Efficient and Secure Data Transmission Approach in Cloud-MANET-IoT Integrated Framework

Anil Kumar Dagar¹, Santosh Kumar Jha², Prangya Padhi³, Priya Chandan Satpathy⁴

¹Department of Electronics & Communication Engineering, Raajdhani Engineering College, Bhubaneswar, Odisha
²Department of Electronics & Communication Engineering, NM Institute Engineering & Technology, Bhubaneswar, Odisha
³Department of Electronics & Communication Engineering, Capital Engineering College, Bhubaneswar, Odisha
⁴Department of Electronics & Communication Engineering, Aryan Institute of Engineering and Technology, Bhubaneswar, Odisha

Abstract

The Internet of Things (IoT) devices have the capabilities to interact and communicate in 5G heterogeneous networks. They also have the capabilities to form a network with neighborhood devices without a centralized approach. This network is called the mobile ad hoc network (MANET). Through an infrastructure-less system of the Internet of Things environment, the MANET enables IoT nodes to interact with one another. Those IoT nodes could interactively connect, communicate as well as share knowledge between several nodes. The role of cloud throughout this structure is to store as well as interpret information through IoT nodes. The communication security has been introduced as one of the techniques to solve the data transmission security issue that could result in increased performance in cloud consumption and ubiquity. The purpose of this research is to establish a communication system among IoT nodes in an embedded Cloud and MANET structure. Aiming to create an efficient and secure approach for communication in Cloud-MANET-IoT integrated framework, this approach has been implemented and tested.

Keywords: Cloud Computing; Internet of Things; Mobile Ad-Hoc Networks (MANET); Smart Devices; Wireless Communication.

I. INTRODUCTION

The IoT connected devices are devices that collaborate and communicate with each other or with other machine. They are expected to increase significantly to approximately 22 billion by 2025 [1]. As shown in Figure 1, the number of IoT connected devices are continuously increasing between 2015 and 2025, although the whole production of IoT devices would not hinge onto the populous of humanity. Although its popularity is increasingly exponentially, one of the most exhaustive issues these devices face is the surveillance and the monitoring of portable devices [2]. The concept of the Internet of things could be defined as "an omnipotent as well as an ubiquitous structure, which further enables monitoring control of a physical planet through gathering, processing, as well evaluating data received from sensors". The IoT framework allows its subscribers to detonate an association to something like a network of computing resources in such a seamless fashion, in which subscribers could rapidly measure high or low requirements to insignificant communication from the supplier. Recently, mobile-based technology has been so popular as the number of connected devices has been rising exponentially day by day [3]. The connected devices are capable of transmitting information to any and all connected devices throughout the network [4]. Figure 2 shows the Cloud-MANET-IoT framework.

Whenever a wireless device does not have adequate information, it communicates the query to its nearby devices. Communication networks protection is the most essential part, which is predicated on cryptography and encryption keys and provides security in intelligent interaction of ad-hoc networks [5]. Connected devices contribute to strengths, such as the context awareness, enhanced processing capabilities, and autonomy from power sources. In 2008, the development of the IoT began by communicating physical things to the World Wide Web [6]. The sensory elements were linked to something like an intelligent repository with a bundle of intelligent data. The structure seems to have the image processing innovation for business as well as consumer verification of both the physical things, buildings, persons, sources, destinations, etc. Then, the IoT shifted from data-based technology to operable-based technology, i.e. IPv4 (man to machine) to IPv6 (machine to machine) [7]. It integrates detectors, connected devices as well as modules like Smart Grid. The growing numbers of detectors and sensor networks are connected to the World Wide Web. Machine-to-machine (M2M) interaction has been the main innovation to sustain sensor data transfer [8]. There are many techniques for transforming integrated M2M interaction paradigms into the proposed systems. In such a broader context, each of the prior end-users will have their issues about weaknesses in cloud services and obstacles that could deter them from accomplishing the goals. The following are the components of IoT: i) Identifiers (ii) Detectors (iii) Surveillance (iv) Calculations (v) Utilities (vi) Terminology, etc.
There are three techniques that have contributed to the development of Cloud-MANET-IoT system. The ubiquitous computation is capable for smart physical things to perform the data transmission among physical devices. The IPv6 is utilizing pervasive computations that cover the area of proposed architecture as well as supporting machine-to-machine talking. IPv4 internet have a disadvantage that adds billions of smart appliances around each other; However, it is feasible in IPv6 internet as it enables the IoT to wirelessly connect billions of smart devices around the world [9]. Association in omnipresent computations used the specified mobility using sensor interconnection. Such techniques must be frequently improved to allow the advancement of smart devices internet including multi-sensor structures to store, calculate, evaluate and own mechanism abilities with smaller size or lower power consumptions [10].

The rest of the paper is organized as follows. Section II represents the related works, Section III represents the methodologies, Section IV represents the data transmission approach in Cloud-MANET-IoT framework, Section V shows the results and discussions and Section VI shows the conclusion.

II. RELATED WORKS

A decentralized based infrastructure is referred to as MANET. The IoT devices form MANET with nearby devices. The MANET is a set of many endpoints that transmit the information, which uses a peer-to-peer mechanism. Therefore, a specifically assigned device is independent of any existing framework, such as wireless devices as well as wireless networks. Although the self-created network is usually helpful to create MANET, the MANET connected with the Internet is significantly more attractive. The Internet is considered as the key part of the daily life of many people by providing an extensive scope of administration. Access points are being used to integrate the MANET and the connected outer spaces.

In the article [11], the authors discuss ways to minimize the limitations connected to IoT deployment and implementation in a smart city environment using a multi mediator scheme. Also, they developed the data transmission scheme in the Vehicular Ad-Hoc Networks (VANET) for the traffic congestion in the smart cities [11].

In article [12], the authors proposed an efficient energy-aware routing scheme for cloud-based MANET in the 5G network. They obtained positive results and demonstrated better performance in terms of less energy consumption compared to previous studies [12].

In article [13], the authors proposed an approach to secure communication in mobile ad-hoc networks of Android devices. In this approach, they developed an algorithm for secure communication in the MANET of smart devices [13]. In article [14], the authors provided the solution of the data transfer securely among the smart devices and IoT based cloud services.

In article [15], the author described the roles of the Cloud-MANET framework in the Internet of Things. They developed an algorithm for secure communication among smart devices. They also compared the previous approaches and obtained positive results [15].

III. METHODOLOGIES

The research contribution ties a special wireless communication approach that uses cloud computing and MANET techniques in the internet of things. The following are the key challenges of the centralized system so that the proposed research is highly needed.

1. It is not simple to set up data from billions of detectors in such a centrally controlled structure of smart devices.
2. Handling computing resources in a wide network that can retrieve environmental data from either the centrally controlled structure is not easy.
3. It is very difficult to control detectors operating the same kind of information similarity and stored in the centrally controlled structure.

Nowadays, smart devices are becoming the requirements of our daily life. These devices could connect with each other. The time is not far away whereas in real-time millions of physical objects will relate to each other [16]. They will interact or send data as well as process their required information onto the cloud [17]. However, there seems to be
a lack of a scientific standardized security point of view on the architecture of IoT. Cloud computing has indeed been regarded as one of the most famous computing concepts. This also resulted from innovations in previous computing frameworks that integrate simultaneous computation, grid computation, distributed computation, and other computing frameworks [18]. Cloud computing offers its consumers with three important features of administration: SaaS, PaaS as well as IaaS. Software as a service (SaaS) is specifically intended for consumers that must use the software as part of their routine practices [19]. Platform as a Service (PaaS) is specifically intended for software developers that need development abilities, interaction, protection difficulties and cyberattacks to smart devices [20]. The author has identified some security issues or attacks in this article. The first threat is the interruption of action due to attacks [21]. Recently, existing attacks in a distributed system could be made accountable for serious security violations. The second challenge would be to reject provider threats. This is given as distinctive, numerous or easy attacks. A challenge occurs if it arrives in differentiating in both the unlawful packet as well as the legal packet [22].

Clearly, such attacks must provide moment cooperation, in which unexperienced cybercriminals could cause them because they only operate easy codes and techniques [23]. As just a matter of fact, packets can pass by the selected providers. Its restraint of these attacks could be attempted via emerging technologies. Any of these innovations seem to be the protection system for the intrusion [24].

The cloud-MANET-IoT layered structure (Figure 3) is a novel methodology in the connected device interaction throughout the Internet of Things that realizes as well as integrates neighboring devices without any centrally controlled technology. The current mobile network would not enable all smart devices to also be linked without centrally controlled technology even though they are very near to one another [25].

The suggested methodology would be very helpful in M2M networks because there are many machines close to one another in the M2M network. Developing the MANET framework integrated with IoT and Cloud could be very effective and beneficial for saving energy and speed performance. Cloud-based services in MANET designed for user-to-device connectivity might be a very valid solution to optimizing the strengths of the smart devices [26]. Consumers of devices will be using cloud storage services to explore devices, reduce valuable information in big data, and that can process videos, pictures, messages, and recordings [27]. Throughout this paper, the author suggested a new structure to improve the ability of smart devices on the Internet for MANET and cloud computing which could be helpful throughout the highly diverse 5G service.

The following procedure is used to connect a device with the Cloud-MANET-IoT framework.

i. Register the IoT node in the clouds. The cloud server will generate the node id as well as login details.

ii. Enter the node id and login details in the clouds.

iii. Install the configuration file on the new connected device.

iv. Start the MANET service on the IoT nodes using this file.

The first threat is the interruption of action due to attacks [21]. Recently, existing attacks in a distributed system could be made accountable for serious security violations. The second challenge would be to reject provider threats. This is given as distinctive, numerous or easy attacks. A challenge occurs if it arrives in differentiating in both the unlawful packet as well as the legal packet [22].

Clearly, such attacks must provide moment cooperation, in which unexperienced cybercriminals could cause them because they only operate easy codes and techniques [23]. As just a matter of fact, packets can pass by the selected providers. Its restraint of these attacks could be attempted via emerging technologies. Any of these innovations seem to be the protection system for the intrusion [24].

The cloud-MANET-IoT layered structure (Figure 3) is a novel methodology in the connected device interaction throughout the Internet of Things that realizes as well as integrates neighboring devices without any centrally controlled technology. The current mobile network would not enable all smart devices to also be linked without centrally controlled technology even though they are very near to one another [25].

The suggested methodology would be very helpful in M2M networks because there are many machines close to one another in the M2M network. Developing the MANET framework integrated with IoT and Cloud could be very effective and beneficial for saving energy and speed performance. Cloud-based services in MANET designed for user-to-device connectivity might be a very valid solution to optimizing the strengths of the smart devices [26]. Consumers of devices will be using cloud storage services to explore devices, reduce valuable information in big data, and that can process videos, pictures, messages, and recordings [27]. Throughout this paper, the author suggested a new structure to improve the ability of smart devices on the Internet for MANET and cloud computing which could be helpful throughout the highly diverse 5G service.

The following procedure is used to connect a device with the Cloud-MANET-IoT framework.

i. Register the IoT node in the clouds. The cloud server will generate the node id as well as login details.

ii. Enter the node id and login details in the clouds.

iii. Install the configuration file on the new connected device.

iv. Start the MANET service on the IoT nodes using this file.

The first threat is the interruption of action due to attacks [21]. Recently, existing attacks in a distributed system could be made accountable for serious security violations. The second challenge would be to reject provider threats. This is given as distinctive, numerous or easy attacks. A challenge occurs if it arrives in differentiating in both the unlawful packet as well as the legal packet [22].

Clearly, such attacks must provide moment cooperation, in which unexperienced cybercriminals could cause them because they only operate easy codes and techniques [23]. As just a matter of fact, packets can pass by the selected providers. Its restraint of these attacks could be attempted via emerging technologies. Any of these innovations seem to be the protection system for the intrusion [24].

The cloud-MANET-IoT layered structure (Figure 3) is a novel methodology in the connected device interaction throughout the Internet of Things that realizes as well as integrates neighboring devices without any centrally controlled technology. The current mobile network would not enable all smart devices to also be linked without centrally controlled technology even though they are very near to one another [25].

The suggested methodology would be very helpful in M2M networks because there are many machines close to one another in the M2M network. Developing the MANET framework integrated with IoT and Cloud could be very effective and beneficial for saving energy and speed performance. Cloud-based services in MANET designed for user-to-device connectivity might be a very valid solution to optimizing the strengths of the smart devices [26]. Consumers of devices will be using cloud storage services to explore devices, reduce valuable information in big data, and that can process videos, pictures, messages, and recordings [27]. Throughout this paper, the author suggested a new structure to improve the ability of smart devices on the Internet for MANET and cloud computing which could be helpful throughout the highly diverse 5G service.

The following procedure is used to connect a device with the Cloud-MANET-IoT framework.

i. Register the IoT node in the clouds. The cloud server will generate the node id as well as login details.

ii. Enter the node id and login details in the clouds.

iii. Install the configuration file on the new connected device.

iv. Start the MANET service on the IoT nodes using this file.

This file is now connected with the mobile application.

v. MANET has started.

vi. Discover the neighborhood IoT devices within the MANET area as well as discover by device id.

vii. Connection established.

viii. Able to Communicate.

IV. DATA TRANSMISSION APPROACH IN CLOUD-MANET-IOT INTEGRATED FRAMEWORK

The Cloud-MANET-IoT structure is an integrated model of Cloud computing and MANET technologies in the Internet of things. The MANET's capability varies depending on the mobility of its clusters as well as on the communication of resources like storage and power efficiency. Cloud service operators maintain communications infrastructure, warehouses, as well as mobile applications that sustain versatility, effectiveness, as well as usability. The following algorithm is used to compute the IoT node velocity in the Cloud-MANET-IoT framework.

\[
\text{Input: Total number of IoT nodes, transmission function value (t).}
\]

\[
\text{Output: Velocity of IoT node.}
\]

\[
\text{Initialization: } \text{Count}=0, \text{Velocity}=0.
\]

Step 1: Discover all IoT nodes in each direction of the selected IoT node.

Step 2: Find a Communication session using the formula.

Step 3: Calculate speed and directions.

Step 4: Calculate transmission function value

\[
(t). \text{Step 5: Find entropy per symbol.}
\]

Step 6: Find Transmission in bits/sec.

Step 7: Find velocity (V) in

\[
\text{MANET mobile devices could interact with one another in the Cloud-MANET-IoT framework, but at least one smart device should be tied to wireless or Wi-Fi networks. All MANET smart devices will be independently enrolled in the cloud. The proposed system would be accessed in the disjointed style. Whenever a MANET is detected, cloud providers would trigger in real-time as well as provide services to MANET's devices. The smart devices submit a report to the cloud for a communication session. Cloud offers better interaction with smart devices. Communication life is defined as a mathematical function in equation (1) as follows.}
\]

\[
\text{Communication Session (life)}
\]

\[
= \frac{1}{2n \times \text{maximum entropy}}
\]

\[
(1)
\]

IJESPR

www.ijesonline.com
The integral expression would be 0 whether the limit tends to be as high as 0. Since computation session life using the above deterministic function, every device involves computational the values of $\pi$ and $\mu$. Such two variables are connected to the link established between MANETs and cloud service which could be calculated and used the preceding function via connected devices, $e^{\mu(t)}m^2$.

Whenever a smart device estimates the communication life among MANET and Cloud, this will efficiently transfer or receive information. A link would be triggered and there is high stabilization. They considered that when generating a cloud session, every smart device is guaranteed of creating the path around MANET and Cloud. Using the Gauss-Markov utility system, the electronic devices could start moving from one area to the next area via the velocity of 20 meters per second. The next equations (2) and (3) can be used to measure the move of the smart device velocity inside the MANET scope.

$$\text{Speed}(t) = \text{Speed}_{t-1} + (1 - \delta)\sqrt{\frac{D}{D_{t-1}}}$$

(2)

$$\text{Direction}(t) = \text{Direction}(t - 1) + (1 - \delta)\text{Direction}_{t-1}$$

(3)

The $\delta$ is a random degree if computational velocity and the trajectory of the smart device in such a period (t). During the time interval $[t_i, t_{i-1}]$, the transmission ($t_i$) of data ($I_k$) between the number of smart devices could be calculated. Within the MANET, the smart devices could start moving as well as connect directly the cloud storage service using the multifaceted function (t) in equation (4).

$$t = C, S, k, I_k$$

(4)

where: $k = 0, 1, 2, 3 \ (\in (+ve))$

When electronic devices start moving outside of the MANET, after which k will be a negative number. Here, they recognize that somehow the transition of data takes place concurrently. We understand that the probability becomes proportional to the inverse data, $p_i$ a $\frac{1}{t_i}$.

The probability density function for transmission is calculated mathematically as follows.

$$P(S_i, I_i, t) = 1 - \sum_{q=0}^{M} \left( \sum_{r=0}^{n} \left( \sum_{k=0}^{\infty} \frac{\left( \frac{\delta}{\sqrt{1 - d^2}} \right)^{I_k} \Gamma_{\delta}(I_k)}{1 - d^2} \right) \right)$$

(5)

where: $\delta = 1$

So, we have divided the probability density function of all associations that used the entropy per symbol for all smart devices of 3-dimensional locations.

$$H_{x,y} = \sum_{k=0}^{m} \left( \sum_{k=0}^{n} \left( \sum_{k=0}^{\infty} \left( \frac{\left( \frac{\delta}{\sqrt{1 - d^2}} \right)^{I_k} \Gamma_{\delta}(I_k)}{1 - d^2} \right) \right) \right)$$

(6)

Here $\sum_{k=0}^{m} S_{x,y}$ the Chi-Square distribution method that is used for congruence. Now, we will measure all the probabilities, entropies for each direction as well as finally, create the transition matrix from the probabilities of all smart devices.
Transmission in MANET of Smart Devices at 5 m/s

<table>
<thead>
<tr>
<th>Devices</th>
<th>t=0.1</th>
<th>t=0.2</th>
<th>t=0.4</th>
<th>t=0.6</th>
<th>t=0.8</th>
<th>t=1</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1.2</td>
<td>1.5</td>
<td>1</td>
<td>1.3</td>
<td>2</td>
<td>1.8</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>2.4</td>
<td>2.6</td>
<td>2.8</td>
<td>3</td>
<td>2.9</td>
</tr>
<tr>
<td>25</td>
<td>4</td>
<td>3.7</td>
<td>4.1</td>
<td>3.8</td>
<td>3.9</td>
<td>3.7</td>
</tr>
</tbody>
</table>

Transmission in MANET of Smart Devices at 10 m/s

<table>
<thead>
<tr>
<th>Devices</th>
<th>t=0.1</th>
<th>t=0.2</th>
<th>t=0.4</th>
<th>t=0.6</th>
<th>t=0.8</th>
<th>t=1</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1.1</td>
<td>1.4</td>
<td>1.2</td>
<td>1.5</td>
<td>1.4</td>
<td>1.8</td>
</tr>
<tr>
<td>15</td>
<td>3.1</td>
<td>1.9</td>
<td>2.7</td>
<td>1.4</td>
<td>1.9</td>
<td>2.3</td>
</tr>
<tr>
<td>25</td>
<td>2.9</td>
<td>2.8</td>
<td>3.8</td>
<td>3</td>
<td>2.6</td>
<td>2.8</td>
</tr>
</tbody>
</table>

Transmission in MANET of Smart Devices at 25 m/s

<table>
<thead>
<tr>
<th>Devices</th>
<th>t=0.1</th>
<th>t=0.2</th>
<th>t=0.4</th>
<th>t=0.6</th>
<th>t=0.8</th>
<th>t=1</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1.2</td>
<td>1.3</td>
<td>1.8</td>
<td>1.4</td>
<td>1.2</td>
<td>1.8</td>
</tr>
<tr>
<td>15</td>
<td>2.2</td>
<td>3</td>
<td>3.2</td>
<td>2.6</td>
<td>2.8</td>
<td>3</td>
</tr>
<tr>
<td>25</td>
<td>3</td>
<td>3.4</td>
<td>2.9</td>
<td>2.4</td>
<td>3.1</td>
<td>2.6</td>
</tr>
</tbody>
</table>

VI. CONCLUSION

The Cloud-MANET-IoT framework has the ability to play an important role in diverse 5G communication. The framework has been developed to enhance interaction efficiency. It was found that the cloud framework was predicated on such a diversified structure, many precautions or security risks linked to disbursed concepts are acquired. Data transmission security issues or obstacles which depend on behind cloud computing were enticed. Moreover, many of these excessive risks has strengthened in most of the cloud framework. The security requirements as well as communication security problems between all connected devices throughout the cloud services were also analysed. The proposed framework has been constructed, implemented and tested.

REFERENCES


M. Aljohani and T. Alam, "Design an M-learning framework for smart learning in ad hoc network of Android devices," 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, 2015, pp. 1- 5. DOI: https://doi.org/10.1109/ICCIC.2015.7435817

