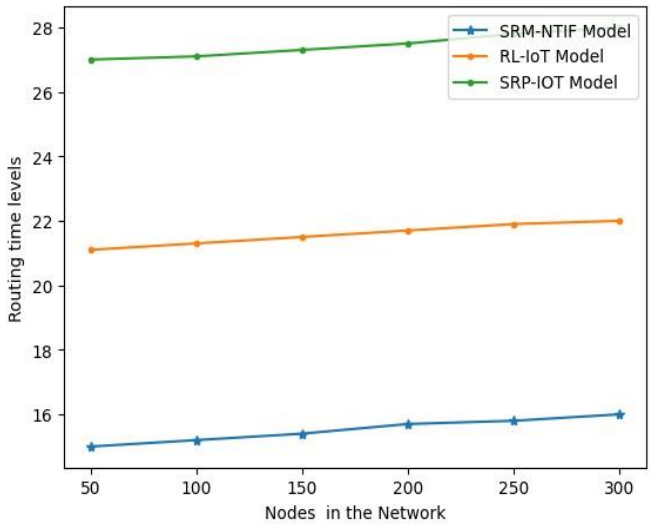

Figure 9. Routing time levels

The proposed model generates the key pairs that are used to identify the normal and malicious nodes in the network. The trusted nodes will use a key in the key pair for node authentication and for initiating data transmission. The key generation time levels are indicated in Table 5 and Figure 10.

Table 5. Key generation time levels

Nodes in the Network	Models Considered		
	PbGKM-CLA Model	GKM Model	ACKE Model
50	11.1	16.1	18.0
100	11.3	16.3	18.2
150	11.5	16.5	18.4
200	11.7	16.7	18.6
250	11.9	16.9	18.9
300	12	17	19

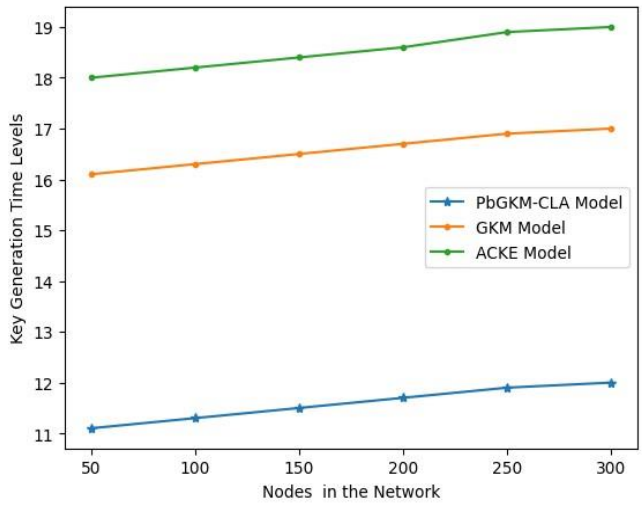

Figure 10. Key generation time levels

Each node is allocated with a priority based on trust factor and the nodes that have highest priority are considered for data transmission. The nodes that are trusted and having high performance metrics are considered as high priority nodes. The priority allocation accuracy levels of the proposed and existing models are shown in Table 6 and Figure 11.

Table 6. Priority allocation accuracy levels

Nodes in the Network	Models Considered		
	PbGKM-CLA Model	GKM Model	ACKE Model
50	97.5	92.8	94.2
100	97.7	92.9	94.4
150	97.9	93.1	94.6
200	98.1	93.3	94.8
250	98.3	93.5	94.9
300	98.5	93.6	95

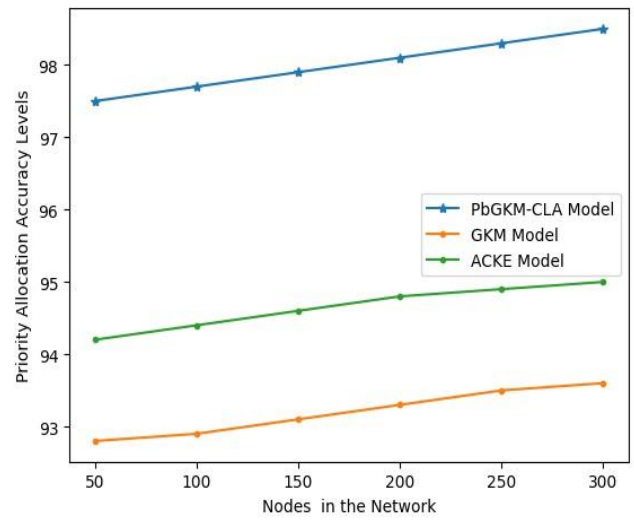

Figure 11. Priority allocation accuracy levels

The proposed model makes use of key pairs to secure the network by authenticating nodes in the network. The proposed model considers only trusted nodes in the network. The nodes are authenticated during transmission process so that normal nodes and malicious nodes can be easily identified. The data security levels are indicated in Table 7 and Figure 12.

Table 7. Data security levels

Nodes in the Network	Models Considered		
	PbGKM-CLA Model	GKM Model	ACKE Model
50	97.7	93.1	92.5
100	97.9	93.3	92.7
150	98.1	93.5	92.9
200	98.3	93.7	93.1
250	98.5	93.9	93.3
300	98.7	94	93.5

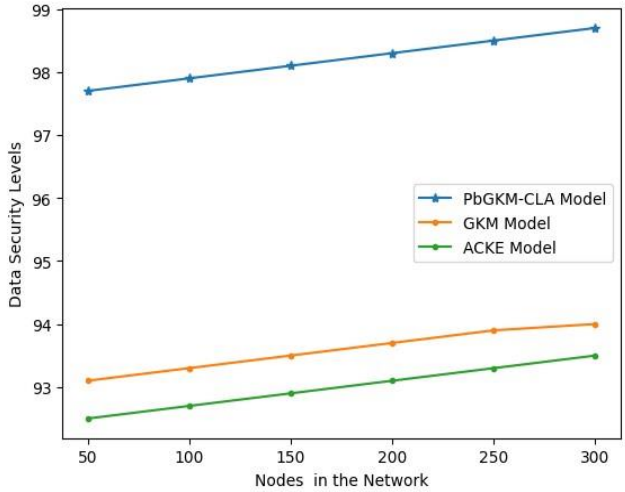

Figure 12. Data security levels

Table 8. Neighbor signal feedback consideration time levels

Nodes in the Network	Models Considered		
	STVNF-MND Model	CorrAUC Model	DMN-ML-ANN Model
50	13.1	20.1	26.0
100	13.3	20.3	26.2
150	13.5	20.5	26.4
200	13.7	20.7	26.6
250	13.9	20.9	26.8
300	14	21	27

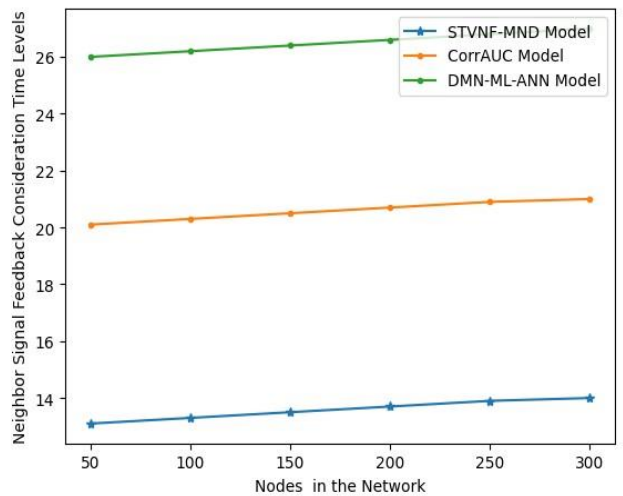

Figure 13. Neighbor signal feedback consideration time levels

The proposed model considers the trust factor of each node to involve them in communication process. The neighbor

feedback is also considered so that node behaviour and performance will be monitored and identified. The neighbor signal feedback consideration time levels of the proposed and existing models are shown in Table 8 and Figure 13.

Table 9. Signal behaviour analysis time levels

Nodes in the Network	Models Considered		
	STVNF-MND Model	CorrAUC Model	DMN-ML-ANN Model
50	12.6	17.6	20.2
100	12.8	17.7	20.4
150	12.9	17.9	20.6
200	13.0	18.0	20.8
250	13.3	18.2	20.9
300	13.5	18.4	21

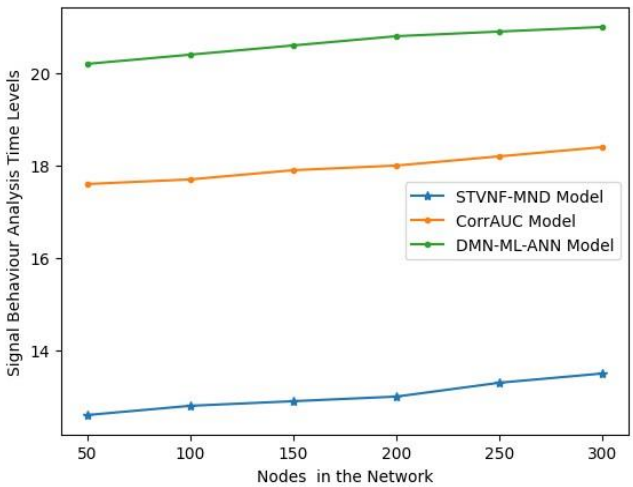

Figure 14. Signal behaviour analysis time levels

Table 10. Malicious signal detection accuracy levels

Nodes in the Network	Models Considered		
	STVNF-MND Model	CorrAUC Model	DMN-ML-ANN Model
50	97.7	93.6	94.3
100	97.9	93.7	94.6
150	98.1	93.9	94.8
200	98.3	94.0	94.9
250	98.4	94.2	95.0
300	98.6	94.4	95.2

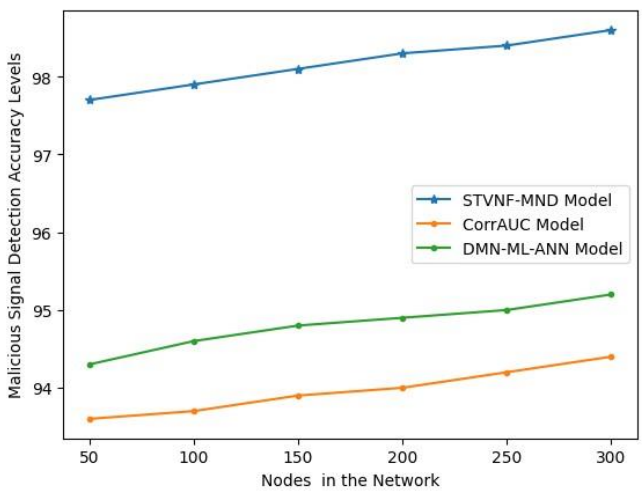

Figure 15. Malicious signal detection accuracy levels

Each signal behaviour is analyzed by monitoring the similarities and changes in the signal patterns. The signal behaviour changes in detection of malicious actions in the network. The frequent signal behaviour analysis is used to enhance the network performance by immediately detecting the malicious signals. The signal behaviour analysis time levels are depicted in Table 9 and Figure 14.

Malicious signals in the network will degrade the performance of the network and also increase the data loss rate. The proposed model accurately identifies the malicious signals based on the node performance monitoring and signal pattern analysis. The malicious signal detection accuracy levels are represented in Table 10 and Figure 15.

6. CONCLUSION

The establishment of a trusted route among the devices becomes more complex due to the association of trust between non-derived nodes, the immoral changes in the network topology, and the dynamic presence of IoT networks, all of which make trust calculation a challenging issue in any network. The network can be more exact because all the connecting IoT nodes have their trust factors determined. A node's trust value needs to be higher than the threshold range before it can be considered to be communicating data. In addition, to fix a problem with the integrated trust calculation's arbitrary weight allocation, a dynamic weight factor is also used. According to the proposed dynamic model of trust, node behavior can be used to accurately and objectively assess trust. Handling erroneous path selection and content alterations are two areas that could use improvement in order to guarantee the safe delivery of network packets. The healthcare industry's Internet of Things applications place a premium on secure group communication. In order for any entity to communicate securely over a network, mutual authentication is a must. Our solution for healthcare IoT network group key management is based on mutual authentication. Individual patient-moving sensor nodes are able to correctly transmit the group key to the gateways. Since the keys are generated in response to requests from healthcare resource servers and healthcare user groups, less space is required by both the key server and the group member. The act of managing cryptographic keys for different groups, including assigning and revoking them, is called Group Key Management. One can construct key pairs that can be utilized for both encoding and decoding. We can lessen the possibility of harmful behaviors occurring within the IoT network by restricting key distribution to authorized users. One effective strategy for identifying harmful signals in these types of assaults is to pay close attention to the messages that each signal sends and receives. It takes a lot of time to get information about each signal in the network, and gathering all of the messages from the network would be too much for the limited capabilities of the IoT. To find a secure way for data to travel between IoT devices, this research looks at the Swift Routing Model, which uses trustworthy nodes as an identifier. For data security, this study takes into account a group key management model, and for malicious node identification, it proposes a technique based on Secured Trust Level Verification with Neighbor Feedback. When compared to the current models, the performance levels of the suggested model are superior. Further enhancements to the trust factor computation and the maintenance of a central authority node for network monitoring are possible in the future, both of

which will increase the network's security.

REFERENCES

[1] Malik, T.S., Malik, K.R., Afzal, A., Ibrar, M., Wang, L., Song, H., Shah, N. (2022). RL-IoT: Reinforcement learning-based routing approach for cognitive radio-enabled IoT communications. IEEE Internet of Things Journal, 10(2): 1836-1847. https://doi.org/10.1109/JIOT.2022.3210703

[2] Zhang, Y., Ren, Q., Song, K., Liu, Y., Zhang, T., Qian, Y. (2021). An energy-efficient multilevel secure routing protocol in IoT networks. IEEE Internet of Things Journal, 9(13): 10539-10553. https://doi.org/10.1109/JIOT.2021.3121529

[3] Zhou, X., Yang, X., Ma, J., Kevin, I., Wang, K. (2021). Energy-efficient smart routing based on link correlation mining for wireless edge computing in IoT. IEEE Internet of Things Journal, 9(16): 14988-14997. https://doi.org/10.1109/JIOT.2021.3077937

[4] Safaei, B., Taghizade, H., Monazzah, A.M.H., et al. (2022). Introduction and evaluation of attachability for mobile IoT routing protocols with Markov chain analysis. IEEE Transactions on Network and Service Management, 19(3): 3220-3238. https://doi.org/10.1109/TNSM.2022.3176365

[5] Patel, N.R., Kumar, S., Singh, S.K. (2021). Energy and collision aware WSN routing protocol for sustainable and intelligent IoT applications. IEEE Sensors Journal, 21(22): 25282-25292. https://doi.org/10.1109/JSEN.2021.3076192

[6] Tian, X., Du, X., Wang, L., Zhao, L., Han, D. (2023). LSLPR: A layering and source-location-privacy based routing protocol for underwater acoustic sensor networks. IEEE Sensors Journal, 23(19): 23676-23691. https://doi.org/10.1109/JSEN.2023.3305544

[7] Dammak, M., Senouci, S.M., Messous, M.A., Elhdhili, M.H., Gransart, C. (2020). Decentralized lightweight group key management for dynamic access control in IoT environments. IEEE Transactions on Network and Service Management, 17(3): 1742-1757. https://doi.org/10.1109/TNSM.2020.3002957

[8] Wang, H., Wen, J., Liu, J., Zhang, H. (2023). ACKE: Asymmetric computing key exchange protocol for IoT environments. IEEE Internet of Things Journal, 10(20): 18273-18281. https://doi.org/10.1109/JIOT.2023.3279283

[9] Sudheeradh, K., Jahnavi, N.N., Chine, P.N., Kasbekar, G.S. (2024). Efficient and secure group key management scheme based on factorial trees for dynamic IoT settings. IEEE Access, 12: 5659-5671. https://doi.org/10.1109/ACCESS.2024.3350780

[10] Yıldız, H., Cenk, M., Onur, E. (2020). PLGAKD: A PUF-based lightweight group authentication and key distribution protocol. IEEE Internet of Things Journal, 8(7): 5682-5696. https://doi.org/10.1109/JIOT.2020.3032757

[11] Subrahmanyam, R., Rekha, N.R., Rao, Y.S. (2023). Authenticated distributed group key agreement protocol using elliptic curve secret sharing scheme. IEEE Access, 11: 45243-45254. https://doi.org/10.1109/ACCESS.2023.3274468

[12] Shafiq, M., Tian, Z., Bashir, A.K., Du, X., Guizani, M. (2020). CorrAUC: A malicious bot-IoT traffic detection method in IoT network using machine-learning techniques. IEEE Internet of Things Journal, 8(5): 3242-3254. https://doi.org/10.1109/JIOT.2020.3002255

[13] Khan, A.Y., Latif, R., Latif, S., Tahir, S., Batool, G., Saba, T. (2019). Malicious insider attack detection in IoTs using data analytics. IEEE Access, 8: 11743-11753. https://doi.org/10.1109/ACCESS.2019.2959047

[14] Awan, K.A., Din, I.U., Zareei, M., Almogren, A., Seo-Kim, B., Pérez-Díaz, J.A. (2023). Securing IoT with deep federated learning: A trust-based malicious node identification approach. IEEE Access, 11: 58901-58914. https://doi.org/10.1109/ACCESS.2023.3284677

[15] Hafeez, I., Antikainen, M., Ding, A.Y., Tarkoma, S. (2020). IoT-KEEPER: Detecting malicious IoT network activity using online traffic analysis at the edge. IEEE Transactions on Network and Service Management, 17(1): 45-59. https://doi.org/10.1109/TNSM.2020.2966951

[16] Yu, H., Zikria, Y.B. (2020). Cognitive radio networks for internet of things and wireless sensor networks. Sensors, 20(18): 5288. https://doi.org/10.3390/s20185288

[17] Lakshman Narayana, V., Lakshmi Patibandla, R.S.M., Pavani, V., Radhika, P. (2022). Optimized Nature-inspired computing algorithms for lung disorder detection. In Nature-Inspired Intelligent Computing Techniques in Bioinformatics, pp. 103-118. https://doi.org/10.1007/978-981-19-6379-7_6

[18] Narayana, V.L., Sujatha, V., Sri, K.S., Pavani, V., Prasanna, T.V.N., Ranganarayana, K. (2023). Computer tomography image based interconnected antecedence clustering model using deep convolution neural network for prediction of COVID-19. Traitement du Signal, 40(4): 1689-1696. https://doi.org/10.18280/ts.400437

[19] Abu Diab, R.A., Abdrabou, A., Bastaki, N. (2020). An efficient routing protocol for cognitive radio networks of energy-limited devices. Telecommunication Systems, 73: 577-594. https://doi.org/10.1007/s11235-019-00628-x

[20] Aslam, M.M., Du, L., Zhang, X., Chen, Y., Ahmed, Z., Qureshi, B. (2021). Sixth generation (6G) cognitive radio network (CRN) application, requirements, security issues, and key challenges. Wireless Communications and Mobile Computing, 2021(1): 1331428. https://doi.org/10.1155/2021/1331428

[21] Hu, Q., Duan, M., Yang, Z., Yu, S., Xiao, B. (2020). Efficient parallel secure outsourcing of modular exponentiation to cloud for IoT applications. IEEE Internet of Things Journal, 8(16): 12782-12791. https://doi.org/10.1109/JIOT.2020.3029030

[22] Li, H., Yu, J., Zhang, H., Yang, M., Wang, H. (2020). Privacy-preserving and distributed algorithms for modular exponentiation in IoT with edge computing assistance. IEEE Internet of Things Journal, 7(9): 8769-8779. https://doi.org/10.1109/JIOT.2020.2995677

[23] Bouillaguet, C., Martinez, F., Vergnaud, D. (2022). Cryptanalysis of modular exponentiation outsourcing protocols. The Computer Journal, 65(9): 2299-2314. https://doi.org/10.1093/comjnl/bxab066

[24] Anitha Josephine, J., Senthilkumar, S., Rajkumar, R., Arun Kumar, C M. (2022). Detection of authorized nodes to provide an optimal secure communication in amalgamated internet MANET. In International Conference on Internet of Things: Third International

Conference, ICIoT 2022, Chennai, India, pp. 93-102. https://doi.org/10.1007/978-3-031-28475-5_9
[25] Farraj, A. (2023). Coordinated security measures for industrial IoT against eavesdropping. In 2023 IEEE Texas Power and Energy Conference (TPEC): College Station, TX, USA, pp. 1-5. https://doi.org/10.1109/TPEC56611.2023.10078577
[26] Rosero-Montalvo, P.D., István, Z., Tözün, P., Hernandez, W. (2023). Hybrid anomaly detection model on trusted IoT devices. IEEE Internet of Things Journal, 10(12): 10959-10969. https://doi.org/10.1109/JIOT.2023.3243037
[27] Benlloch-Caballero, P., Wang, Q., Calero, J.M.A. (2023). Distributed dual-layer autonomous closed loops for self-protection of 5G/6G IoT networks from distributed denial of service attacks. Computer Networks, 222: 109526. https://doi.org/10.1016/j.comnet.2022.109526
[28] Abbasi, M., Plaza-Hernández, M., Mezquita, Y. (2022). Security of IoT application layer: Requirements, threats, and solutions. In International Symposium on Ambient Intelligence, L´Aquila, Spain, pp. 86-100. https://doi.org/10.1007/978-3-031-22356-3_9
[29] Verma, R., Chandra, S. (2023). RepuTE: A soft voting ensemble learning framework for reputation-based attack detection in fog-IoT milieu. Engineering Applications of Artificial Intelligence, 118: 105670. https://doi.org/10.1016/j.engappai.2022.105670
[30] Subramani, S., Svn, S.K. (2023). Review of security methods based on classical cryptography and quantum cryptography. Cybernetics and Systems. https://doi.org/10.1080/01969722.2023.2166261
[31] Ouyang, L., Wang, F.Y., Tian, Y., Jia, X., Qi, H., Wang, G. (2023). Artificial identification: A novel privacy framework for federated learning based on blockchain. IEEE Transactions on Computational Social Systems, 10(6): 3576-3585. https://doi.org/10.1109/TCSS.2022.3226861
[32] Philip, A.O., Saravanaguru, R.K. (2023). Multisource traffic incident reporting and evidence management in Internet of Vehicles using machine learning and blockchain. Engineering Applications of Artificial Intelligence, 117: 105630. https://doi.org/10.1016/j.engappai.2022.105630