Research Case Study: Design and Development of secure and energy efficient techniques for IoT Device

[1]Binod Kumar, [2]Dev Ras Pandey,[3]Mohit Kumar, [4]Sidharth Prakash, [5]Shrikant Upadhyay

[1]Kalinga University Raipur, [2]Kalinga University Raipur, [3]MIT Art, Design and Technology University, Rajbaug, Pune, [4]Swarnrekha group of Institutions, [5]Department of Electronics and Communication Engineering, Cambridge Institute of Technology, Ranchi, Jharkhand

[1]bit.binod15@gmail.com, [2]dev.ras.pandey@kalingauniversity.ac.in, [3]mohit.kumar@mituniversity.edu.in, [4]siddharthprakash101@gmail.com, [5]shri.kant.yay@gmail.com

DOI: 10.31838/ecb/2023.12.si6.092

Abstract

The development of design of Safe and Energy Effective Methods for IoT Devices initiative is a great effort to solve the crucial challenges of Safety and Energy Effective for IoT Devices by using Cisco Packet Tracer. The rise of IoT devices has made it essential to protect them from online attacks. Also, IoT devices have to be fuel efficient in order to function properly because they frequently depend on batteries. The major goal of the project was to create and put into use an IoT device that was safe and energy-efficient utilizing Cisco Packet Tracer. To ensure the security of the device, the project made use of a number of security measures, including the implementation of secure passwords, the use of encryption methods, and the configuration of firewalls. Energy-saving techniques including using low-power hardware, simplifying the software, and implementing sleep modes significantly improved the usefulness of the device. Overall, the study was successful in achieving its objectives and demonstrated that adding security and power generation capabilities to IoT devices is doable. The project's outcomes might be used to improve the energy efficiency as well as safety of emerging IoT devices as well as industry best practises. The project's success illustrates the importance of addressing security and efficiency issues in IoT devices as well as the requirement for more research in this area. IoT devices must be maintained secure, reliable, and energy-efficient because they're crucial to our daily lives and are employed in increasingly crucial infrastructure. In this specific project, the whole idea of energy-efficient and secure solutions for IoT devices has already been covered in detail, alongside all the relevant information and references that may offer accurate data about all things. Every approach that is depicted in this project is explained in the methodology section. These techniques will be used to create a variety of high effective and energy-efficient purpose.

Keywords: IOT Devices, Energy management, WSNs , ML, AI

1. Introduction

The Internet of Things (IoT) has grown into an essential part of our everyday lives, featuring a wide range of products connected to the web, from wearable and home automation to automated factories. Yet, new issues including potential threats and energy inefficiencies have emerged due to the growing use of IoT devices. Designing and creating safe and resource-saving methods for IoT devices has become more crucial due to these issues. The requirement for safe communication, as well as data security, becomes more critical as the amount of Internet of Things devices keeps growing. The lack of built-in security features in many IoT devices leaves them open to attacks that may jeopardize consumer privacy or even result in bodily injury. As a result, it is crucial to conduct research on methods for ensuring safe communications and data security for IoT systems.

IoT device fuel efficiency is a significant hurdle in addition to safety issues. Several of these gadgets are dependent on batteries that, if not properly handled, can rapidly deplete. This may lead to shorter device lifespan, more frequent repairs, and higher user expenditures. Thus it's essential to find energy-efficient methods to reduce the energy usage of IoT devices. Both of these issues are going to address by the project "Design and Development of Secure and Energy Efficient Techniques for IoT Device," which develops strategies to provide secure communication and data security while maximizing the energy usage of IoT devices. The initiative entails the creation of techniques, protocols, and procedures that allow safe communication among Internet of Things (IoT) devices and the network that they are connected to, as well as strategies to decrease the energy use of these equipment. To assure the usefulness and effectiveness of the established approaches, the program also will comprise testing and assessment.

2. Aim and Objectives

2.1 Aim

The aim of this project is to examine the many methods and strategies that may be applied to improve the energy efficiency as well as safety of IoT devices through Cisco packet tracer. This entails researching the dangers and vulnerabilities posed by IoT devices in addition to creating plans to lessen these dangers. Also, this project tries to look into ways to lower energy usage without sacrificing IoT device performance.

2.2 Objective

- Analysing the security threats and vulnerabilities of IoT devices and identifying potential risks.
- Developing secure communication protocols and data encryption techniques to ensure the confidentiality and integrity of data transmitted by IoT devices in Cisco packet tracer.
- Investigating the use of block chain technology to enhance the security and transparency of IoT devices.
- Exploring energy-efficient techniques for IoT devices, including low-power hardware and software optimization.

3. Project Specifications

This project is going to accurately design as well as develop various secret techniques for all the IoT devices out there with the help of Cisco packet tracer as it is going to provide all the necessary elements that are important for that. Through these projects, it is also necessary to critically analyse the whole environment in the most appropriate way so that it becomes very easy to understand all the technology that is directly connected with the IoT devices and which can be honourable in different situations. Define security techniques along with the energy efficiency technique of IoT devices is also going to be explained with appropriate integration of security and another execution process. This project is going to clearly specify all the important and necessary activities that are required to implement for better secure connection of all the IoT devices and which can provide very basic and effective features to all the users out there. The proper understanding of secure key management inside IoT devices and the importance of efficient techniques that are secure is also going to evaluate with proper information and data. The overall design and development of IoT secure devices are going to be analysed with the help of a Cisco packet tracer and the result is going to be evaluated with appropriate techniques and methods.

4. Literature Review

4.1 : Security Techniques for IoT device

IoT device design and development must take security seriously. IoT devices are vulnerable to security breaches because of their constrained processing and storage capabilities as well as their widespread use. IoT device security is essential for preventing cyber-attacks, which might result in serious repercussions including data loss, privacy breaches, and even bodily injury.

Encryption is one of the security methods for IoT devices that are most frequently utilized. Data may be protected both while it is in transit and while it is at rest by using encryption to scramble it so that only authorized individuals can access it (Xiao *et al.* 2018). [23] Access control is another frequently used method that uses authentication and authorization techniques to guarantee that only those with the proper permissions may access the device or its contents. Firewalls, intrusion detection and prevention systems, secure boot, and firmware update procedures are further IoT device security measures. Incoming and outgoing network traffic may be filtered using firewalls, and unwanted access attempts can be found and stopped using intrusion detection and prevention systems (Liao *et al.* 2020). [11] IoT devices are kept up to date with the most secure software versions thanks to procedures for secure boot and firmware updates.

Other methods, such as edge computing security, and block chain-based security, are developing in addition to these conventional security measures. Although edge computing security uses local devices to execute security duties and lessen the strain on centralized servers, block chain-based security offers a decentralized and tamper-proof method of authenticating transactions and maintaining data integrity. IoT device security still faces a number of obstacles despite the availability of various security methods. The absence of established security protocols is one of the main issues since it makes it difficult for device manufacturers to incorporate security features consistently (Alladi *et al.* 2020). [3] In order to prevent people from embracing IoT devices, too complicated security methods must be balanced with usability and convenience. To guarantee the security and integrity of IoT devices and the data they gather and send it is essential to address these concerns.

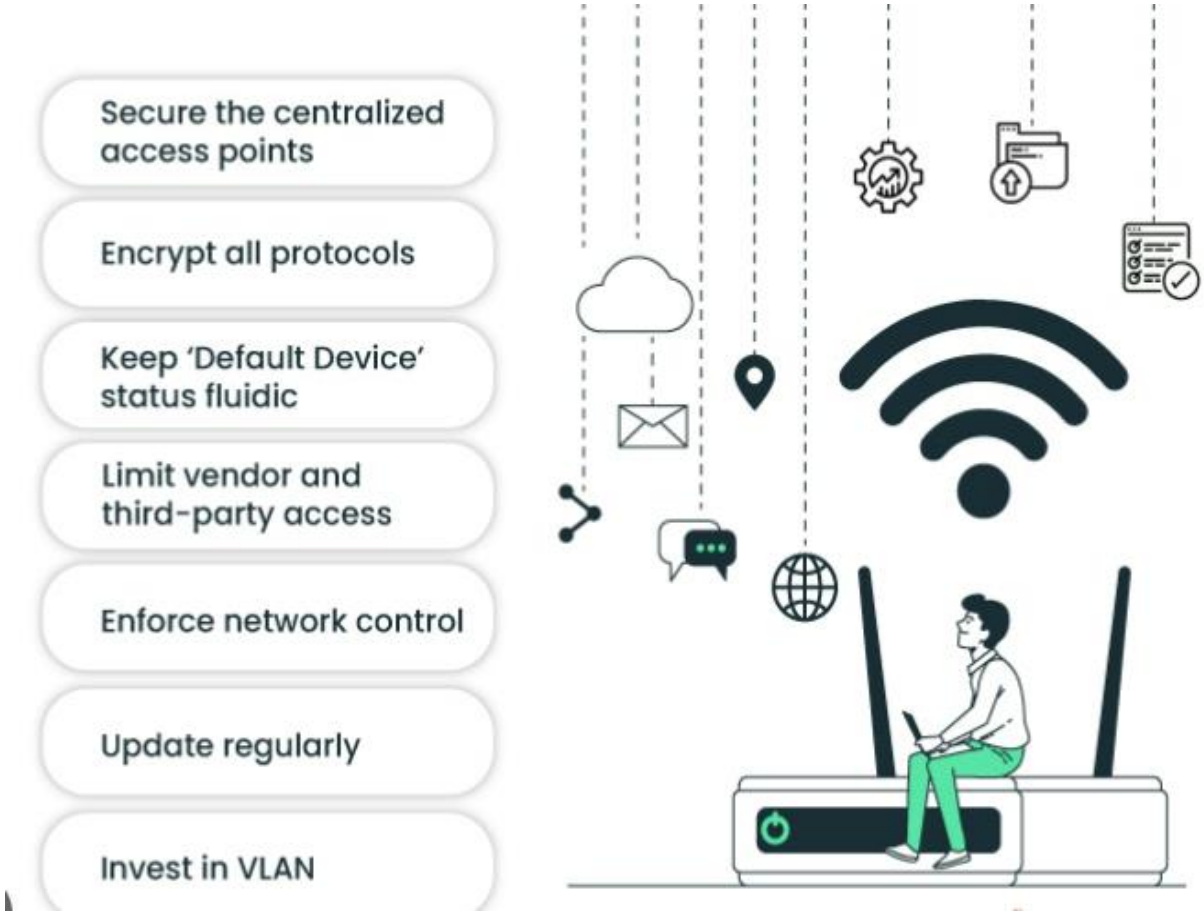

Secure the centralized access points
Encrypt all protocols
Keep 'Default Device' status fluidic
Limit vendor and third-party access
Enforce network control
Update regularly
Invest in VLAN

Figure 1: Security Techniques

5. Energy Efficient Techniques for IoT devices

One of the most important features of IoT devices is energy efficiency since it has a direct influence on their running costs, battery life, and environmental sustainability. The expansion of IoT devices across a range of sectors and applications has increased the need of using energy-efficient approaches. These gadgets are frequently battery-operated and need a reliable power supply to work well for lengthy periods of time. To improve the energy efficiency of IoT devices, researchers have created a number of ways.

Power management, which includes controlling a device's power usage in order to maximize performance, is one of the most important energy efficiency approaches. This method consists of a number of strategies, including duty cycling, which changes the device between the active and sleep modes in order to save energy (Tawalbeh *et al.* 2020). [19] Moreover, energy consumption is decreased using dynamic voltage and frequency scaling (DVFS) approaches, which change the processor's voltage and frequency to fit the demands of the moment. Data compression, which decreases the amount of data that has to be transferred or stored, is another method to improve energy efficiency (Safara *et al.* 2020). [15] The battery life of the device is increased through the use of compression methods, which lower the energy needed to transmit and store data. In addition, methods for capturing ambient energy sources including light, heat, and motion have been developed to power IoT devices. Lightweight communication protocols that consume less energy than conventional protocols have also been studied by researchers. These protocols improve energy efficiency and cut down on data transport overhead. Moreover, edge computing has become a viable energy-efficient method for IoT devices. In order to save energy on data transport and speed up reaction time, it entails processing data closer to its source, at the network's edge (Azar *et al.* 2019). [5] Overall, energy-saving methods are essential for the optimal and sustainable operation of IoT devices. Given their expanding usage and relevance across a range of sectors and applications, researchers must continue to investigate and create creative strategies to improve the energy efficiency of these devices.

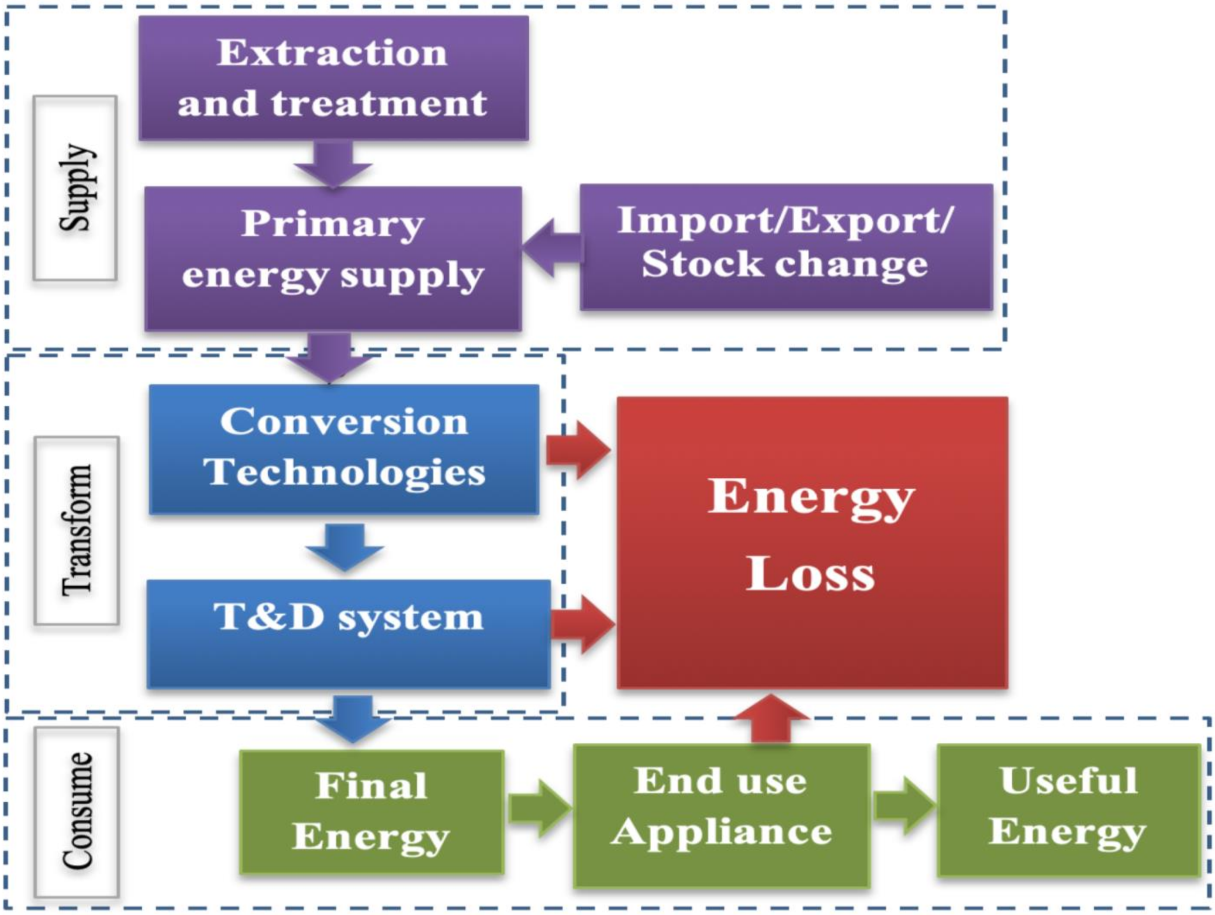


Figure 2: Energy Efficiency Techniques for IoT Devices

6. Integration of Security and Energy Efficiency in IoT Devices

Security and energy efficiency are becoming more and more necessary as the number of IoT devices increases quickly. Energy efficiency is necessary to increase the lifespan of the devices and cut down on energy consumption, while security is crucial to safeguard IoT networks from malicious assaults and illegal access. A crucial field of study focuses on creating solutions that can solve both issues concurrently, integrating security and energy efficiency in IoT devices. Using security measures that are intended to reduce energy usage is one strategy (Sen *et al.* 2018) [16]. Asymmetric key cryptography, for instance, can be used to lower the amount of energy required for encryption and decryption processes.

Another strategy is to create methods that can balance the compromise between energy efficiency and security. It was suggested in a study by Zhukovskiy *et al.* (2019).[24] that an IoT device's energy efficiency may be maximized by altering the level of security in accordance with the context and the type of data being broadcast by the device. This method necessitates that the gadget is capable of dynamically adapting to various security and energy needs. Moreover, the usage of lightweight security methods that utilize little energy may be used to integrate security with energy savings (Iwendi *et al.* 2021). [9] One such lightweight protocol is the Constrained Application Protocol (CoAP), which was created especially for Internet of Things (IoT) devices. It enables encryption and authentication using Datagram Transport Layer Security (DTLS).

Moreover, IoT device security and energy efficiency may be integrated using machine learning and artificial intelligence (AI) approaches. For example, machine learning algorithms may optimize the energy consumption of IoT devices by anticipating their usage patterns and modifying their energy consumption appropriately, while AI-based security solutions can be used to identify and mitigate possible security risks.

A crucial component of the design and development of IoT devices is the combination of security and energy efficiency. Researchers have suggested a number of strategies to achieve this integration, including the use of lightweight security protocols, the development of energy-efficient security mechanisms, balancing the trade-off between security and energy efficiency, and the use of machine learning and AI techniques (Zhukovskiy *et al.* 2019). [24] These methods are meant to make sure that IoT devices can function effectively while still being safe from security risks. To address the ever-increasing security and energy needs of IoT devices, additional research is needed to provide more effective and efficient solutions.

7. Resource Management Techniques for Energy Efficiency in IoT Devices

Resource management is a crucial component in creating IoT devices that are energy-efficient. IoT devices are often made to be constantly online, always on, and constantly gathering and transferring data, all of which can use up a lot of energy. Techniques for resource management seek to maximize energy consumption by reducing wasteful resource use and managing resources more effectively. Using adaptive power management strategies, which modify a device's power consumption depending on its usage patterns, is one method of managing resources (Latif *et al.* 2022). [10] When a device is not actively processing information or transferring data, for instance, it may switch to a low-power mode. The significance and urgency of the data may also be used by devices to determine which data to broadcast and when. Using energy harvesting technologies to increase the power supply of IoT devices is another method. In order to generate electrical energy that can power the device, energy harvesting entails gathering energy from the environment, such as solar, thermal, or mechanical energy. This strategy can lessen the frequency of battery changes and increase the battery life of IoT devices. Resource management includes the effective use of additional system resources, such as memory, computing power, and network bandwidth, in addition to managing system power (Stergiou *et al.* 2018). [18] To minimize the size of data packets being transported and the amount of bandwidth needed, one strategy is to employ data compression techniques. In order to maximize memory use, devices can also prioritize which data to process and retain depending on its value and relevance. In general, resource management strategies are crucial for creating IoT devices that use less energy. By using these methods, IoT devices may use less energy overall and have a less negative impact on the environment (Thera *et al*. 2020). [20] They can also last longer on batteries. There is still a lot of research to be done in this field, especially in terms of creating adaptive power management algorithms that are more advanced and enhancing the effectiveness of energy harvesting equipment.

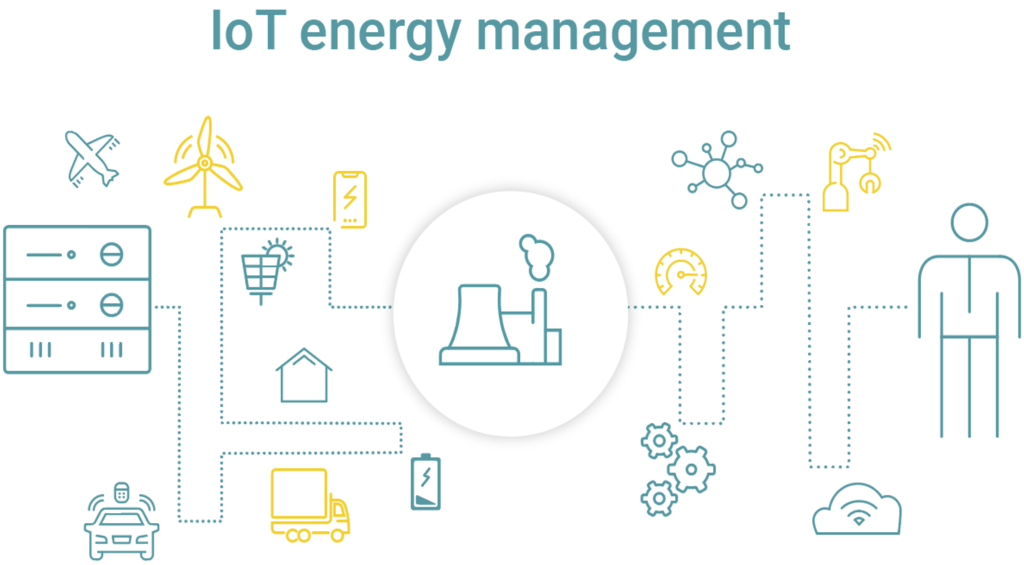


Figure 3: Energy Management

8. Machine Learning and Artificial Intelligence Techniques for Security and Energy Efficiency in IoT Devices

The potential of machine learning (ML) and artificial intelligence (AI) approaches to solve the security and energy efficiency issues in IoT devices has attracted a lot of interest in recent years. IoT devices can adapt to changing situations, optimize their energy use, and improve their security thanks to ML and AI approaches' capacity to learn from data and make predictions. The identification of anomalies is a crucial use of ML and AI in IoT devices. Algorithms for detecting anomalies can recognize abnormalities from regular patterns of device activity that can be signs of security risks or unusual energy use. A deep neural network-based approach for detecting abnormal energy usage in IoT devices was utilized in a paper by Vinueza Naranjo (2018). [22] The outcomes demonstrated that the algorithm was successful in identifying abnormalities and enhancing energy efficiency.

Predictive maintenance is another use of ML and AI in IoT devices. When determining when equipment is likely to malfunction or need repair, predictive maintenance algorithms can use information from sensors and other sources. Ensuring that equipment is running effectively, this may assist save downtime and maximizing energy utilization. A deep learning-based predictive maintenance algorithm was created for an Internet of Things system for smart buildings in a paper by Musaddiq *et al.* (2018). [13] The outcomes demonstrated that the algorithm was successful in foretelling equipment breakdowns and minimizing downtime. IoT security may also be improved with the use of ML and AI approaches. AI approaches may be used to find patterns of behaviour that can suggest security issues, while ML algorithms can be used to detect and respond to cyber-attacks in real-time. An AI-based security framework for IoT devices was suggested in a paper by Ullah *et al.* (2020), [21] which uses a combination of ML algorithms and rulebased systems to detect and address security threats. The outcomes demonstrated that the framework was efficient in identifying and countering different sorts of assaults.

Lastly, by anticipating energy consumption and modifying device settings accordingly, ML and AI approaches may be utilized to improve energy utilization in IoT devices. A deep learning-based energy management system for a smart home IoT system was created in research by Tun *et al.* (2020). [20]. The system was able to anticipate the amount of energy needed and modify device settings to optimize energy use while preserving user comfort levels. There are issues that need to be resolved even if ML and AI approaches show promise for enhancing the security and energy efficiency of IoT devices. These concerns range from the necessity for specialized hardware and software to those relating to data protection and scalability. Yet, the complicated security and energy efficiency concerns in IoT devices may be addressed through the use of ML and AI approaches.

9. Methodology

Clearly defining the project's goals and goals for the study will constitute the initial stage. In order to do this, it would be necessary to specify the precise security and energy-efficiency problems the study wants to solve as well as the kinds of IoT networks and devices that would be employed. The next step would be to use Cisco Packet Tracer to build the network architecture once the study objectives have been established. In addition to designing the topology of the network and standards, this entails choosing the IoT devices, sensors, and networks that will be utilised in the study. Implementing the energy-saving and security measures mentioned in the research goals would be the next stage. This would entail setting up data aggregation, variable power management, computing, inexpensive cryptographic techniques, important management methods, and firmware upgrades for the network's IoT devices. The system would've been tested to make sure it is operating properly once the security and energy-saving strategies have been implemented. To confirm the efficacy and efficiency of the adopted procedures, simulations and tests would need to be undertaken. Analysis of the testing and simulation data would be the last phase (Osifeko *et al.* 2020). [14] This would entail assessing the network's performance in regard to safety, energy usage, and functionality. Choose the IoT components and sensors that are crucial for this project first. The library of IoT devices in Cisco Packet Tracer may be used to choose from a variety of gadgets, including cameras, moisture sensors, and temperature monitoring. Set up the networks by giving the devices IPs, setting up the gateway, and setting the DNS servers. To set up the devices, use the CLI for Cisco Packet Tracer. To protect the link between the gadgets and the server, use security protocols like Transport Layer Security (TLS), Secure Sockets Layer (SSL), and Virtual Private Network (VPN). To mimic the connection, use the decryption and encryption capabilities in the packet tracer.

Positivism has been chosen as the research philosophy for the study of the creation and formation of secure and resource-saving solutions for IoT devices utilizing Cisco Packet Tracer. In order to further science, positivism places a strong emphasis on empirical research and observation. A quantitative methodology will be used in the study to collect data and evaluate hypotheses in order to create safe and energy-saving IoT device approaches. This study's research design will be experimental. The experimental design is suitable for evaluating the efficacy of different approaches in a controlled setting. In order to conduct the study, an entire network made up of IoT devices and sensors will be created in Cisco Packet Tracer, and different security and energy-saving measures will be put into practice (Machorro-Cano *et al.* 2020). [12] The system's efficiency will be evaluated in light of elements including energy usage, security, and network congestion. A deductive research methodology will be used for this project. A conceptual foundation will be utilized to create the study's initial set of hypotheses. The experimental design, which will involve multiple security and power strategies, will subsequently be used to verify the hypotheses. The outcomes of the tests will be utilized to confirm or disprove the assumptions and formulate suggestions for the creation of safe and resource-conserving methods for IoT devices. IoT sensors and devices will be arranged into network architecture in Cisco Packet Tracer (Sihombing *et al.* 2018). [17] A series of tests will be created to evaluate the effectiveness of the network architecture utilizing various security and energy-saving methods. In the topology of the network, safety and energy-saving approaches will be used. Data will be gathered on a variety of factors, including security effectiveness, network congestion, and energy use. Each study's data will be meticulously documented, and the findings will be collated for analysis. The efficacy of different security and power strategies in lowering energy consumption and enhancing security efficiency will be assessed by statistical evaluation of the information collected. To find the best approach for energy security and efficiency, each technology's performance will be evaluated, and the findings will be examined. It entails designing an experimental topology, putting it into practice, gathering data, and documenting it. Data cleansing, statistical analysis, data visualization, comparing, and result drafting are all steps in the method of data analysis. The outcomes of the data gathering will be utilized to create suggestions for the development and production of safe and resource-conserving methods for IoT devices.

10. Result

In order to develop as well as designed the secure along with energy efficient techniques for all the IoT devices the Cisco packet is a software that has been specifically used in this particular project for better implementation and understanding of the whole scenario. Firstly various IoT devices have been properly implemented inside the software platform and appropriate configuration has been executed so that all these devices can run without any error and provide a proper simulation model. The link that has been made between all of the layout part's branches is explained in this section of the project (Assim, M. and Al-Omary, 2020). [4] This portion of the scientific report clearly explains every aspect of the connection. This section of the technical project clearly illustrates all of the criteria. It is crucial to fulfilling all of the requirements listed for this report since it is recognized that no sort of network design can be completed without linking all of the elements.

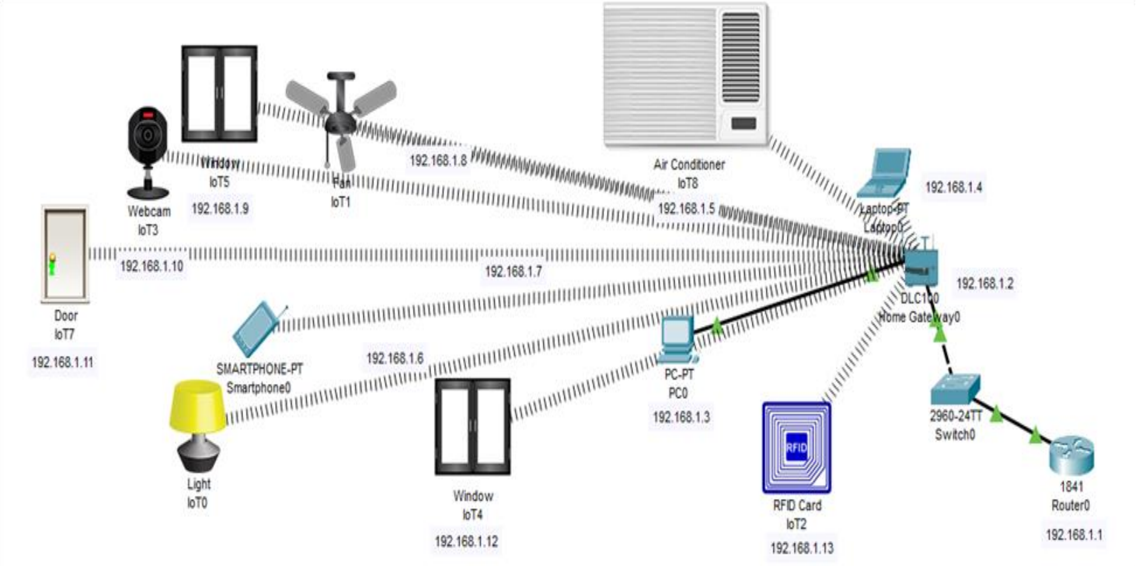
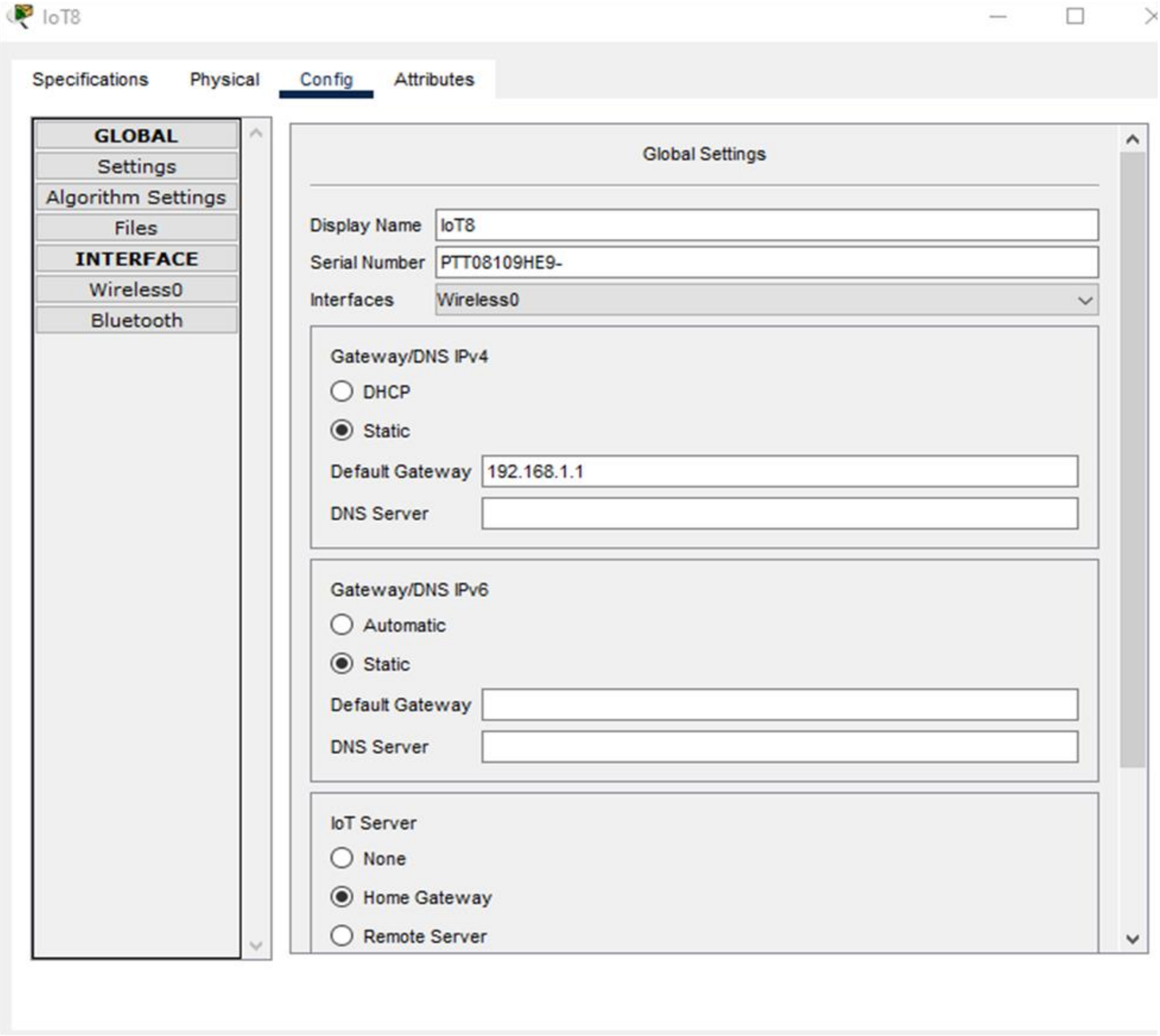


Figure 4: Technical Model of IoT Devices

The network connection's specifics have been expertly detailed in the image above, and each component is precisely shown. Switch, router, and computer are the names of the parts that are utilised to build a net connection. Each of the three elements is linked to the others. All the components that have been mentioned in the above picture are accurately connected with each other in order to develop a proper connection of IoT devices which can specifically help to understand the overall scenario and also maintain proper energy efficient and secure techniques. In order to connect all the elements in the most appropriate way it has been specifically observed that if the connection is not appropriate there is a huge chance of vulnerability which is not at all recommended because it cans proverb different kinds of the hacking process through all these devices (Badshah *et al.* 2019). [6] In the Cisco packet tracer platform, all the devices have been taken from the devices list and accurately connected with each other so that it can send the network in the most appropriate manner and there is no chance of security breaching in all those devices.



Global Settings

Display Name IoT8

Serial Number PTT08109HE9-

Interfaces Wireless0

Gateway/DNS IPv4

○ DHCP

● Static

Default Gateway 192.168.1.1

DNS Server

Gateway/DNS IPv6

○ Automatic

● Static

Default Gateway

DNS Server

IoT Server

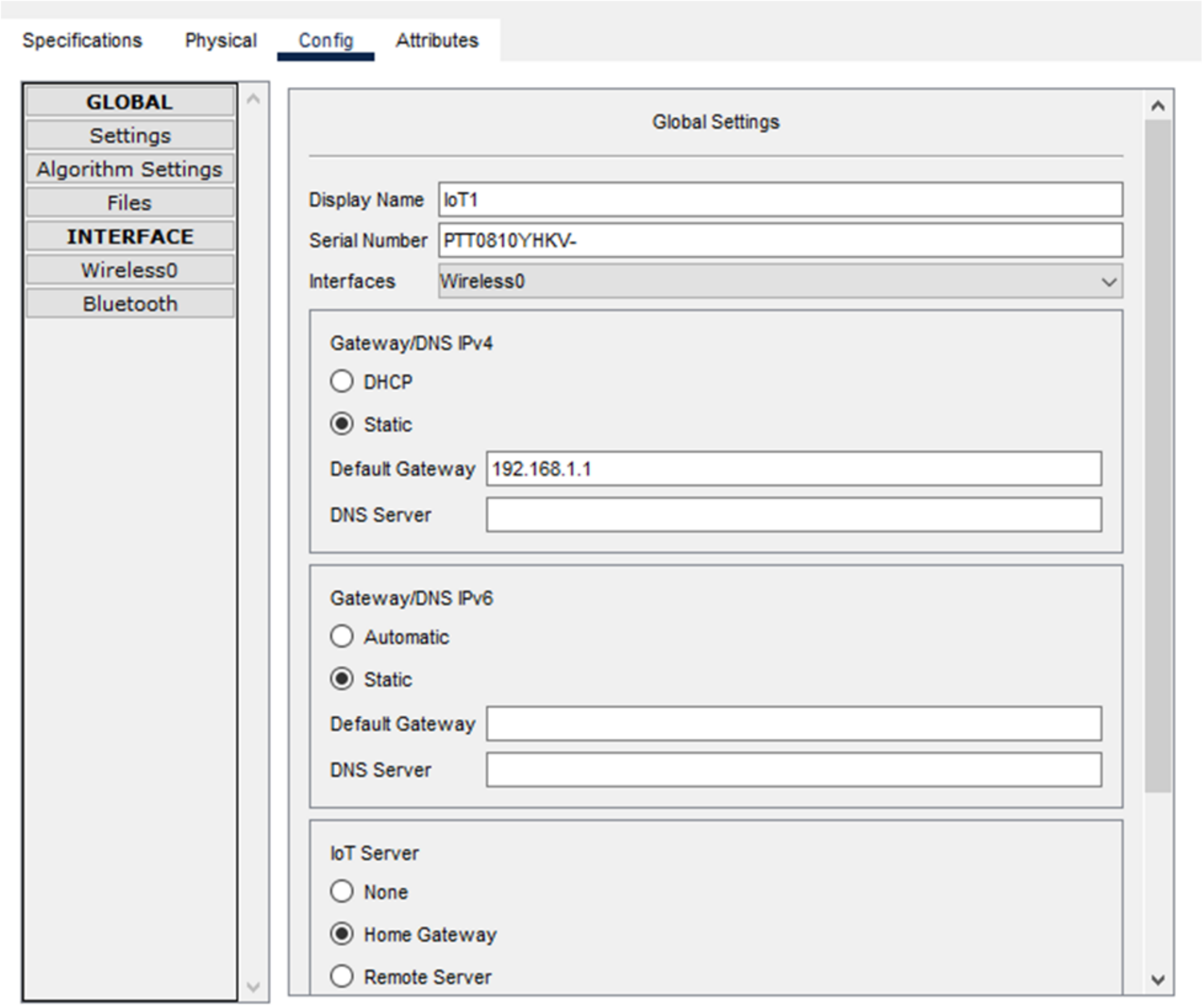
○ None

● Home Gateway

○ Remote Server

Figure 5: Configuration Model

The above mention picture specifically describes the configuration model for doors with the appropriate default gateway that has been provided so that the network can be very much accurate without any kind of error. Proper display name serial number, as well as interface, is clearly shown in the above mention configuration model which can help to determine the particular device and maintain the proper energy efficient technique that is required for the device. The Gateway as well as DNS is also static for this particular device and the server is the home gateway (Al-hamarneh, 2021). [2] All these IoT devices have a specific serial number along with their configuration model is also different so it is very much important to have a proper understanding of all these and maintain appropriate attributes for all these devices inside the Cisco tracer platform.



Global Settings

Display Name: IoT1

Serial Number: PTT0810YHKV-

Interfaces: Wireless0

Gateway/DNS IPv4

○ DHCP

● Static

Default Gateway: 192.168.1.1

DNS Server:

Gateway/DNS IPv6

○ Automatic

● Static

Default Gateway:

DNS Server:

IoT Server

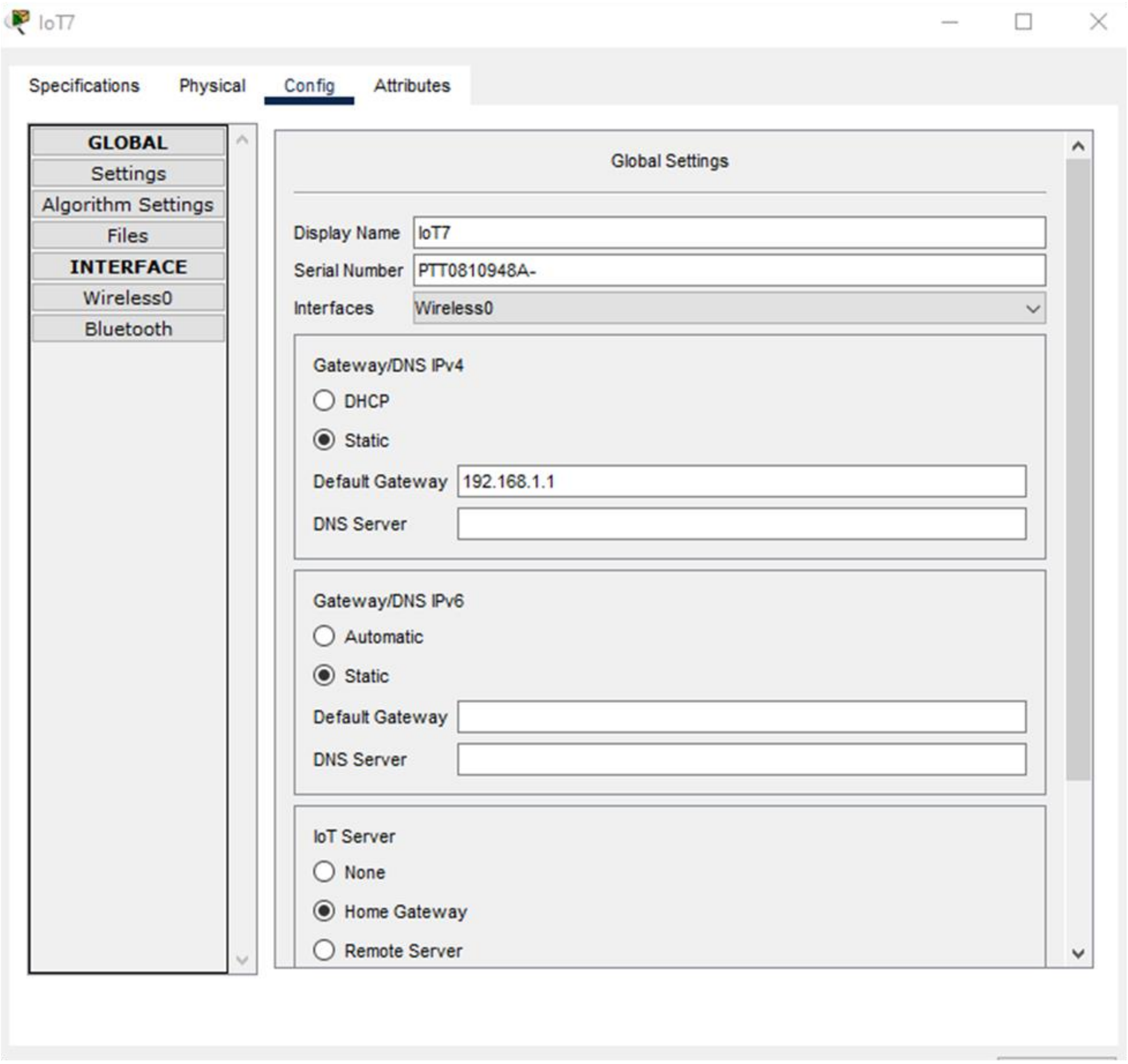
○ None

● Home Gateway

○ Remote Server

Figure 6: Configuration Model

This above mention picture is the configuration model of the fan which is also another IoT device and all the attributes that are directly connected with this device have been specifically discussed with all the necessary information. It is also a home gateway and it is also static all these things have been specifically determined through the help of different tools of Cisco packet research which accurately help to develop very secure techniques for all these devices for providing a very safe experience to define individuals out there (Gwangwava and Mubvirwi, 2021). [7]



Global Settings

Display Name: IoT7

Serial Number: PTT0810948A-

Interfaces: Wireless0

Gateway/DNS IPv4

○ DHCP

● Static

Default Gateway: 192.168.1.1

DNS Server:

Gateway/DNS IPv6

○ Automatic

● Static

Default Gateway:

DNS Server:

IoT Server

○ None

● Home Gateway

○ Remote Server

Figure 7: Configuration Model

The configuration model of a door, another IoT device, is shown in the image above. All the features that are clearly relevant to these devices have been specifically explained with all the relevant details. It serves as a home gateway, and it is static. Each of these details has been precisely determined with the use of various Cisco packet analysis tools, which accurately aid in the development of extremely secure approaches for each of these gadgets so as to provide the public with a very safe environment (Hazim and Alabady, 2022). [8] The configuration model mentioned above clearly displays the right screen name, registration number, and connector, which can be used to identify the specific item and keep up with the energy-efficient strategy that is necessary for the equipment.

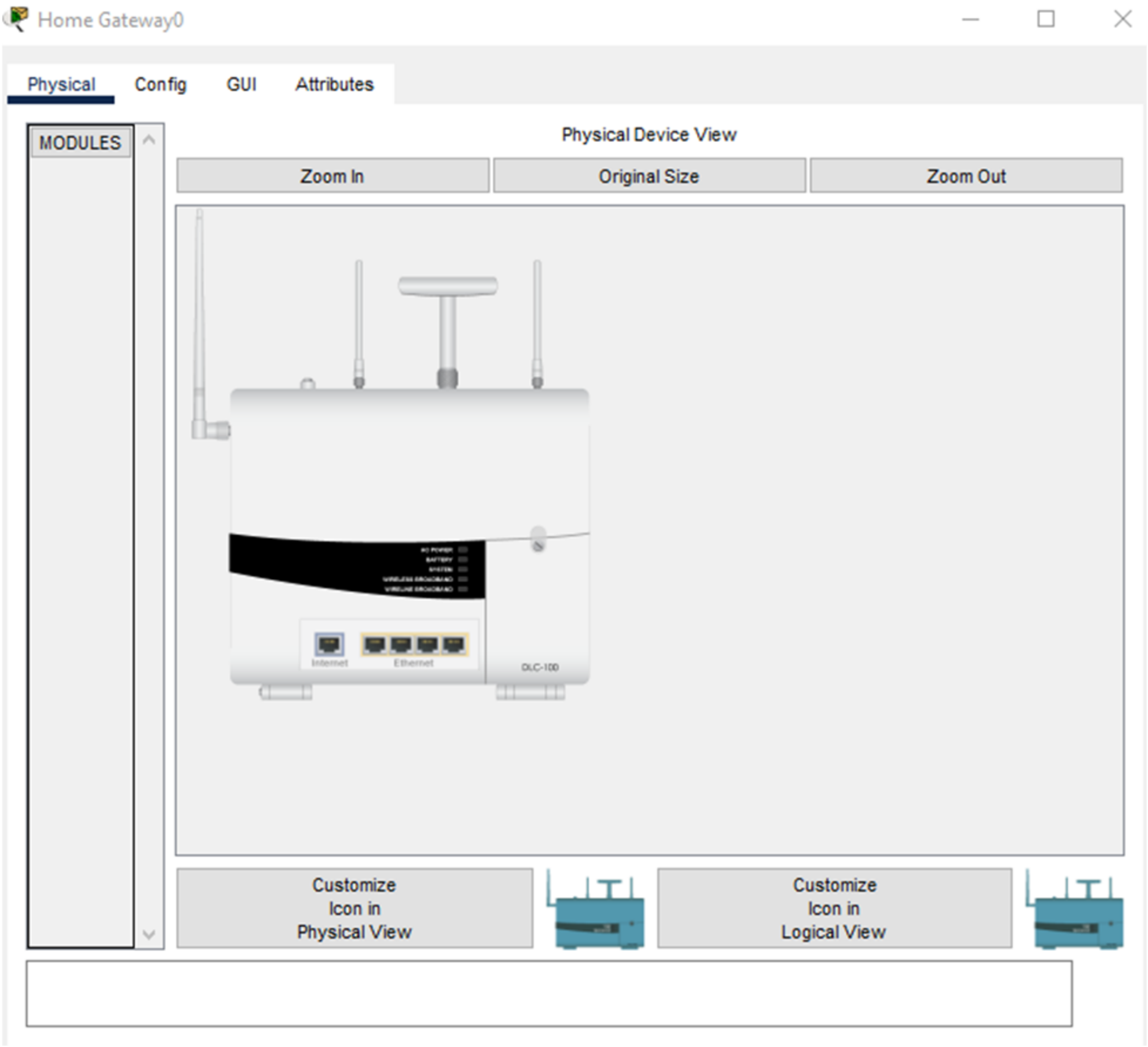
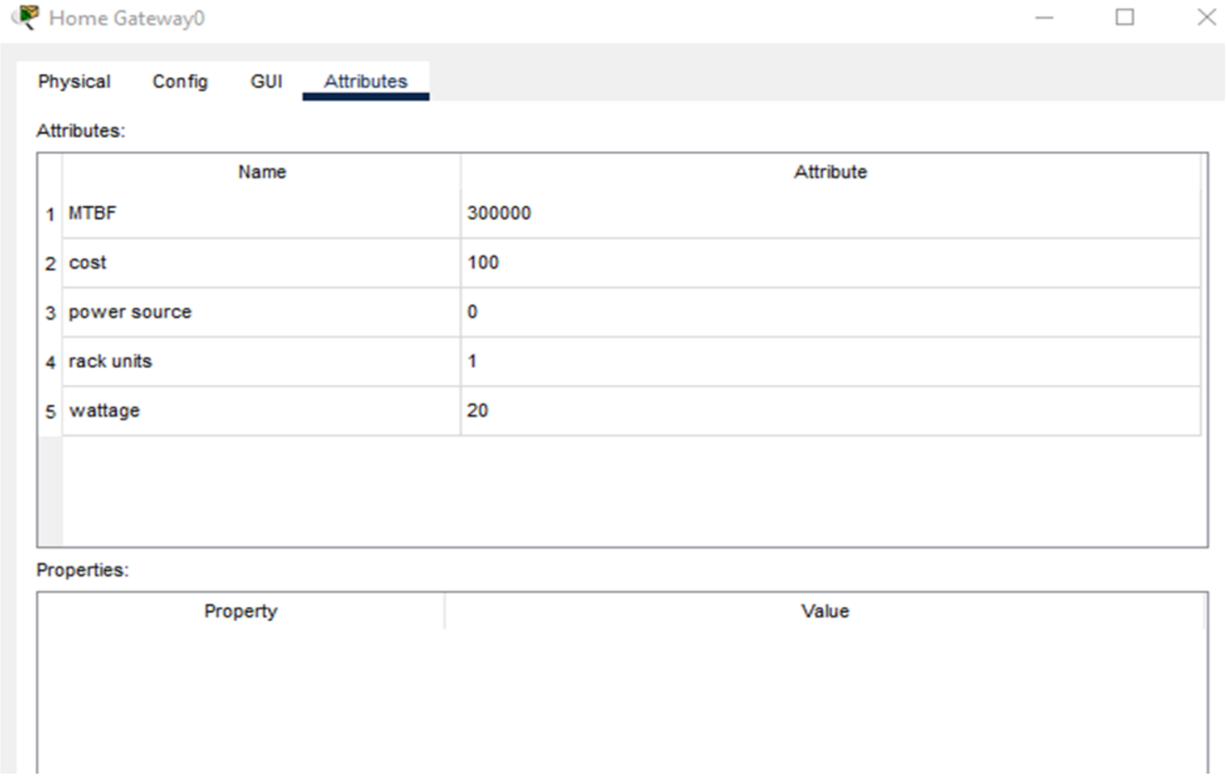


Figure 8: Physical Model Configuration

This particular picture that has been discussed above is the physical view of the router which is directly connected with different other devices through the proper adaptor. The logical as well as physical few are clearly visible in the above mention feature with all the adopting point where different kind of adaptor is needed to connect to the proper network (Thera *et al.* 2020). [20] This display is accurately helping to understand the whole scenario in the most appropriate manner with the specific view of a router and all the necessary equipment that are directly connected to it.



Home Gateway0

Attributes:

	Name	Attribute
1	MTBF	300000
2	cost	100
3	power source	0
4	rack units	1
5	wattage	20

Properties:

Property	Value

Figure 9: Various Attributes

All the attributes have been specifically discussed in the above mention picture which has been determined by the tools of the Cisco packet tracer and the value has also been mentioned which is very much appropriate. After determining as well as developing the energy-efficient techniques of all these IoT devices that have been mentioned it becomes possible to determine the value of all these attributes which are directly connected with the network model

.

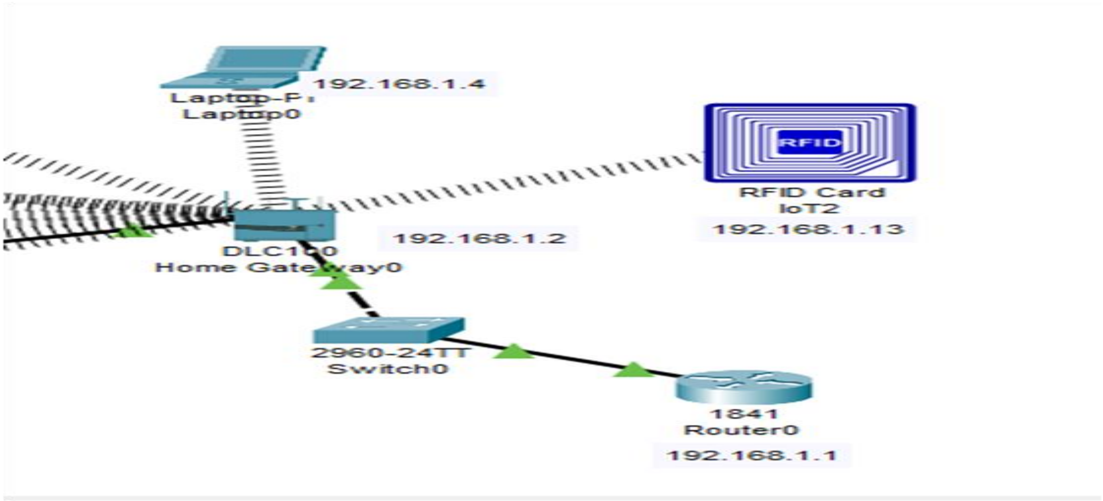
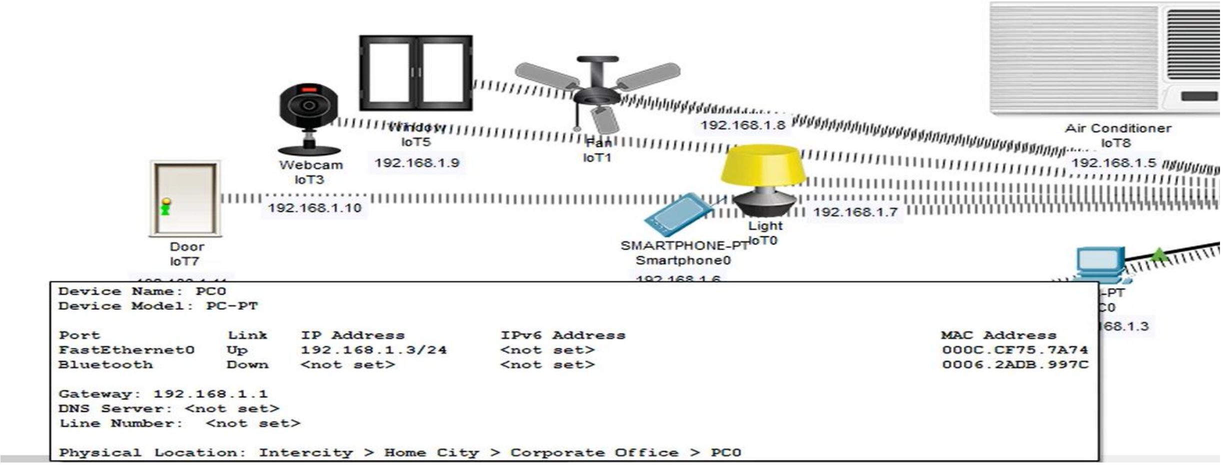


Figure 10: IoT Devices

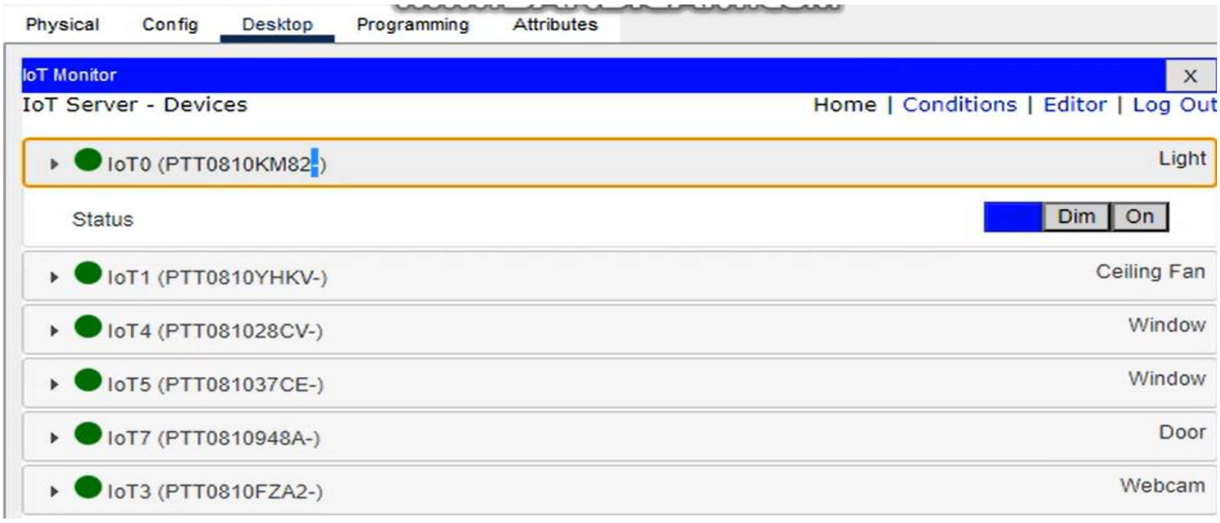
In this particular picture all the equipment has been specifically described which are switch, router, and home gateways along with RFID cards. All these elements are very much necessary for the appropriate development of energy-efficient techniques for different IoT devices because without all the elements it is not at all possible to develop the whole network model which can help to determine all these important aspects of it (Finardi, 2018). [6]



```
Device Name: PC0
Device Model: PC-PT

Port            Link   IP Address       IPv6 Address                                MAC Address
FastEthernet0   Up     192.168.1.3/24   <not set>                                   000C.CF75.7A74
Bluetooth       Down   <not set>        <not set>                                   0006.2ADB.997C

Gateway: 192.168.1.1
DNS Server: <not set>
Line Number:  <not set>

Physical Location: Intercity > Home City > Corporate Office > PC0
```

Figure 11: IoT Device Details

In this picture it is very much possible to see that there are Air conditioners, Automatic doors, webcams, fan as well as automatic lights which can possibly to regulate by a Smartphone. The IP address of all these devices along with their DNS server has specifically described and in the above mention picture it is also possible to see that all these are directly connected to the router and if someone crosses the door then it will automatically on.



IoT Server - Devices

● IoT0 (PTT0810KM82-)	Light
Status	Dim On
● IoT1 (PTT0810YHKV-)	Ceiling Fan
● IoT4 (PTT081028CV-)	Window
● IoT5 (PTT081037CE-)	Window
● IoT7 (PTT0810948A-)	Door
● IoT3 (PTT0810FZA2-)	Webcam

Figure 12: Various Device Servers

This is the whole desktop mode of the Cisco packet tracer where all the devices along with their status are possible to see and it can help to determine whether the devices are on or off. Various devices' name is clearly shown in the above mention picture and their status is also possible to understand which can vary through the motion of any people who are entering the door. Through this particular desktop IoT monitor process it is very much possible to see all the devices along with their status and it can be very helpful for all the individuals out there to understand whether it is on or off (Akmandor *et al.* 2018). [1] This status is also directly connected with the energy efficient technique along with the secure techniques which is very much important for all the IoT devices to provide a very safe experience.

11. Conclusion

Using Cisco Packet Tracer, the development, and design of Safe and Energy Effective Methods for IoT Devices initiative is a great effort to solve the crucial challenges of Safety and Energy Effective for IoT Devices. The rise of IoT devices has made it essential to protect them from online attacks. Also, IoT devices have to be fuel efficient in order to function properly because they frequently depend on batteries. The major goal of the project was to create and put into use an IoT device that was safe and energy-efficient utilizing Cisco Packet Tracer. To ensure the security of the device, the project made use of a number of security measures, including the implementation of secure passwords, the use of encryption methods, and the configuration of firewalls. Using low-power equipment, streamlining the software, and adopting sleep modes were some of the energy-saving strategies that greatly increased the effectiveness of the gadget. Overall, the research was effective in accomplishing its goals and showed that it is feasible to incorporate security and energy-saving features in IoT devices. The project's results may be integrated into industry best practices and standards and utilized to increase the safety and energy efficiency of upcoming IoT devices. The project's accomplishment demonstrates the significance of solving security and efficiency challenges in IoT devices and the requirement for more study in this field. IoT devices must be kept safe, dependable, and energy-efficient since they are essential to our everyday lives and are being employed in more and more important infrastructure. It makes a substantial contribution to the fields of energy efficiency and IoT safety. More study in this field is essential for the development of the Internet of things (IoT as it may be used to increase the safety and power efficiency of IoT devices, rendering them more dependable and secure. The proper IoT network development as well as energy-efficient techniques that are necessary for all the IIT devices has been specifically described in the particular project with proper software implementation inside the Cisco packet tracer. Various tools along with techniques of the specific software have been particularly used in the project for the better implementation process and Secure techniques that are the most important part of a very secure environment for IoT devices. Different IoT devices have been particularly used in these projects inside the software platform for a specific network model and proper analysis has been given with all the necessary information that can help to get a proper idea about the whole scenario. The overall concept of secure techniques for IoT devices along with energy efficient techniques for all these devices has been clearly discussed in this particular project with all the necessary information and different reference that can provide correct data about all these. In the methodology part all the method that has been used in this project has specifically described which can help to develop and design Different techniques that is very much and energy efficient for various will devices.

12. References

1. Akmandor, A.O., Hongxu, Y.I.N. and Jha, N.K., 2018. Smart, secure, yet energy-efficient, Internet-of-Things sensors. *IEEE Transactions on Multi-Scale Computing Systems*, *4*(4), pp.914-930.
2. Al-hamarneh, R., 2021 improve security in smart cities based on IoT, solve cyber electronic attacks with technology by using packet tracer.
3. Alladi, T., Chamola, V., Sikdar, B. and Choo, K.K.R., 2020. Consumer IoT: Security vulnerability case studies and solutions. *IEEE Consumer Electronics Magazine*, *9*(2), pp.17-25.
4. Assim, M. and Al-Omary, A., 2020, December. Design and implementation of smart home using WSN and IoT technologies. In *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)* (pp. 1-6). IEEE.
5. Azar, J., Makhoul, A., Barhamgi, M. and Couturier, R., 2019. An energy efficient IoT data compression approach for edge machine learning. *Future Generation Computer Systems*, *96*, pp.168-175.
6. Badshah, A., Ghani, A., Qureshi, M.A. and Shamshirband, S., 2019. Smart security framework for educational institutions using internet of things (IoT). *Comput. Mater. Contin*, *61*(1), pp.81-101. Finardi, A., 2018. Iot simulations with cisco packet tracer.
7. S. Upadhyay, SK Sharma et. al. "Analysis of Different Classifier Using Feature Extraction in Speaker Identification and Verification Under Adverse Acoustic Condition for Different Scenario", International Journal of Innovations in Engineering and Technology, Volume 6 Issue 4, pp. 425-434, April 2016.

8. A. Updhay, N. Gangdotra et. al."Impact of Mobility on the Performance of Wireless Ad hoc Networks Scenario using Distance Vector Routing Protocol", International Journal of Computer Application (IJCA), Volume-57, No. - 12, pp. 14-21, November 2012.
9. Iwendi, C., Maddikunta, P.K.R., Gadekallu, T.R., Lakshmanna, K., Bashir, A.K. and Piran, M.J., 2021. A metaheuristic optimization approach for energy efficiency in the IoT networks. *Software: Practice and Experience*, *51*(12), pp.2558-2571.
10. Latif, S.A., Wen, F.B.X., Iwendi, C., Li-li, F.W., Mohsin, S.M., Han, Z. and Band, S.S., 2022. AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. *Computer Communications*, *181*, pp.274-283.
11. Liao, B., Ali, Y., Nazir, S., He, L. and Khan, H.U., 2020. Security analysis of IoT devices by using mobile computing: a systematic literature review. *IEEE Access*, *8*, pp.120331-120350.
12. S. Upadhyay, M. Kumar, A. Upadhyay, "Digital Image Identification and Verification using Maximum and Preliminary Score Approach with Watermarking for Security Enhancement and Validation", Journal of Electronics, Vol. 12, Issue 7, pp. 1-15, 2023.
13. Musaddiq, A., Zikria, Y.B., Hahm, O., Yu, H., Bashir, A.K. and Kim, S.W., 2018. A survey on resource management in IoT operating systems. *IEEE Access*, *6*, pp.8459-8482.
14. Osifeko, M.O., Hancke, G.P. and Abu-Mahfouz, A.M., 2020. Artificial intelligence techniques for cognitive sensing in future IoT: State-of-the-Art, potentials, and challenges. *Journal of Sensor and Actuator Networks*, *9*(2), p.21.
15. MC Saxena, F Banu, A Shrivastava, M Thyagaraj & S. Upadhyay, "Comprehensive Analysis of Energy Efficient Secure Routing Protocol for Sensor Network", Volume 62, Part 7, pp. 5003-5007, 2022**,** Material Today
16. Sen, S., Koo, J. and Bagchi, S., 2018. TRIFECTA: security, energy efficiency, and communication capacity comparison for wireless IoT devices. *IEEE Internet Computing*, *22*(1), pp.74-81.
17. S. Upadhyay, M. Kumar, A. Kumar & K Z Gafoor, "Smart Healthcare Solution for Future Development using Speech Feature Extraction Integration Approach with IoT and Blockchain", Journal of Sensors, Vol. 2022, pp. 1-13, May 2022.
18. Stergiou, C., Psannis, K.E., Kim, B.G. and Gupta, B., 2018. Secure integration of IoT and cloud computing. *Future Generation Computer Systems*, *78*, pp.964-975.
19. Tawalbeh, L.A., Muheidat, F., Tawalbeh, M. and Quwaider, M., 2020. IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), p.4102.
20. Thera, D., 2020. *Internet of things simulation using cisco packet tracer* (Doctoral dissertation, Izmir Institute of Technology (Turkey)). Tun, Y.K., Park, Y.M., Tran, N.H., Saad, W., Pandey, S.R. and Hong, C.S., 2020. Energy-efficient resource management in UAV-assisted mobile edge computing. *IEEE Communications Letters*, *25*(1), pp.249-253.
21. Ullah, Z., Al-Turjman, F., Mostarda, L. and Gagliardi, R., 2020. Applications of artificial intelligence and machine learning in smart cities. *Computer Communications*, *154*, pp.313-323.
22. S. Upadhyay, M. Kumar, A. Kumar, R. Kranti, "Feature Extraction Approach for Speaker Verification to Support Healthcare System using Blockchain for Data Privacy", Computational and Mathematical Methods in Medicine, Vol. 2022, pp. 1-12, July 2022.
23. Xiao, L., Wan, X., Lu, X., Zhang, Y. and Wu, D., 2018. IoT security techniques based on machine learning: How do IoT devices use AI to enhance security? *IEEE Signal Processing Magazine*, *35*(5), pp.41-49.
24. Zhukovskiy, Y., Batueva, D., Buldysko, A. and Shabalov, M., 2019, October. Motivation towards energy saving by means of IoT personal energy manager platform. In *Journal of Physics: Conference Series* (Vol. 1333, No. 6, p. 062033). IOP Publishing.