IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURE CAMPUS AREA NETWORK IN CISCO PACKET TRACER

[1]B. Midhun Krishna Yadav, [2]Akhilendranath Mummadi, [3]Vishnu Vardhan Ciripuram, [4]Dr. R Uma Mageswari

[1]Student, [2]Student, [3]Student, [4]Associate Professor

[1,2,3,4]Department of Computer Science & Engineering,

[1,2,3,4]Vardhaman College of Engineering, India

Abstract: Communication has always been an import part of life and its importance came to light as internet and intranet technology has started to constantly evolve and users looking for increasingly sophisticated services and thus Networks have been laid out all around the globe at different levels for their respective needs and necessities. Without networks the communication between two individual bodies present in different location would seem impossible. The network has woven itself into the very fabric of our lives. We worked on a problem for Campus Area Network, also known as CAN, and its potential gaps that can be a channel for hackers to penetrate the organization, and we presented a smart and safe network architecture for colleges to boost security and limit the danger of any type of threat. This architecture consists of various departments which are often found in most of the colleges and each of them housed in different buildings and this architecture is secured by VLANs, ACLs and IoT monitoring systems. This entire simulation is duplicated and laid out in Cisco Packet Tracer, which allows us to configure all parts of the network and its respective devices and imitate its working as in the real world.

Index Terms **- Campus Area Network, IoT, VLAN, ACL, RIP**

I. INTRODUCTION

Over time, the Internet has expanded incredibly quickly. It is the most widely used method of connecting people, data, and technology. Since the advent of Internet technology on campuses, there has been a strong connection between university life and the Internet. The usage of Internet for teaching and learning purposes has received increasing attention over the world. There has been a strong connection between university life and the Internet., not just as a means of teaching many departments in a college like Computer science department, Information technology department etc. and many more which depend on systems to learn. Devices are connected over the network as they can exchange data, files and communicate with each other and the outer world. Without a network, the entire system may cease to exist as it has been the primary mode of communication in the fast-growing digitalized world. There are various types of networks in various levels and are separated based on the geographic area and the size it needs to cover, the networks can be classified into many different types [1]

- LAN: A local area network is referred to by the acronym "LAN." It's a kind of network that's often connected in a small space, such a house, workplace, school, or set of buildings, to let users to communicate and share resources like printers and scanners. Both wired and wireless communications could be used to connect those devices. Each LAN is either completely independent of other networks or connected to other LANs. A local area network typically consists of PCs and other peripherals that are linked to a local domain server and used to share printers and other resources like games, software, and disc storage. Each LAN is either completely independent of other networks or connected to other LANs. Wide Area Networks, which can also link to the Internet, are also possible (WAN). A home network is often made up of individual LANs and

numerous LANs in terms of practical use, which refers to a home network setting up a guest network. This network operates at high speed.

- WAN: Wide area networks, or WANs, it is a telecommunications networks covering a large geographic area. It provides communication between towns and span vast areas of land like continents and nations. WANs have more capacity than LANs and MANs do. Telecommunications networks that span a considerable geographic area are known as wide area networks. The internet, which has impacted people's daily lives all around the world, is the best example of a wide area network. In order to allow computers to exchange, send, and access information on a broader scale, wide area networks are linked to local area networks.
- MAN: Metropolitan area networks, or MANs, are smaller than WANs yet span areas that are larger than LANs. MAN is typically used to provide Internet access and link devices within cities. The Metropolitan network allows connecting
  a larger area, such as an entire city, to the WAN. Metropolitan can also include a number of LANs connected by bridge to a single backbone line. LANs are linked to form MAN. Since data does not need to travel across great distances, MANs are typically more efficient than WANs. Instead of being run by a single organization, MANs often combine the networks of several different organizations.

A topology is the arrangement of various nodes in a specific pattern in a network. There are different types of topologies available which have its own advantages and disadvantages. Different types of topologies are used based on various needs and situations. There are a total of six mainstream topologies which are:

- Bus Topology
- Star Topology
- Mesh Topology
- Ring Topology
- Tree Topology and
- Hybrid Topology

Multiple factors affect the arrangement of a network, all these factors are to be taken into consideration when choosing a specific topology for any kind of network:

- All the Hardware devices available in the network
- Scalability requirement at individual level
- The types of business processes you intend to execute
- The administrative work required are a few examples
- anticipated volume of traffic on the network
- Budget set aside for the network, or the sum of money you are ready to put up
- Time necessary for the response from different nodes.

The IP address plays a vital role in connecting devices to participate in data transmission. There are billions of devices available in the world which are constantly active and sharing information in the network. Every Internetconnected device has a specific IP address that is issued to it. In the world of cyberspace, a device is uniquely identified by its IP address [2]. Every device has 2 IP addresses which are known as Public and Private IP addresses. The public IP address is an address that is used to identify the device in the outside world or the internet while private IP address is used to identify the device internally. There are two different types of IP addresses in the world right now which are IPv4 and IPV6.

IPv4: An IP address is a 32-bit (4 bytes) number normally written as follows: xxx.xxx.xxx.xxx There are a finite number of IP addresses which do not satisfy the need of all the devices in the world currently present and are growing at a very rapid rate. This is because of its size which is only 32 bits. The IPv4 addresses are categorized into 5 different classes namely Class A (range:0-127, subnet mask:255.0.0.0); Class B (range128-191, subnet mask:255.255.0.0); Class C (range:192-223, subnet mask:255.255.255.0); Class D (range:224-239); Class E (range:240-255). Class D addresses are used for multicast networking, while class E addresses are designated for future or experimental use.

IPv6: Since we are running out of IPv4, Ipv6 addresses were introduced and it is practically not possible to use all the available IPv6 addresses. There are 128 bits in one IPv6 address. Because every bit has two possible values (1 or 0) and there are 128 bits total. In the actual world, these addresses are gradually being used and will slowly replace the Ipv4 addresses. Ipv4 is still being used till date but not for long. For Ipv6 addresses, there are no special classes for it like the general Ipv4 addresses.

II. REVIEW OF PREVIOUS STUDIES

The research paper "Enhancing the College Network "published by Jagdish K.P. and Pavan Kumar [4], which deals with creating an advanced network with CISCO-PACKET Tracer. The proposed system here does not have many switches which leads to increase in the usage of routers at different levels of the organization which is not cost effective and can in turn increase the threat if there are potential misconfigurations on these devises. In the research paper "Designing a secure campus network and simulating it using Cisco packet tracer", Alaa H. Ahmed, Mokhaled N. Hamadani et al. [2] they have divided the entire network into small chunks known as VLANs which are referred to as virtual LANs. These VLAN's are a set of sub-networks which can be configured just like a router. They have implemented VLAN's but failed to configure them in a secure manner and missed some important authorization methods which can be done. In the paper "Design and Implementation of a Secure Campus Network" proposed by Ali, Md. Nadir [10] is a secure network, and the authors employed VLANs to separate the networks from one another, but they failed to address the MAC Flooding attack, and they also improperly configured the switches, leaving open the used ports that an attacker could access directly if they were left open. Abdi, A. [11] proposed an CAN architecture in "Designing Smart Campus Using Internet of Things", the author used IoT technology to make the Campus Area Network smarter, but he did not suggest using a fire alarm system to make the architecture system more efficient. These fire alarm systems are quite beneficial in the event of a fire. Milind V. Mahajan, Gaurav P. Sonar et al. [5] proposed a network architecture which is advantageous for organization in many possible ways but neglected some of the important components that are required to safeguard a network. They failed to add and configure many essential components like IDS, firewalls and IPS. Without these components and necessary configurations, the network is not safe and secure and is vulnerable to many potential attacks and data breaches.

III. PROPOSED ARCHITECTURE

To create this architecture, we have used a simulation software known as Cisco packet tracer. The Cisco packet tracer is a networking simulator which is utilized for teaching and learning programming by providing a realistic scenario which is a duplicate copy of a general network. We have created the secure network architecture my making use of the features of Cisco Packet Tracer. The upper hand of using this tool is

- It provides simulation and visualization in real time
- The ability to design, build, configure, and debug complicated networks
- The ability for students to experiment and explore ideas.
- This simulator software dynamically supports programming languages like Python.

The network architecture which we proposed here focuses on the usage of switches at different parts of the organization which helps reduce the excessive use of routers and is cost efficient. It is crucial to have a cost-effective network which uses switches to eliminates the need for multiple routers. Unlike many Campus Area Architectures which use Star or Bus topology, our model is based on Mesh topology. The Mesh network is typically a local area network (LAN) in which every node is interlinked with the neighboring nodes. The network as a whole is unaffected by the failure of a single node or a link. The failure can be quickly found and fixed at the same time. The cost of maintenance may rise over time, but our model has central management which in turn aids in network monitoring. In our proposed architecture we are implementing VLAN's in a more efficient and secure way and also adding ACL's which are known as Access Control Lists, these are used to prevent access of a network form other networks. ACLs are particularly important for regulating traffic flow control, a degree of security for network access that specifies which sections of the server/network/service a user may access [3]. We segmented some of the crucial LAN networks in the architecture into different VLANs (Virtual LAN) to separate these smaller networks from the main network as these VLANs are configured with ACLs (Access control Lists) which restrict unauthorized users from accessing these authorized user's devices [6]. Each and every department in the organization has its own specific routers, switches, and networks. The HOD network is completely isolated from the lab network to make sure no student or any other unauthorized user can access the HOD's computer. In addition to this, we have also configured a DHCP Server that dynamically allocates IP addresses to any new devices that are connected to the network. The web Server is configured so that the devices can access and browser and the Internet. The FTP server is used to transfer files within the network and the users are authenticated with a username and password. The E-mail server is configured in such a way that they can send and receive e-mails.

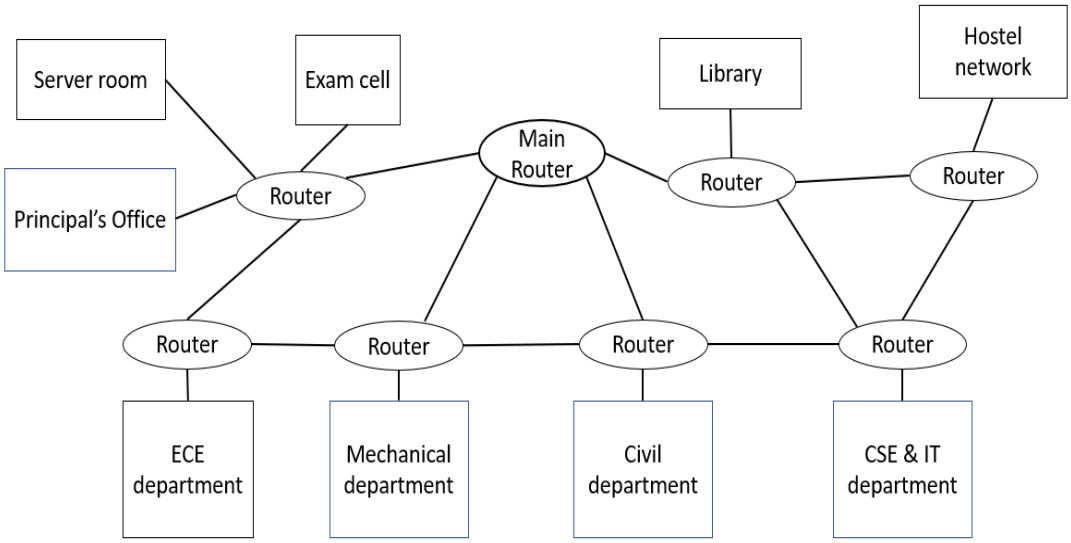

fig. 1. topology of the proposed architecture

Fig. 1 describes the planned architecture's topology as well as all the networks that exist. In this proposed architecture, the routing protocol used is RIPv2 (Routing Information Protocol). The Routing Information Protocol (RIP) is a distance-vector, interior gateway (IGP) routing protocol used by routers to exchange routing information. RIP uses the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. We placed the NAT into place (Network Address Translation). IPs of one class can communicate with IPs of the other class with the aid of NATs. To communicate with the computer on the other side of the world, NATs are used. NAT enables us to change our private IP addresses to public IP addresses and vice versa. We require a public IP in order to communicate with the Internet because our private IP is only used to communicate within the network and cannot be interpreted by devices outside the network. The majority of topologies employ dynamic NAT, which means that each private network device chooses its own public IP address while interacting with the Internet. In dynamic NAT, there is a pool of public IP addresses that the device uses before releasing them after use. These IPs are recycled. We switched from Dynamic NAT to NAT overload, often known as PAT (Port Address Translation). In this NAT, the private network as a whole communicates with the Internet using a single public IP address. There aren't many IPs available for use because these IPs are IPv4 addresses hence PAT is recommended. If an attacker plugs in his device to any one of the switch's open ports, he can quickly gain access to the network. In order to strengthen security at this stage and stop these unauthorized users from directly connecting to the switch, the admin must shut down the working of these unused switch ports. In a mac flooding attack [12], phony mac addresses are used to try and fill the Content Addressable Memory (CAM) table. The attacker intends to convert the switch into a hub by bombarding it with bogus mac addresses. The total number of mac addresses saved in the switches will be limited as part of our architecture to mitigate any possible risk of this attack. Through this method, if the CAM table fills up, the attacker's attempted connection to the interface will be denied and that interface will

automatically be shut down. Our proposed system has filled the gaps which were left out by them as we have added all the essential components and configured them by taking into consideration of all security measures.

IoT (Internet of Things) devices have become increasingly important in enhancing the efficiency and security of campus area networks (CANs) [8]. Devices such as fire alarms, automatic doors, and lights are specifically designed to work seamlessly within networked environments, making it easy for educational institutions to automate various operations and improve campus security. Fire alarms connected to CANs can quickly alert security personnel, reducing response times and preventing major disasters. Automated doors can also be programmed to open and close based on specific events, improving accessibility while preventing unauthorized access. Furthermore, smart lighting systems equipped with motion sensors and daylight sensors can enhance energy efficiency and security within the campus. By collecting data from IoT devices like sensors placed throughout the campus, institutions can optimize energy usage, improve air quality, and enhance the learning environment for students. In summary, the integration of IoT devices like fire alarms, automatic doors, and lights into the CAN architecture is crucial in creating a smart and secure campus environment. These devices can improve overall security, optimize energy consumption, and enhance the learning experience for students in educational institutions.

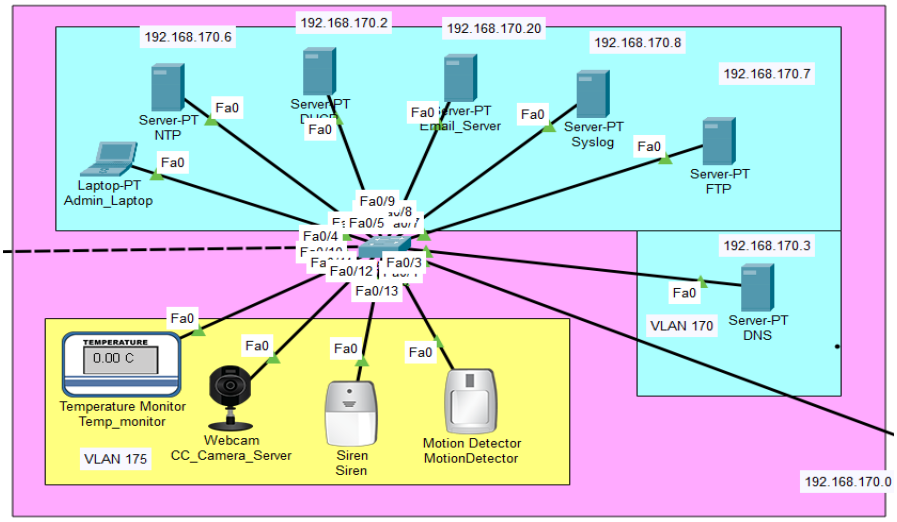

fig. 2. iot technology in server room

Fig. 2. Demonstrates the importance of IoT technology in managing and monitoring server rooms. Server rooms require optimal conditions to ensure smooth operation, making it important to maintain stability and efficiency [9]. IoT devices play a key role in achieving these objectives. IoT sensors monitor temperature, humidity, air quality, and air pressure, providing realtime data to prevent equipment failures due to overheating. Additionally, IoT devices monitor server usage, network traffic, and security, improving resource allocation and detecting potential security breaches.

Overall, the integration of IoT technology in server rooms is essential for maintaining optimal conditions, preventing equipment failures, and improving efficiency and security. By leveraging the power of IoT devices, businesses and organizations can ensure the smooth operation of their IT infrastructure and avoid costly downtime.

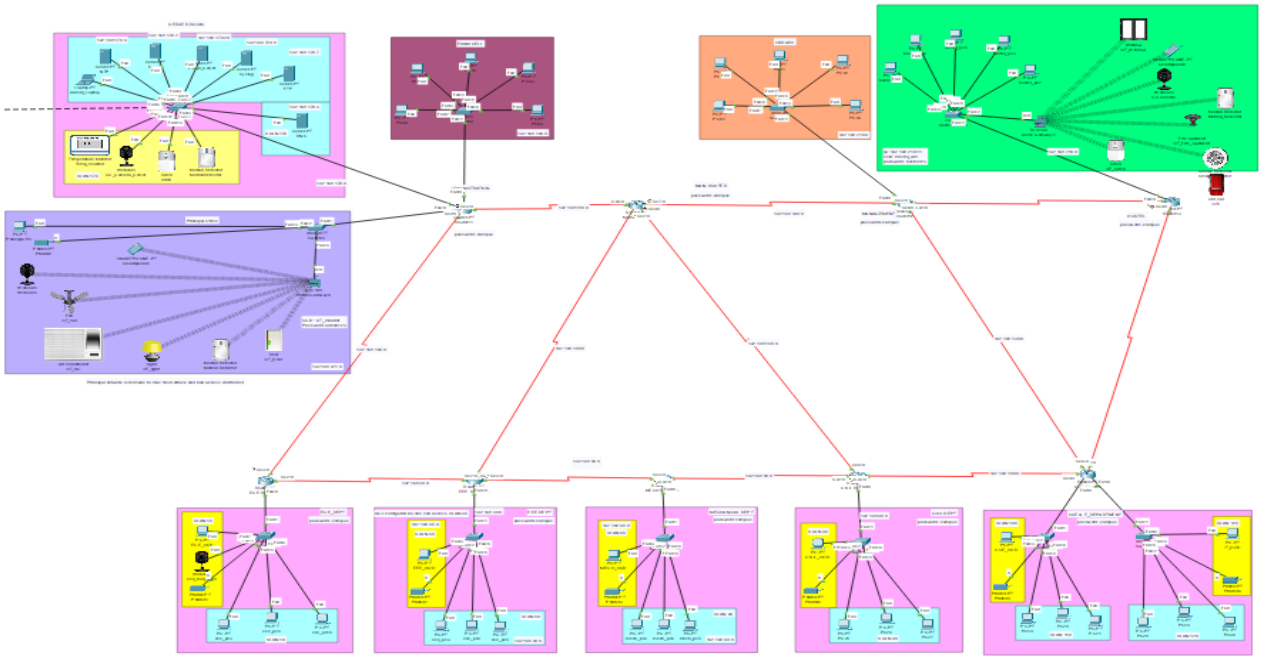

fig. 3. campus area network architecture

IV. RESULTS AND DISCUSSION

Secure campus area network (CAN) can provide a range of benefits for businesses and organizations. A properly configured CAN with VLANs, firewalls, and access control lists can enhance security, improve network performance, and provide better control over network access.

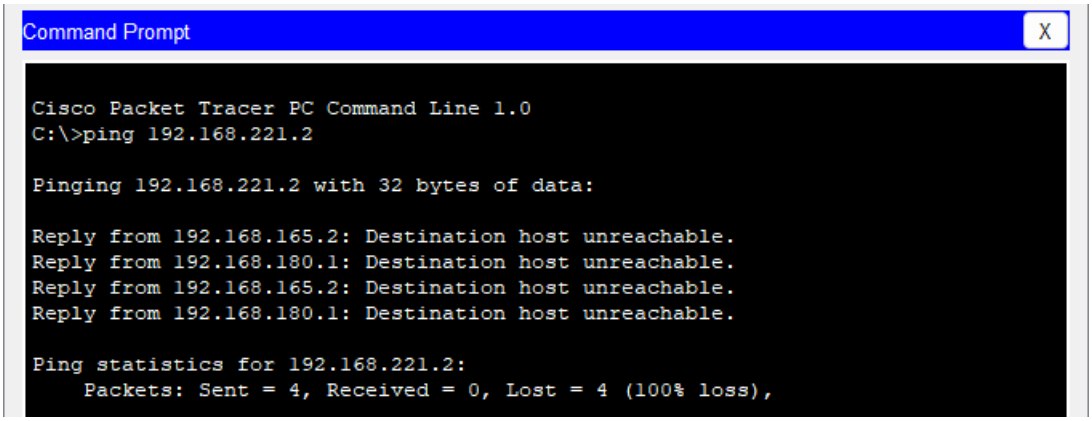

fig. 4. blocking ping requests using acl and vlan

The use of VLANs can segment the network, reducing the impact of security breaches and containing attacks. Firewalls can monitor and control traffic, protecting against unauthorized access, malware, and hacking attempts. Access control lists can restrict network access to authorized users and devices, further strengthening network security as demonstrated in Fig. 4.

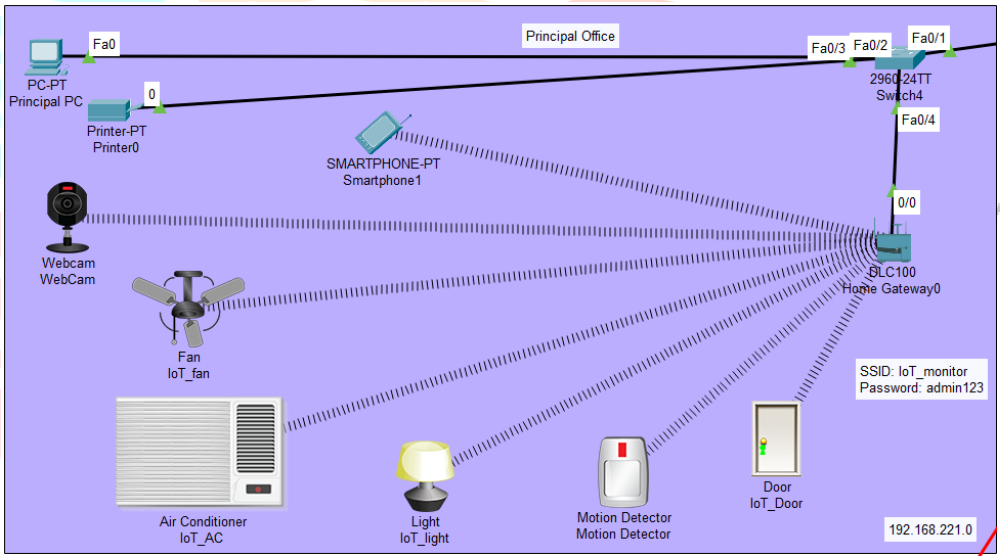

fig. 5. iot technology to improve physical security

The automation of several processes through IoT devices such as lighting and HVAC systems can enhance energy efficiency in campus networks. The automation also leads to cost savings for the institution. The incorporation of IoT devices in the campus area network can improve the security of the network and the physical premises. As demonstrated in Fig. 5. devices like motion sensors, cameras, and access control systems can detect and prevent unauthorized access to the network.

```
Switch#sh mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0030.a31a.e388    STATIC      Fa0/2
   1    0040.0b1a.6401    DYNAMIC     Fa0/4
   1    00e0.a3d9.5e14    STATIC      Fa0/1
Switch#
```

fig. 6. mac address table

Better control over network access is another benefit of a secure CAN. It helps in preventing MAC flooding by limiting the number of MAC addresses that can be learned on a specific port. This can be achieved by using the "switchport port-security maximum" command followed by the maximum number of MAC addresses that can be learned on the port as shown in Fig. 6.

V. CONCLUSION

We presented a secure area network scenario designing and simulating utilizing the Cisco packet tracer tool to raise the security level in the network's system, particularly on campuses. In this paper, a topology with eight buildings, various networks, and various kinds of devices is presented. We divide the end devices into various VLANs in few buildings for security reasons. In order to prevent outside or unauthorized accesses, we also deployed security approaches to the switches and routers that link the networks and the end devices with one another. This paper also demonstrates the true importance of some protocols in connecting and safeguarding the entire campus network. Future additions to this network architecture include IDS/IPS, which can be used to detect and prevent adversary attacks, as well as a web application firewall, which can shield web applications from unwanted traffic and attacks.

VI. ACKNOWLEDGMENT

We would like to express our heartfelt gratitude to Dr. R Uma Mageswari for her invaluable guidance and support throughout the research process. We would also like to acknowledge Akhilendranath Mummadi for proposing the idea behind this research project. Our sincere appreciation goes out to B. Midhunkrishna Yadav for conducting the experiments and providing valuable insights into the data analysis. Finally, we would like to thank Vishnu Vardhan Ciripuram for his efforts in writing this paper. We are grateful for their support and collaboration in this endeavor.

REFERENCES

[1] S. Sudharsan, M. Naga Srinivas, G. Sai Shabareesh, P.Kiran Rao , " CAMPUS NETWORK SECURITY AND MANAGEMENT " , International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 6, November - December 2014 , pp. 052-056 , ISSN 2278-6856.

[2] Ahmed, Alaa & Al-Hamadani, Mokhaled. (2021). Designing a secure campus network and simulating it using Cisco packet tracer. Indonesian Journal of Electrical Engineering and Computer Science. 23. 479-489. 10.11591/ijeecs.v23.i1.pp479-489.

[3] Sita, K., Akram, P. S., Javvaji, K. H., & Attota, T. P. (EasyChair, 2019). Design and implementation of Smart Campus Network. EasyChair Preprint no. 1882.

[4] Jagdish K.P & Pavan Kumar, 'Enhancing the College Network', Department of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Banglore IJIRSET- International Journal of Innovative Research in Science, Engineering & Technology, ISSN(online):2319-8753, Vol.7, May 2018.

[5] Milind V. Mahajan1 , Gaurav P. Sonar2 , Dharmendra P. Suralkar3 , Gaurav K. Ranmore4 , Pro. Pooja V. Naval5, "Cisco Packet Tracer for an Enterprise Network Infrastructure", IJIRE-V3I02-214-217.

[6] Rahman, Md. Toufiqur & Fatima, Kaniz & Shompa, Anny & Jabiullah, Md. Ismail & Student,. (2019). Securing a LAN by using Router through VLAN and ACL.

[7] Ali, Md. Nadir. (2015). Design and Implementation of a Secure Campus Network. Journal of Surface Engineered Materials and Advanced Technology. 5.

[8] A.T, Jeevanandham & P, Sivamurgan. (2020). IoT Based Automatic Fire Alarm System. Bulletin of Scientific Research. 2. 29-34. 10.34256/bsr2015.

[9] Barik, Lal. (2019). IoT based Temperature and Humidity Controlling using Arduino and Raspberry Pi. International Journal of Advanced Computer Science and Applications. 9. 494-502. 10.14569/IJACSA.2019.0100966.

[10] Ali, Md. Nadir. (2015). "Design and Implementation of a Secure Campus Network." Journal of Surface Engineered Materials and Advanced Technology. 5.

[11] Abdi, A. (2018). Designing Smart Campus Using Internet of Things.

[12] L. Senecal, "Understanding and preventing attacks at layer 2 of the OSI reference model," 4th Annual Communication Networks and Services Research Conference (CNSR'06), 2006, pp. 1 pp.-, doi: 10.1109/CNSR.2006.57.