International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/217704 Volume 9, Issue 6, November – December (2022)

RESEARCH ARTICLE

A Novel Trust Negotiation Protocol for Analysing and Approving IoT Edge Computing Devices Using Machine Learning Algorithm

V. Maruthi Prasad
Department of Computer Science Engineering, Sathyabama Institute of Science and Technology, Jeppiaar Nagar, Chennai, Tamil Nadu, India.
maruthi.vv@gmail.com

B. Bharathi
Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Jeppiaar Nagar, Chennai, Tamil Nadu, India.
bharathi.cse@sathyabama.ac.in

Received: 20 September 2022 / Revised: 29 November 2022 / Accepted: 03 December 2022 / Published: 30 December 2022

Abstract – In this paper, we come up with an effective approach for the management of security using machine learning, and we derive a solution for problems with privacy and security in Internet of Things devices. Recent apps' connections to numerous IoT devices, use of edge computing, and use of fog computing cause numerous DDoS attacks to be launched against the servers of the dynamic network. For computing on the edge of the Internet of Things, the upgraded Trust Negotiation Protocol is used, making use of better period data. The application of security management is used to maintain the automation, minimize the risk level, and reduce the complexity of the system. The fundamental objective of this system is to enable user-level security in all edge computing devices related to the Internet of Things. Using Machine Learning techniques, a proposed model is utilized to develop a secure environment for E2E IoT security at the user level. A low-cost solution is obtained using machine-learning-based security management techniques. The Enhanced Trust Negotiation Protocol is simulated, and the experiment results demonstrate that the suggested model is superior to the current one in terms of the efficiency with which security management approaches may be implemented.

Index Terms – Secured IoT, IoT Network, Security Algorithm, Trust Protocol, Edge Computing, MLA (Machine Learning Algorithm).

1. INTRODUCTION

The Internet of Things is an upcoming topic in this modern world, which influences all fields such as technical, social, and economic significance. It is a part of our day-to-day life. To imagine how everyday human activity is connected with IoT devices, see Figure 1. It is the whole world connecting all devices through the Internet. It integrates Internet connectivity and powerful data analysis capabilities into almost everything we use on a daily basis, including consumer goods, durable goods, automobiles, trucks, industrial and utility components, sensors, and almost everything else we encounter. This has the potential to completely transform our way of life. One of the most important steps to take into consideration is whether or not to terminate a contract that involves a large number of devices that use a variety of communication protocols [1]. It is difficult to build separate service contracts when many protocols are involved because different protocols are crucial components of any cybersecurity framework for the Internet of Things. It was revealed that a few easy actions need to be followed in order to assist lessen the challenges connected with Internet of Things cybersecurity. This is necessary in order to assure the dependability of the IoT framework in the area of cybersecurity. This was done to guarantee that the IoT framework will be suitable for usage in the cybersecurity industry [2].

It was revealed that a few easy actions need to be followed in order to assist lessen the challenges connected with Internet of Things cybersecurity. This is necessary in order to assure the dependability of the IoT framework in the area of cybersecurity. This was done to guarantee that the IoT framework will be suitable for usage in the cybersecurity industry [3]. The hacking of Internet-connected devices, concerns about being monitored, and anxieties about one's right to privacy are now being brought to the attention of the general public through the headlines of news items. Still, however, the technical challenges are unsettled, and new policy, legal, & development challenges are coming to light. The outline of this paper is to help the Internet society community to know about the IoT's competing vision and its merits and demerits. The IoT leads to a wide range of

RESEARCH ARTICLE

complex ideas and twists from unexpected perspectives. Thus, it is highly essential to secure personal data during IoT communication [4].

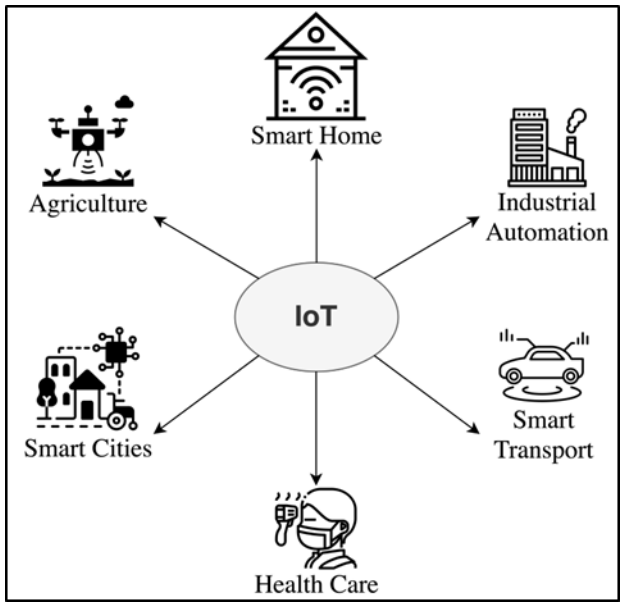

Figure 1 Sample IoT Devices Connected in Human Daily Life

Because of the features of various implementations of the internet of things, new and unique security difficulties are created, which means that the requirement of security is not new in the field of information technology [5]. Facing and ensuring the security challenges in the IoT field should have a priority. Users need to have faith that the Internet of Things devices and related data services are protected from potential threats, particularly given the pervasiveness of this technology in everyday life. Inadequately protected Internet of Things devices and services are the root cause of cyberattacks as well as the loss or theft of data [6]. Because of the linked nature of IoT devices, it is clear that any online-connected item that does not have sufficient security would adversely influence the stability and safety of the internet as a whole [7]. This danger is increasing as a result of the widespread deployment of comparable Internet of Things devices, the ability of certain devices to connect automatically to other devices, and the potential of using these devices in settings that are not adequately protected. The developers and users of Internet of Things devices should have ethics in order to prevent end users and the Internet from being exposed to possible dangers. Therefore, it is necessary to take a holistic approach to security in order to find effective solutions to the difficulties posed by the internet of things [8].

Plans that provide individuals more control over their privacy settings are essential to the success of the Internet of Things. IoT users stand to gain enormous benefits from the data streams and user attention that are made available by IoT devices; nevertheless, full adoption of IoT may be hampered by concerns around privacy and the potential for harm. It implies that users should have rights to their own privacy and reasonable expectations for their own privacy in order to maintain their faith and trust in the Internet and services associated to it. In point of fact, the Internet of Things is reviving arguments about privacy concerns and the widespread use of technologies that will alter the methods in which personal data is gathered, processed, utilised, and safeguarded [9]. The Internet of Things, for instance, has some legitimate concerns over the possibility of increasing monitoring and tracking, and it is resistant to some types of data collecting. No matter what the future may bring, we must never lose sight of these instruments, or their location, for that matter. We need to be aware of what kinds of gadgets we have, what those devices link to, and how they make those connections. When it comes to protecting your business from the Internet of Things in any way, visibility is essential. These points of contact are where attackers will look for vulnerabilities in order to close the gap between the device and the company infrastructure. It has been discovered that there is a need for an effective security model to be applied in the IoT-Edge Computing network [10]. This is the case when security and privacy are considered, as well as the continually expanding number of IoT devices and the data that they generate.

The other parts of the report are structured as follows: Section 2 provides a demonstration of the Literature Review; Section 3 describes the work that is going to be done; Section 4 describes the performance assessment; and lastly, Section 5 describes the conclusion of the report.

2. LITERATURE REVIEW

The whole of the network industry is now going through a significant technical upheaval. The issue of network automation is now popular and has been trending for a considerable amount of time. The Internet of Things (IoT) is a technology that paves the way for providing that element. Then, it is described as the inter-device environment that is built up by the devices that concentrate on three important activities, which are sending, receiving, and processing information. In the beginning, the definition of an Internet of Things network includes Internet-connected devices that were able to do real-time data processing. The scale of the Internet of Things network has expanded over the course of time, going from being comparable to a single workstation to being comparable to a whole industrial framework [11]. The research works on IoT illustrate the expansion of IoT in a variety of domains including education, business analytics, industrial setup, and health care, amongst others. As of 2019, the Internet of Things, which formerly operated in more constrained network areas, has been upgraded to work with wide area networks. This comes with the risks that are

RESEARCH ARTICLE

inherent to wide area networks due to the anticipated increase in the number of IoT devices operating in a diverse setting. The purpose of this research is to explore the latest security solutions in the IoT. Besides this, primary and sub-goals comprise identifying and characterising the modern security risks in the IoT [12].

AI as cluster-based fuzzy logic modules [13], Machine Learning, and Software Enabled Networking [14] have become the new study area for implementing the internet of things (IoT). These are all examples of trending technological disciplines. The deployment of ultra-lightweight protocols [15,16] for the Internet of Things' essential functionality and for reasons of security [17] is a significant advance in the Internet of Things. Regularly, research papers pertaining to the internet of things are made public. When we discuss the security of the internet of things (IoT) in modern times, the primary focus is placed on the hardware-specific security solutions, access control techniques, encryption approaches [18] utilised for transitory phases, and SQL-related input-based attack controls [19,20]. Therefore, the emphasis of our research is placed on the ever-changing security perspectives of the internet of things (IoT). This is accomplished by providing IoT-related security issues with a proper definition and classification, as well as searching for a solution that is currently available to combat them.

Security incorporation into IoT-Edge computing requires first obtaining control of it. Security integrated into the emergence of IoT Edge computing quickly and possibly. It provides a highly flexible and modular architectural model for gaining traction in enterprises around the world [21]. IoT-Edge is described as the same way to add capabilities to IoT devices and systems, and it does not have them. All the IoT-Edge computing devices are interconnected with various models of real-time application, processing, data analytics, and optimization and interact with all the devices [22]. Wireless networks that have the potential of embedded networking are the most recent trend in industry all over the globe. The Internet of Things (IoT) is one of the most important gainers in this networking sector and a substantial advancement achieved by combining Cloud services, which include SaaS, IaaS, and PaaS. Because smart systems such smart home appliances, AI-based smart gadgets, smart home automation, smart cars, smart laboratories, etc. provide convenience of living, the commercial sector has experienced a big increase in the market over the last few years [23]. Despite this, Internet of Things devices have become the new source hotspot for intrusion operations by hackers [24,25]. This is due to the fact that the protocols and standards that are now present on IoT devices are mostly lightweight protocols. On the other hand, entities that make up it have access to the server that is easier to use [26]. These things provide difficulties for the technology since there is no adequate response to the problem of security for the latter.

IoT applications have a significant obstacle in the shape of a growing mountain of data that must be managed and analysed, as the volume of data acquired from various Internet of Things locations continues to increase. Even while enormous data may generally benefit from data compression approaches, there is a possibility that compression will reduce an amount of data that is useless [27]. Big data refers to the information that is compiled from many sources, such as internet communications, mobile devices, social networks, video sharing, sensors and intelligent devices connected to the internet of things, and so on. Big data is characterised by its extensive accumulation of datasets, which focuses primarily on the description of details for the purpose of analysis, manipulation, and efficient storage [28]. Scalable architecture is a prerequisite for big data. The sensors that are dispersed all over the globe as well as the precise gadgets that are connected to the internet Huge volumes of data are being sent to a dispersed storage place when these devices are discovered one by one. In order to make the appropriate choice at the appropriate moment, it is necessary to do an analysis of these facts with the purpose of achieving the appropriate preoccupation [29]. Utilizing data mining techniques and machine learning algorithms is a helpful step in the process of making legitimate selections about people and things. This ensures that you will arrive at the best possible outcomes. The Internet of Things, which infuses enormous volumes of information, necessitates that the parameters of data should be examined and distributed in order to get access to information that is meaningful, relevant, and error-free for the aim of making the best choice and avoiding difficulties [30].

3. PROPOSED MODEL

IoT Edge is Community based only, not owned by any company or entity. It conducts an explosion of experimentation and innovation as the developer focuses on what they do best and lets others do the same. RSA has been involved in the IoT Edge ecosystem from the start and now offers RSA IoT security monitor, cloud-based services that add quality security to IoT Edge platforms. We are pleased to announce that we are extending our community-based with some official partnerships and leading IoT edge companies. Finally, we have developed the RSA Ready Partnership program. The community of RSA includes leading the companies that give expert help for organizations, and they need to manage and design IoT solutions. All of these companies can help manage and implement RSA IoT Security Monitor service to provide thread analytics. New partners are regularly adding. The Euro One is an RSA Ready Partner for all products, now including RSA IoT Security Monitor. It provides complex IT solutions which are defensible in the long run. It offers a wide range of services from business applications and operation support, through infrastructure building and development, to complete IT security solutions.

RESEARCH ARTICLE

IoTech makes systems to develop, deploy, connect and manage IoT systems at the Edge. Its IoT-Edge platform helps you connect and acquire real-time sensor data, run edge intelligence, integrate any cloud with complete deployment flexibility, and manage your edge applications and nodes at scale. Solutions cover the full spectrum of specific hard and soft real-time edge computing requirements. SmartHub delivers complete Edge Device Lifecycle Management (EDLM) for multi-vendor, multi-platform IoT devices and gateways. Its Product Suite improves uptime and reduces risks while supporting IoT and line-of-business priorities. It provides business context for both devices and gateways by inventorying IoT device metadata, including business purpose, importance, alerts, updates, and environment. Infer analyses dataflow and lineage and remediates issues via remote commands or by pushing software updates.

Similarly, TechnoTect helps businesses conceptualize, design, develop, deploy and manage effective industrial IoT solutions. Specializing in intelligent edge services on leading Industrial IoT (IIoT) platforms, TechnoTects architects IoT applications that reduce time to market, increase productivity, and simplify daily operations. With over 20 years of experience across industries, including healthcare, manufacturing, and energy sectors, Technotects has deep knowledge and partnerships throughout the IoT industry, including cloud solutions. Websym provides IoT and Analytics solutions to the manufacturing industry and industrial & consumer OEMs. Its solutions help organizations utilize the power of IoT, big data, and analytics to increase operating margins and improve efficiencies through the real-time generation of actionable insights driven by real-time equipment performance and health data integration with enterprise systems. These partnerships deliver tremendous synergy for organizations that value the benefits of impactful IoT solutions but need a level of security that only RSA can provide. From the introductory part and literature review, it has been identified that the IoT industry still faces more issues and challenges while installation due to the large number of similar devices connected with the same Internet Service Provider (ISP). The RSA used small prime numbers, which are (p, q) very close and helps to observe the input message. People can easily break the RSA-based ciphertexts, applying the **N** factor. The same message broadcasting to multiple people creates Hastad's attack.

Thus, this paper aimed to provide a novel Trust Negotiation Protocol (TNP) to secure IoT-Edge computing applications, where all IoT-Edge nodes are connected in the Net-Chain model.

3.1. Trust Negotiation Protocol

The proposed TNP includes the Net-Chain-based node joining and leaving process, monitoring the node functional behavior, and the authentication and authorization model. The proposed TNP is carried out into two phases such as static and dynamic node behavior analysis. A novel Net-Chain-based model is introduced in the static node behavior analysis to analyze the node that enters and exits the IECN. The functional behavior analysis is carried out in the dynamic node behavior analysis. For example, the TNP analyzes all the nodes entering and exiting the IECN to ensure the nodes are trustable in the first phase. The node-Id, location, type of the node, purpose of the nodes are given in the profile, where it can be verified during the node deployment process. All the investigations of the TNP is illustrated in Figure 2. Each time of communication, the set of all credentials $\boldsymbol{C} = \{\boldsymbol{C_1}, \boldsymbol{C_2}, \dots, \boldsymbol{C_i}, \dots, \boldsymbol{C_K}\}, \forall \boldsymbol{i} = \boldsymbol{1\ to\ K}$, where $\boldsymbol{K}$ varies for different data. If the credential $\boldsymbol{C_i}$ is satisfied, then they are joined in a set $\boldsymbol{S} = \{\boldsymbol{S_1}, \boldsymbol{S_2}, \dots, \boldsymbol{S_i}, \dots, \boldsymbol{S_K}\}, \forall \boldsymbol{i} = \boldsymbol{1\ to\ K}$. Once all the credentials receive Si, then the device can join, participate and leave from the Net-Chain.

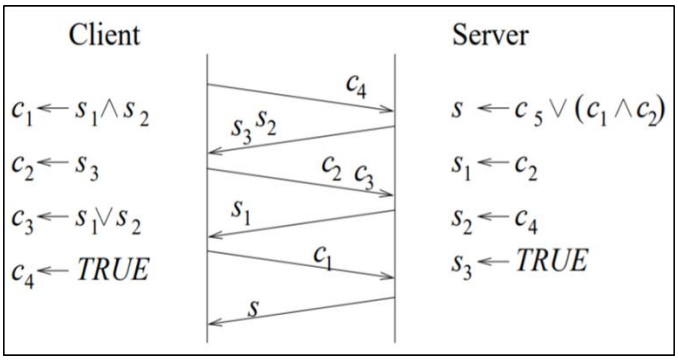

Figure 2 Main Function of TNP

3.2. Net-Chain For IoT-Edge Computing Architecture

Figure 2 presents a visual representation of the Net-Chain (NC) architecture that has been presented. It focuses on the edge layer and proposes a novel architecture for the Internet of Things (IoT) edge that simplifies search and storage while maintaining a high level of security. The newly suggested NC architecture would treat each node in the environment as an entity, regardless of whether it was at the Edge level or the Internet of Things level. As shown in the figure, the nodes are consolidated into what are known as IoT Edge Computing Networks (IECNs), which allows for a reduction in the total number of nodes. However, in addition to the scalability improvements brought about by the grouping of nodes, there are also some fascinating side consequences. The process of collecting nodes will yield one or more fog nodes s a coordinator for a certain IECN.

For instance, there is only one coordinator shown for each IECN in Figure 3. Because this coordinator is seen as representing the whole IECN, any infractions that are committed by members of the IECN are the responsibility of this coordinator. It is required of the coordinator to administer

RESEARCH ARTICLE

the nodes of the member organizations and to represent the IECN within the global Edge community. The global network of fog enthusiasts, also known as Coordinators, is linked together by a Net ring. After obtaining approval from the Cloud Service Provider, Internet of Things devices of any kind may be added to or removed from the Net-Chain at any time (CSP). The CSP is responsible for determining which nodes from the Net-Chain model will be added and which will be removed. When a new node (Ni) joins the IoT-Edge Network (NC), the CSP interview checks the configuration, user profile, and any other limitations that must be met for the node to become part of the network.

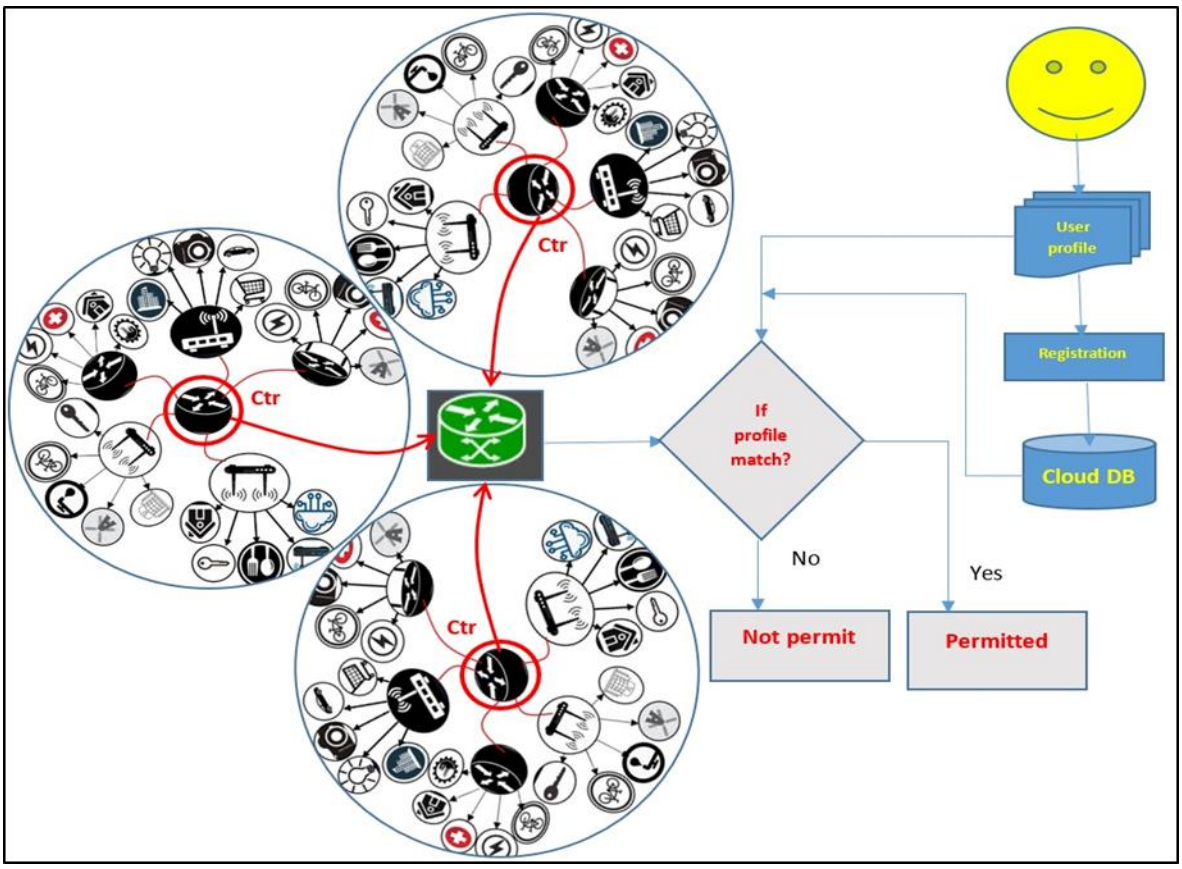

Figure 3 Net-Chain Model for IoT Edge Computing Networks (* Ctr-Controller)

In the next part, in order to create a cohesive and well-running system, we provide a systematic method to defining all system components to fulfil both needs and requirements. This is done in order to accomplish the goal of designing a system that works well. There is a functional architecture as well as an operational architecture included in our suggested technique. These architectures depict the working order of different system components as well as the flow of information between these components. In this section, we explain how our operations are put to use to carry out various duties. The first thing we want to do is demonstrate how the operational profile was derived from the functional profile.

3.3. Functional Architecture

After node deployment and network construction, the nodes in the network are started performing. Each node has been defined with specific functionality and responds under IoT Edge computing admin. For example, an IoT device that belongs to a smart grid performs energy-related functionalities—the IoT device that belongs to communications performs data transmission-related functionalities. While adding a device into the network newly, the complete details like device information, configuration, and user profile are collected and registered in the IoT-Edge network database. It can be verified whenever the admin requires to do cross-verification about the device. Thus, it is ensured that the registration details should be genuine and perfect, else it makes a lot of mismatching and data not available issues.

The functional architecture of the NC-based IoT-Edge Computing architecture that has been presented is shown in Figure 4. The purpose of Net-Chain Model for IoT Edge Computing is to illustrate how distinct levels of architecture are separated from one another in terms of their capabilities.

RESEARCH ARTICLE

Data collection and storage are handled by the fundamental building components of the Internet of Things, which are included under the hardware layer. This layer encompasses a wide variety of devices, from those with a low level of sophistication, such sensors and actuators, to those with a high level of sophistication, like cloud servers. Operating systems for the Internet of Things (IoT) like Contiki and TinyOS handle the physical devices, the processors running on these devices, and the I/O activities. The connection between these devices has to be formed via the communication layer in a way that is safe, efficient, and as cost-effective as possible. The functions of routing, addressing, and forwarding are included in this layer's functionality. Because of the problems posed by the resource-constrained nature of the layer, its design and deployment need careful consideration.

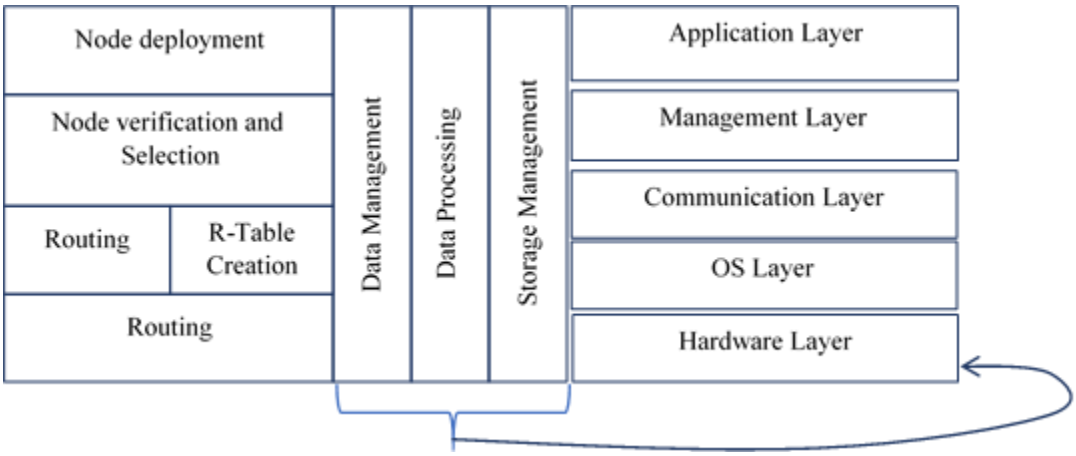

Figure 4 Functional Architecture of the Proposed Chord-Based Fog System

With regard to the logical functions, the private or public key is incorporated with the input data, transported from the application to the node management layer, and then communicated to the data management layer. Logically, the Get() and Set() methods are responsible for deploying both the key and the data. In Internet of Things systems, data sources located at the things layer are responsible for the generation of data items. Because of this, the management layer is essential to the organization of both nodes and data, and it must provide answers to the following questions: The logical structure that exists between the application layer and the management layer is shown by it here. The application layer and the node management layer are able to interact with one another via the usage of an interface. In order to handle IoT data, it makes use of a key-value tuple. Cover the true deeper layers. Keeping the complexity of the implementation in check is one of the goals of this interface. The node management layer is in charge of resolving any and all problems that arise while attempting to manage the dynamic IoT-Edge node environment. IoT-Edge nodes are arranged in a structure that is maintained and may dynamically adjust to accommodate new IoT-Edge nodes when they are added, fail, or depart the system. The data management layer, on the other hand, makes use of IoT-Edge nodes as hash table buckets. This means that each IoT-Edge node saves just a portion of the data that is created. In addition to that, it manages data corruption.

3.4. Functional Behavior

The operational profile, some details like tasks, operational elements, and data flows used to support the entire architecture's functionalities are included. The functional architecture shows both components used in the management named Node and Data management. During the node deployment and communication phase, the following definitions are followed to enhance the efficiency regarding security.

Definition-1: Let D be all IoT devices manufactured by the manufacturer $M = \{M_1, \dots, M_i, \dots, M_m\} \forall\, i = 1\ tom.$ Each device is named as $IoTD = \{IoTD_1, \dots, IoTD_i, \dots, IoTD_m\}$. Most of the time, all the devices are named by the manufacturing company.

Definition-2: A cloud service provider sp_j from $CSP = \{sp_1, \dots, sp_j, \dots, sp_k\} \forall i = 1\ to\ k,$ monitors the services performed by the set of devices logically interconnected with it, is $sp_j^{IoTD_i}$.

Definition-3: The N number of $IoTD \in D$ from various possible domains DO comprises different elements of that network domain like WLAN, WAN, which applies a set of security rules as:

$$NE_1 = WAN, NE_2 = MAN, NE_3 = LAN, NE_4 = VAN\ , and\ etc.$$

RESEARCH ARTICLE

Each rule R of the security concern has n-tuple representing every data field of the IoT data. The set of security rules are given in Table-1.

Definition-4: Every IoTD should follow a security policy P_g, where the g denotes the gateway, which connects more devices and cross-verify the security rules with authentication constraints.

$$P_g = \{R_1, R_2, \dots, R_i, \dots, R_m\}, where\ m > 0, \forall\ i = 1\ to\ m, \ni R_i \neq R_j$$

The set of rules are assigned for N number of IoT devices under various service providers SP. The rules used for the set of entities are given in Table-1.

3.4.1. Node Management

It deals with node discovery, node joining, or leaving dynamically in the IoT-Edge network. It should follow the security rules R. This node management is dependent on the location of the nodes, which both ensures durability and resilience in the event of failures and changes in frequent activities while also decreasing the communication complexity between IoT-Edge nodes. The IoT-Edge nodes are linked with one another in a peer-to-peer configuration, as shown in Figure 3. Because this architecture will be self-managed, there won't be a requirement for centralized management over the network to make sure that the node is either present or absent from the network. The proposed TNP initially focused on creating NC model in the IECN and investigate the node's static data. Investigation compares the data currently feed by the IoTD with the data available in the cloud database (which is persisted during the node registration phase). In addition to the security, rules are verified with the various credentials whenever nodes participate in the network functions.

Table 1 Security Rules

Entities	Rule
Device D, IoTD	Each device is assigned to default and unique name $IoTD_{i,}$ Where the manufacturer M gives the name
Domain DO	Each domain of the devices strictly follows the exact rules applied.
Communication CI	Any device $IoTD_i$can interact with any otherdevices in D
P	The set of all services s={$S_{1,\dots\dots}S_{i\dots\dots}S_t$}, is allowed to each device by the sp_ibased on the CL
RE	Any devices can REQuest any services, but the CSP decides about the service provision

As seen above in Table 1, the IoT-Edge nodes have to come together. Prior to that, the node creation operation should be used to build the nodes. This operation then invokes the distributed hash function to provide each IoT-Edge node a new unique ID by hashing the IP address of the node. After that, it uses the node initialization procedure to initialize its successor and predecessor lists, as well as its finger table. Each node broadcasts a message initially. After broadcasting the data or messages, one neighbor is discovered and added to its neighbor list. Now the node can manipulate the Net-Chain (NC) using NJL interface where it is responsible and act as an interface, care about the node join and leave process. If the node becomes a member of an NC, the node is referred to as the "NC node." If the node rejects the Net-chain of the network, it will reset all the neighbors such as successor, predecessor, and finger table entries and go outside the network, and it can re-join again in place of the NC network. The NC has a lookup process, where it can solve any query. Also, three more operations are performed, such as stabilize, notify, and finger fixing, which is used to maintain good performance through continuous failure and join nodes.

3.4.2. Data Management

The components used in the data management process exploit the network structure established by the node management components to deal with all the tasks related to data allocation, maintaining, and efficiently providing the data pools distributed. Through the get and set operations (see Figure-3), data items are propagated in the NC. The DHT strategy is applied at every IoT-Edge node to describe where the data item will be persisted. The NC is utilized to handle the DHT so that each node will be responsible for keeping only O(log(N)) addresses of other IoT-Edge nodes. The components of the NC system have different functions and services to verify the conformance of the capabilities of the NC devices interconnected through the IoT-Edge infrastructure. The overall functionalities of the NC system are defined here to understand better.

4. PERFORMANCE EVALUATION AND DISCUSSION

The entire proposed and some of the existing models are programmed and simulated using Edge CloudSim Software. The above-explained proposed model ensures the security measures from the node deployment process in the IECN and ensures secured communication by providing authentication and authorization. The proposed TNP protocol is simulated in CloudSim software, and the results are verified. Various parameters are calculated and confirmed in the simulation. For example, the response and service time provided by the TNP is calculated.

Figure 5 shows the average service time obtained using TNP and compared with the other approaches with respect to the number of IoT devices. Service time is the time taken for

RESEARCH ARTICLE

processing the service and network Time. The experiments aimed to improve resource management by minimizing the delays for IoT applications in the Edge-Cloud system. When the system is unloaded, the same performance is happening in all four different approaches. Based on the number of IoT devices, the service time increases in all the approaches, but the service time obtained by the proposed approach is less. The number of IoT devices exceeds 1200 when the service life of the fluorescent algorithm increases. Sonmez algorithm and Utilization-Based have the same performance. It is due to the use of VM Applications in the work policy planning to avoid processing delays and then create in the shortest service time.

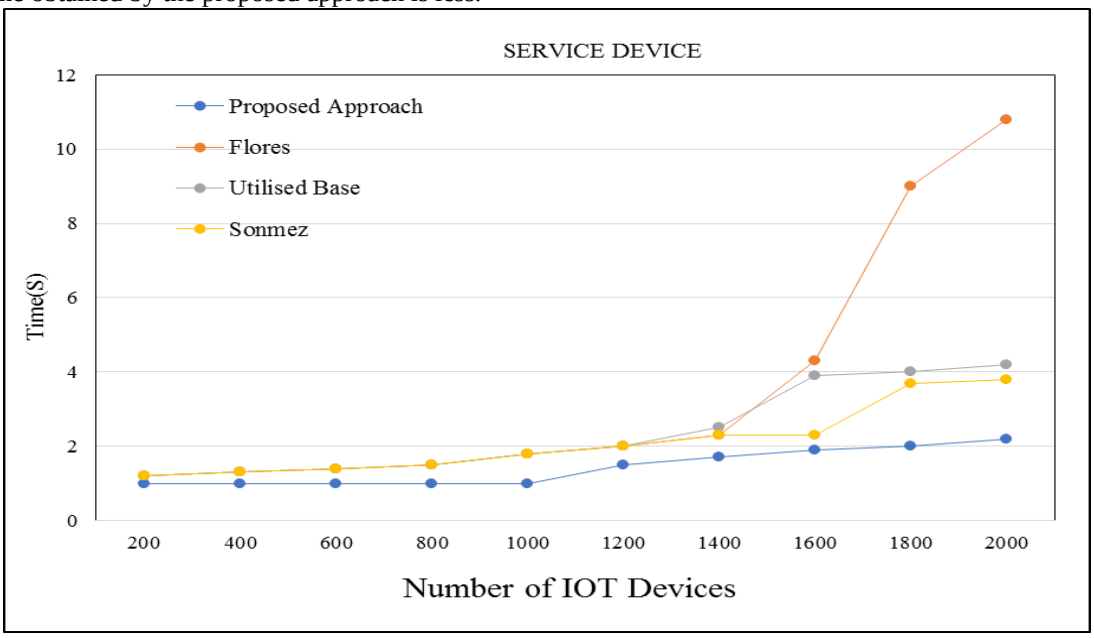

Figure 5 Service Time Comparison

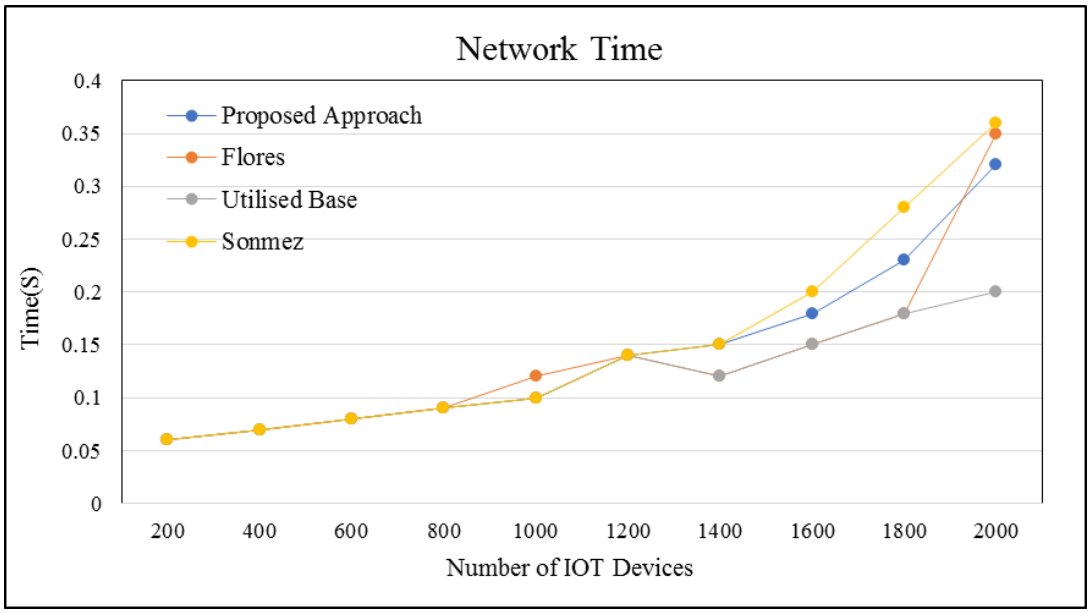

Figure 6 Network Time Comparison

The network time is calculated according to the number of IoT devices in the experiment and given in Figure 6. The network time required in the proposed model is moderate comparing with the other approaches. The TNP requires neither more time nor less time. When the network gets overload, the network time increases to process the requests

RESEARCH ARTICLE

and map the responses. The network time also increases whenever the IoT device is demanding time increases in the cloud. The processing time is calculated for the proposed method and compared with the other approaches. The comparison results are given in Figure 7. The time taken for processing a request or function of any IoTD is called processing time. The obtained result shows that the proposed model took less time for processing the IoT functions. Each device has its defined process, where the time taken to complete its process is estimated in the experiment and compared with one another. From the comparison, it is found that the proposed approach obtained lesser time than the other approaches. The processing time is calculated concerning the number of IoT devices used in the network. It is also noticed that all the approaches have taken more or less similar time, whereas the proposed approach took less time.

Sometimes, processing the IoTD task may fail due to various reasons like lack of resources, inappropriate resource allocation, etc. There may be massive congestion in the simulation due to more IoT devices and increased communication data. Thus, it is essential to analyze the number of tasks get failure in the IECN. It is evaluated by two concerns, such as system stable, and system overloaded. The results obtained for failure tasks estimation are given in Figure 8.

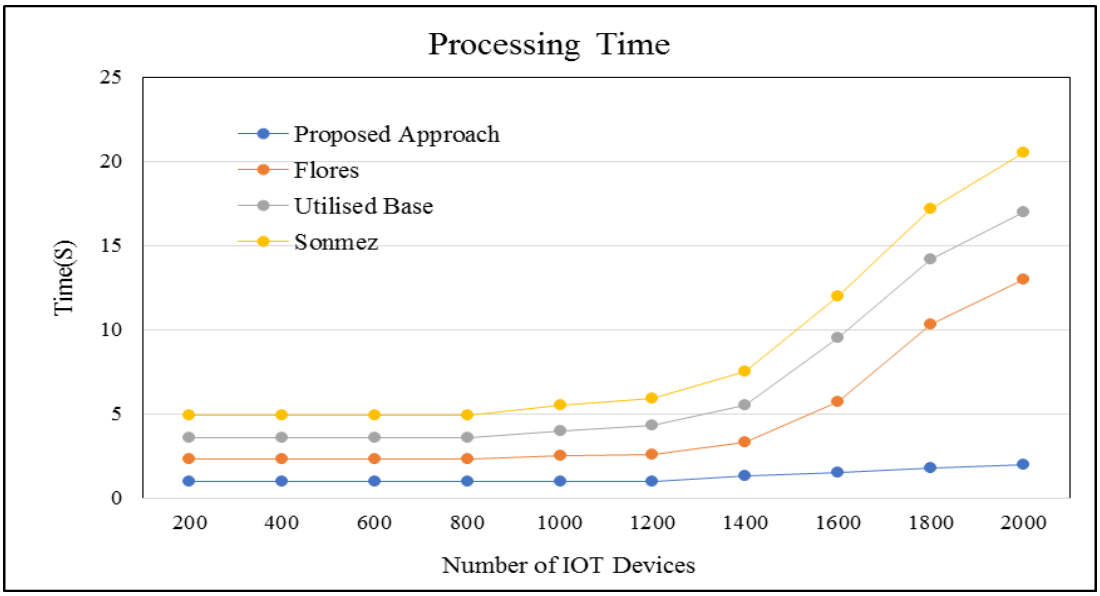

Figure 7 Comparison of Processing Time

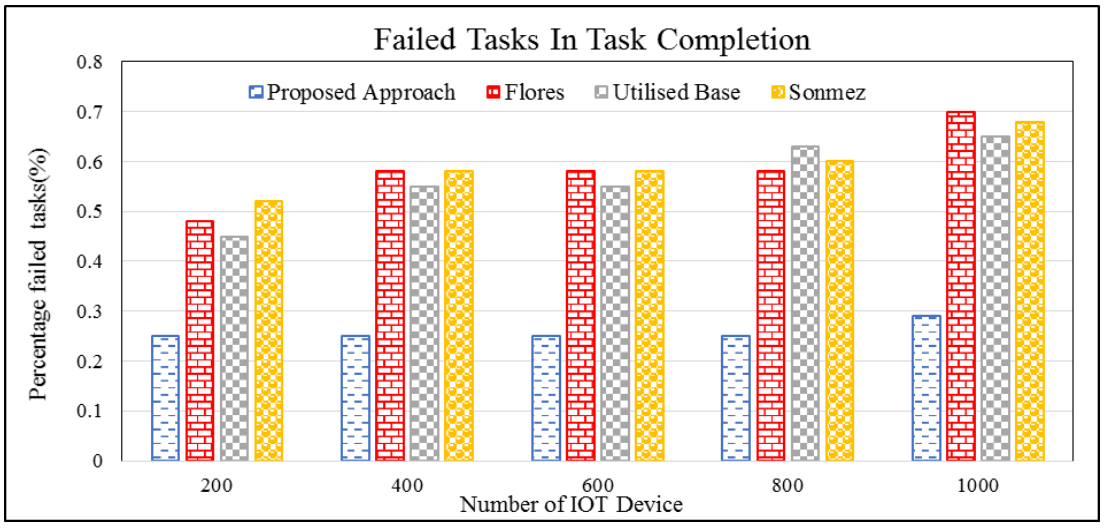

Figure 8 Comparison on Failed Task Estimation

RESEARCH ARTICLE

From above discussion, it comes to know that the proposed approach obtained less percentage of failure than the other approaches. All the existing methods get 0.5% failure in completing their tasks, but the proposed method gets 0.25% failure, which is highly efficient.

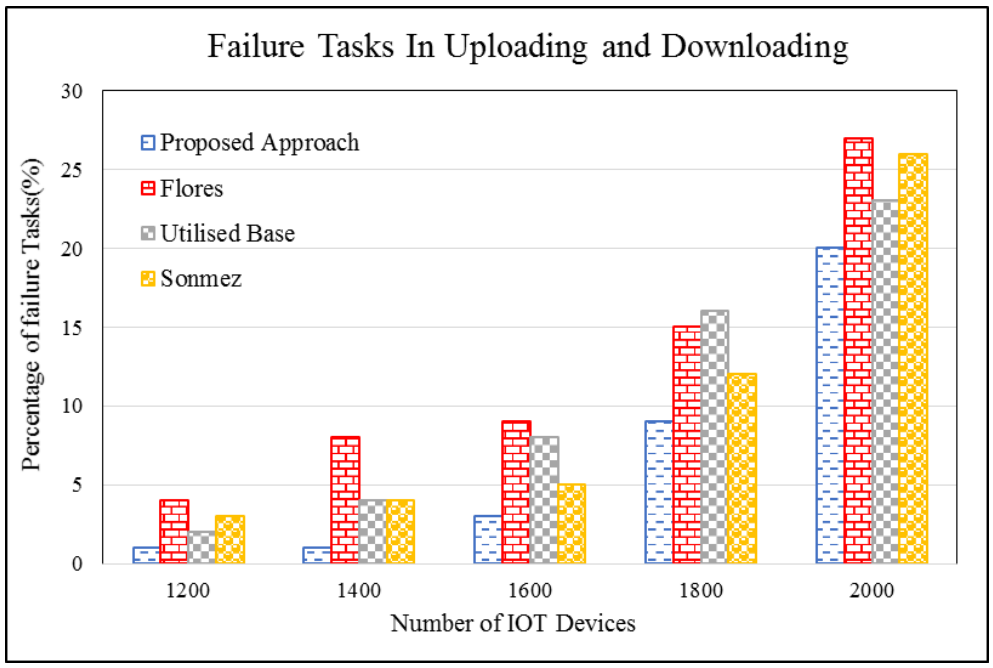

Figure 9 Task Failure Estimation in Terms of Uploading and Downloading

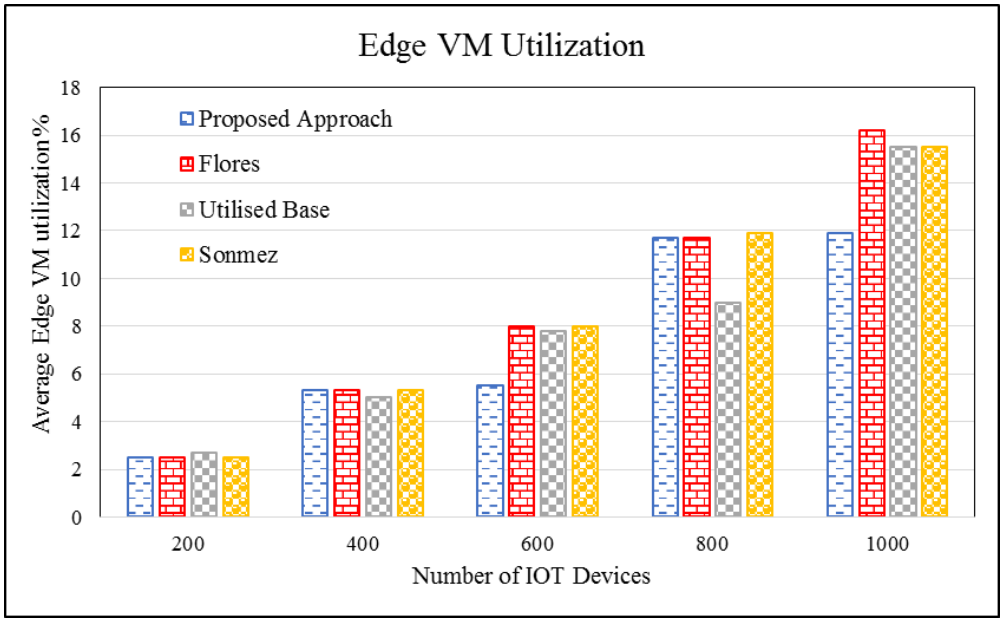

Figure 10 Utilization of Edge Server

Figure 8 shows the % of failure tasks regarding the task file uploading and downloading. The Figure 9 shows that the necessary data is to be uploaded and downloaded using the proposed approach. On the other hand, the minimum average number of task-failure obtained using the proposed method only happens when the system load is high. The proposed approach has minor task failure because it assigns the bulk task to robust Virtual machine allocation. Figure 10 shows

RESEARCH ARTICLE

that if the number of IoTD is 1000 using the Edge System Server, the VM creation and allocation are less. Initially, the average VM allocation concerning the defined number of servers is estimated with the experiment. The obtained result shows that when the number of devices increases, the number of server utilization also increases. Compared to all the other approaches, the proposed approach used the number of servers is less and it is efficient.

Based on the diverse results, The Enhanced Trust Negotiation Protocol is simulated and the experimental results proved that the proposed Trust Negotiation Protocol algorithm is more efficient for security management Techniques compared to the various methods.

5. CONCLUSION

The main objective of this research work is to provide better user-level security for IoT edge computing networks. Though various levels of security provisions are available, the author aimed to provide user-level security as the first stage of the research work. So, a novel Trust Negotiation Protocol (TNP) as an E2E IoT security solution model is designed and simulated for user-level security provision. The proposed TNP examines all the properties and behavior of the IoT devices by implementing a Convolutional Neural Network algorithm and provides approval. The experiment is done in the Edge Cloud Simulator framework, and the results are verified. The proposed algorithm (TNP) performance is evaluated by comparing its impact with the existing algorithms. The comparison shows that the proposed TNP outperforms others and is proved in the results.

REFERENCES

[1] Tawalbeh L, Muheidat F, Tawalbeh M, Quwaider M. IoT Privacy and Security: Challenges and Solutions. Applied Sciences. 2020; 10(12):4102. https://doi.org/10.3390/app10124102.

[2] Carsten Maple (2017) Security and privacy in the Internet of things, Journal of Cyber Policy, 2:2, 155-184, DOI: 10.1080/23738871.2017.1366536.

[3] Mouha, R. (2021) Internet of Things (IoT). Journal of Data Analysis and Information Processing, 9, 77-101. doi: 10.4236/jdaip.2021.92006.

[4] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M.Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347_2376, 4th Quart., 2015.

[5] Khvoynitskaya, S. The History and Future of the Internet of Things. 2020. Available online: https://www.itransition.com/:https://www.itransition.com/blog/iot-history (accessed on 25 March 2020).

[6] Conti, M.; Dehghantanha, A.; Franke, K.; Watson, S. Internet of Things security and forensics: Challengesand opportunities. Future Gener. Comput. Syst. 2018, 78, 544–546. [CrossRef]

[7] Monther, A.A.; Tawalbeh, L. Security techniques for intelligent spam sensing and anomaly detection in online social platforms. Int. J. Electr. Comput. Eng. 2020, 10, 2088–8708.

[8] Makhdoom, I.; Abolhasan, M.; Lipman, J.; Liu, R.P.; Ni, W. Anatomy of threats to the Internet of things.IEEECommun. Surv. Tutor. 2018, 21, 1636–1675. [CrossRef]

[9] Meng, Y.; Zhang, W.; Zhu, H.; Shen, X.S. Securing consumer IoT in the smart home: Architecture, challenges,and countermeasures. IEEE Wirel. Commun. 2018, 25, 53–59. [CrossRef]

[10] Siby, S.; Maiti, R.R.; Tippenhauer, N.O. Iotscanner: Detecting privacy threats in IoT neighborhoods. In Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, Abu Dhabi United Arab Emirates, 2 April 2017; pp. 23–30.

[11] Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. Comput. Netw. 2019, 148, 283–294.

[12] Balamurugan, S., Ayyasamy, A., Suresh Joseph, K., (2021), IoT-Blockchain driven traceability techniques for improved safety measures in food supply chain. International journal of information technology, https://doi.org/10.1007/s41870-020-0058.].

[13] Liu, X.; Zhao, M.; Li, S.; Zhang, F.; Trappe, W. A security framework for the internet of things in the future internet architecture. Future Internet 2017, 9, 27. [CrossRef]

[14] Ali, S.; Bosche, A.; Ford, F. Cybersecurity Is the Key to Unlocking Demand in the Internet of Things; Bain and Company: Boston, MA, USA, 2018.

[15] Antos, M.A., Munoz, R., Olivares, R., RebouçasFilho, P. P., Del Ser, J. and de Albuquerque, V.H.C. (2020). Online heart monitoring systems on the internet of health things environments: A survey, a reference model and an outlook. Information Fusion 53, 222–239.

[16] Culbert, D. Personal Data Breaches and Securing IoT Devices. 2020. Available online: https://betanews.com/ 2019/08/13/securing-iot-devices/ (accessed on 15 September 2019).

[17] Gemalto. Securing the IoT-Building Trust in IoT Devices and Data. 2020. Available online: https://www.gemalto.com/:https://www.gemalto.com/iot/iot-security. (accessed on 17 February 2020).

[18] He, H.; Maple, C.; Watson, T.; Tiwari, A.; Mehnen, J.; Jin, Y.; Gabrys, B. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. In Proceedings of the Evolutionary Computation (CEC), Vancouver, BC, Canada, 24–29 July 2016; pp. 1015–1021.

[19] Boursianis, A.D., Papadopoulou, M.S. and Diamantoulakisetal, P. (2020), Internet of Things (IoT) and Agricultural Unmanned Aerial Vehicles (UAVs) in smart farming: A comprehensive review, Internet of Things, https://doi.org/10.1016/j.iot.2020.100187.

[20] Estrada, D.; Tawalbeh, L.; Vinaja, R. How Secure Having IoT Devices in Our Home. J. Inf. Secur. 2020, 11. [CrossRef]

[21] Sun, Y.; Song, H.; Jara, A.J.; Bie, R. Internet of Things and Big Data Analytics for Smart and Connected Communities. 2016. Available online:https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7406686(accessed on 4 April 2020).

[22] Tawalbeh, M.; Quwaider, M.; Tawalbeh, L.A. Authorization Model for IoT Healthcare Systems: Case Study. In Proceedings of the 2020 11th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 7–9 April 2020; pp. 337–342. [CrossRef]

[23] Balamurugan, S., Ayyasamy, A., Suresh Joseph, K., (2020), Enhanced Petri Nets for Traceability of Food Management using Internet of Things, Peer-to-Peer Networking and Applications..

[24] Wei, X., Zhipeng, Z., Hongxun, W., Yang, Y. and Yanpeng, Z. (2020), Optimization of monitoring network system for Eco safety on Internet of Things platform and environmental food supply chain, Computer Communications, Volume 151, 2020, Pages 320-330, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2019.12.033.

[25] The HIPAA Privacy Rule. Available online: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html (accessed on 19 October 2019).

[26] https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html (accessed on 17 March 2020)

[27] Xiao, L, X. Wan, X. Lu, Y. Zhang and D. Wu, 2018. IoT security techniques based on machine learning. Cryptography Secur. 1: 1-20.

RESEARCH ARTICLE

[28] Chen, F., P. Deng, J. Wan, D. Zhang and A. V. Vasilakos et al., 2015. Data mining for the internet of things: Literature review and challenges. Intl. J. Distrib. Sens. Networks, 2015: 1-14.
[29] M. Trebar, A. Grah, A. A. Melcon, and A. Parreno, "Towards RFID traceability systems of farmed fish supply chain," in Proceedings of the 19th International Conference on Software, Telecommunications and Computer Networks (SoftCOM'11), pp. 6–11, Hvar, Croatia, September 2011.
[30] T. T. L. Tran, L. Peng, Y. Diao, A. McGregor, and A. Liu, "CLARO: modeling and processing uncertain data streams," VLDB Journal, vol. 21, no. 5, pp. 651–676, 2012.

Authors

Mr. V. Maruthi Prasad, Research Scholar - CSE in Sathyabama University, Chennai and Assistant Professor in Dept of CST atMadanapalle Institute of Technology & Science, Madanapalle, Andhra Pradesh. He Completed his Master in Engineering – CSE in Sathyabama University, Chennai. He has a totally 16 years of teaching experience.

Dr. B. Bharathi, Professor and Dean, Academics in Sathyabama Institute of Science and Technology. She has completed her Masters in Software Architectures. She has completed her doctoral research in Performance Evaluation of Software Architectures in 2012.She has a total of 21 years of teaching experience. Published technical research papers in many refereed conference and journals both at the National level and International level. Scopus Index – 76, WoS –20, h-index-8, 4-springer book chapters. Area of Interest is Software Engineering, Predictive Analytics, Artificial Intelligence, and Machine Learning.

How to cite this article:

V. Maruthi Prasad, B. Bharathi, "A Novel Trust Negotiation Protocol for Analysing and Approving IoT Edge Computing Devices Using Machine Learning Algorithm", International Journal of Computer Networks and Applications (IJCNA), 9(6), PP: 712-723, 2022, DOI: 10.22247/ijcna/2022/217704.