**“Securing and increasing productivity of BYOD in classrooms at school”**

## A PROJECT REPORT

***Submitted by,***

|  |  |  |
| --- | --- | --- |
| Sl. No. | Roll Number | Student Name |
| 1 | 20211CSE0168 | B Jashwanth Reddy |
| 2 | 20211CSE0477 | S Kavya Sree |
| 3 | 20211CSE0472 | Gopi Priya G |
| 4 | 20211CSE0473 | O Nagendra Babu |

### *Under the guidance of,*

Ms. Nithya B.A

School of Computer Science,

Presidency University, Bengaluru

***in partial fulfillment for the award of the degree of***

**BACHELOR OF TECHNOLOGY IN**

**COMPUTER SCIENCE AND ENGINEERING, COMPUTER ENGINEERING, INFORMATION SCIENCE AND ENGINEERING**

**At**



**PRESIDENCY UNIVERSITY**

**BENGALURU**

**DECEMBER 2024**

**PRESIDENCY UNIVERSITY**

**SCHOOL OF COMPUTER SCIENCE ENGINEERING**

**CERTIFICATE**

This is to certify that the Project report **“Securing and increasing productivity of BYOD in classrooms at school”** being submitted by “B Jaswanth Reddy, S Kavyasree, Gopi Priya G, Nagendra Babu” bearing roll number(s) “20211CSE0168,20211CSE0477,20211CSE0472,20211CSE0473” respectively in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering is a Bonafide work carried out under my supervision.

|  |  |
| --- | --- |
| **Ms. NITHYA B A**  ASSISSTANT PROFESOR  School of CSE&IS  Presidency University | **Dr. ASIF MOHAMMED**  PROFESSOR & HoD  School of CSE&IS  Presidency University |

|  |  |  |
| --- | --- | --- |
| **Dr. L. SHAKKEERA**  Associate Dean  School of CSE  Presidency University | **Dr. MYDHILI NAIR**  Associate Dean  School of CSE  Presidency University | **Dr. SAMEERUDDIN KHAN**  Pro-Vc School of Engineering  Dean -School of CSE&IS  Presidency University |

**PRESIDENCY UNIVERSITY**

**SCHOOL OF COMPUTER SCIENCE ENGINEERING**

**DECLARATION**

We hereby declare that the work, which is being presented in the project report entitled **Securing and increasing productivity of BYOD in classrooms at school** in partial fulfillment for the award of Degree of **Bachelor of Technology** in **Computer Science and Engineering**, is a record of our own investigations carried under the guidance of **NITHYA B A, Assistant Professor,** **School of Computer Science Engineering & Information Science, Presidency University, Bengaluru.**

We have not submitted the matter presented in this report anywhere for the award of any other Degree.

**Name: Roll No: Signature:**

|  |
| --- |
| **B Jashwanth Reddy 20211CSE0168**  **S Kavya Sree 20211CSE0477**  **Gopi Priya G 20211CSE0472**  **O Nagendra Babu 20211CSE0473** |
|  |

**TABLE OF CONTENTS**

|  |  |
| --- | --- |
| **Abstract** | **6** |
| **1.INTRODUCTION** | **8** |
| 1.1 Motivation | **8** |
| 1.2 Problem Statement | **8** |
| 1.3 Objective of the Project | **8** |
| 1.4 Scope | **8** |
| 1.5 Project Introduction | **8** |
| **2.LTERATURE SURVEY** | **9** |
| 2.1 Related Work | **10-33** |
| **3. SYSTEM ANALYSIS** | **10-33** |
| 3.1 Existing System | **10-33** |
| 3.2 Disadvantages | **10-33** |
| 3.3 Proposed System | **10-33** |
| 3.4 Advantages | **10-33** |
| 3.5 work Flow of Proposed system | **10-33** |
| **4. REQUIREMENT ANALYSIS** | **34** |
| 4.1Function and non-functional requirements | **34** |
| 4.2 Hardware Requirements | **34** |
| 4.3 Software Requirements | **34** |
| 4.4 Architecture | **34** |
| **5.TIMELINE OF THE PROJECT** | **40** |
| **6.OUTCOMES** | **41** |
| **7.RESULTS AND DISCUSSIONS** | **42** |
| **8.CONCLUSION** | **43** |
| **9.REFERENCES** | **44** |
| **10.PSEUDOCODES** | **45-46** |
| **11.SCREENSHOTS** | **47-48** |

**ABSTRACT**

This project seeks to address the growing trend of Bring Your Own Device (BYOD) initiatives in educational institutions. While BYOD enhances learning by allowing students to use familiar personal devices, it also poses significant challenges to school networks, including data security risks, compliance with privacy regulations, network congestion, and the potential for students to access distracting or harmful content.

The primary goal of the project is to create a secure and productive learning environment tailored to the needs of modern classrooms. The system will incorporate a **robust security framework** that safeguards sensitive school data, prevents unauthorized access, and ensures compliance with privacy laws such as GDPR, FERPA, or local equivalents.

To enhance **productivity**, the system will include **web filtering software** that blocks inappropriate or distracting content while allowing access to educational resources. Teachers will have fine-grained control over what websites or tools can be accessed, ensuring alignment with lesson plans. Additionally, the integration of **real-time analysis firewalls** will allow for dynamic threat detection and prevention, mitigating risks such as malware, phishing attacks, or excessive bandwidth usage.

The project will leverage **cloud services** to ensure cost efficiency, scalability, and ease of deployment. Cloud-based tools allow for centralized management of the BYOD system, enabling schools to monitor network performance, enforce policies, and adapt to changing requirements without investing heavily in on-premises infrastructure. Moreover, **real-time monitoring and feedback mechanisms** will be implemented to assess the effectiveness of the system, identify weaknesses, and allow for continuous improvements.

By integrating these features, the project aims to strike a balance between maintaining a secure network and allowing students the flexibility to use their personal devices productively. The result will be a seamless, secure, and efficient environment that supports both educational goals and technological advancements, ultimately fostering better engagement and collaboration in the classroom.

**ACKNOWLEDGEMENT**

First of all, we indebted to the **GOD ALMIGHTY** for giving me an opportunity to excel in our efforts to complete this project on time.

We express our sincere thanks to our respected dean **Dr. Md. Sameeruddin Khan**, Pro-VC, School of Engineering and Dean, School of Computer Science Engineering & Information Science, Presidency University for getting us permission to undergo the project.

We express our heartfelt gratitude to our beloved Associate Deans **Dr. Shakkeera L and Dr. Mydhili Nair,** School of Computer Science Engineering & Information Science, Presidency University, and “**Dr. ASIF MOHAMMED**”, Head of the Department, School of Computer Science Engineering & Information Science, Presidency University, for rendering timely help in completing this project successfully.

We are greatly indebted to our guide **Ms. NITHYA B A** and Reviewer **Dr.Prakash S**, School of Computer Science Engineering & Information Science, Presidency University for his inspirational guidance, and valuable suggestions and for providing us a chance to express our technical capabilities in every respect for the completion of the project work.

We would like to convey our gratitude and heartfelt thanks to the PIP2001 Capstone Project Coordinators **Dr. Sampath A K, Dr. Abdul Khadar A and Mr. Md Zia Ur Rahman,** department Project Coordinators and Git hub coordinator **Mr. Muthuraj.**

We thank our family and friends for the strong support and inspiration they have provided us in bringing out this project.

**B Jashwanth Reddy 20211CSE0168**

**S Kavya Sree 20211CSE0477**

**Gopi Priya G 20211CSE0472**

**O Nagendra Babu 20211CSE0473**

**CHAPTER-1**

**INTRODUCTION**

The problem statement revolves around the growing trend of schools allowing students to bring their own devices (like laptops, smartphones, or tablets) for educational purposes. As more teachers encourage the use of online resources, with content being enriched by videos, interactive activities, and even exams conducted digitally, there arises a need for increased control over what students can access during class.

Teachers need a way to manage and filter the online content that students access in order to keep the learning process focused and aligned with the curriculum. For example, during a lesson, teachers might want to restrict access to non-educational websites, such as social media or gaming platforms, to maintain productivity and ensure that students are not distracted.

The solution involves building a web portal that gives schools the ability to empower teachers with control over web access. This portal will allow teachers to filter or block specific websites based on the identity of the students, such as their names or classes. The system would be integrated with the school’s wireless network and utilize device and username information gathered from wireless access points. A firewall or other filtering mechanism would then apply the desired restrictions on internet usage for each student.

This type of system would significantly help teachers in guiding students through their learning journey in a more controlled digital environment while ensuring the content they access aligns with the educational goals.

**CHAPTER-2**

**LITERATURE SURVEY**

Existing Methods for Web Access Control in Educational Environments:

In today's digital age, schools are increasingly adopting technology-driven learning approaches. The Bring Your Own Device (BYOD) model in schools, where students use their personal devices for academic purposes, introduces new challenges in controlling access to online content. To address these challenges, several existing methods and technologies have been implemented to monitor and filter students’ internet activities. Below is an overview of 8-10 methods with their advantages and limitations in the context of web access control in educational environments.

1. **Router-Based Content Filtering:**

Router-based content filtering is a common method used in educational environments to control and monitor the web traffic within a school’s network. This approach involves configuring the school’s internet routers to block or allow access to specific websites or categories of websites. Router-based filtering typically works by inspecting the destination IP addresses, domain names, or URL patterns of the traffic passing through the router, and applying rules that either block or permit the traffic based on predefined criteria.

**How It Works:**

* Configuration on Routers: The school’s network administrator configures the router with a set of filtering rules. These rules can be set at different levels, such as blocking certain categories (e.g., "social media," "adult content") or specific domains (e.g., "facebook.com").
* Traffic Monitoring: The router continuously monitors the incoming and outgoing traffic based on its configuration. When a user tries to access a website, the router checks the request against the predefined filters.
* Decision Making: If the request matches a blocked domain or category, the router denies access, usually sending an error or a blocked page to the user. If the request is allowed, the traffic is routed to the destination without interruption.
* Real-time Updates: Some routers offer real-time filtering services that can be updated dynamically, meaning that administrators can block newly identified inappropriate content almost instantly.

**Advantages of Router-Based Content Filtering:**

**1.Centralized Control:** Since routers are the gateway to the internet for all devices in the network, applying filtering rules at this level ensures that the entire network is subject to the same policies. This provides centralized control for the school’s IT department, simplifying the management process.

**2.No Need for Client Software:** One of the biggest advantages of router-based filtering is that it requires no software installation on individual student devices. This makes it suitable for a BYOD (Bring Your Own Device) environment, where students bring their personal devices (laptops, tablets, smartphones) to school.

**3.Category-Based Filtering:** Most router filtering systems come with pre-defined categories of content that can be blocked, such as adult content, gambling, social media, or streaming services. This makes it easier for schools to enforce broad policies without having to specify each individual website.

**4.Scalability:** Router-based filtering scales well with the size of the network. Whether a school has 50 or 500 devices connected, the same router rules apply network-wide, making it easier to manage larger networks.

**5.Low Maintenance**: Once set up, router-based filtering systems require minimal day-to-day intervention. Administrators only need to adjust the filters when new rules are required or if new categories need to be added.

**6.Blocking Malicious Content:** Many routers also come with security features that block access to known malicious sites (such as phishing or malware-infected websites), thus helping to protect the school network from cybersecurity threats.

**Limitations of Router-Based Content Filtering:**

**1.Lack of Granular Control:** Router-based filtering typically applies rules to the entire network or specific subnets, which means that it is difficult to tailor the filtering to individual users or classes. For example, it might block access to social media for everyone, including teachers who might need to access it for instructional purposes.

**2.Bypassing Filters**: Tech-savvy students may find ways to bypass router-based filters using VPNs (Virtual Private Networks), proxies, or even custom DNS (Domain Name System) settings. Once they bypass the filter, they can access restricted content.

**3.Limited Contextual Control:** Router-based filtering usually relies on domain name or IP address filtering and does not provide content-level filtering within a website. For instance, it can block access to YouTube entirely, but it cannot block specific inappropriate videos while allowing access to educational content on the same platform.

**4.No Real-Time Control for Teachers:** Unlike systems designed specifically for classroom management (such as teacher-controlled filtering tools), router-based filters do not offer real-time control for teachers to block or allow websites during lessons. Any changes need to be made by the network administrator, which can be inefficient during live classroom sessions.

**5.Overblocking:** Depending on the level of filtering, router-based systems may block legitimate educational websites that share domains or categories with inappropriate content. For example, a router may block all forums, even those used for academic collaboration, or all gaming websites, even educational ones.

**6.Difficulty in User Identification:** Router-based filters usually don’t differentiate between users on the same network. Without additional infrastructure, it’s difficult to apply different rules to different users (such as allowing a teacher to access a website that is blocked for students).

**7.DNS Bypass:** Some students may bypass the router filters by changing their device’s DNS settings to a public DNS service (like Google’s or Cloudflare’s DNS), which might allow them to access blocked websites.

**Best Practices for Router-Based Content Filtering:**

To maximize the effectiveness of router-based content filtering, schools can implement the following best practices:

* **Combining with User Authentication**: Integrate the filtering system with user authentication (e.g., LDAP, RADIUS) to apply different rules to different user groups (e.g., students vs. teachers).
* **Regular Rule Updates**: Periodically update filtering rules to account for new websites or changing educational needs. This could also involve enabling dynamic updates from trusted content filtering providers.
* **Use of Layered Filtering**: Combine router-based filtering with other content filtering solutions, such as endpoint protection or browser-based filtering, to provide a multi-layered defence against inappropriate content and cyber threats.
* **Monitoring and Reporting**: Use routers that provide detailed reports on web activity, allowing administrators to monitor what websites are being accessed and by whom. This helps in identifying misuse and fine-tuning the filtering rules.
* **Blocking VPNs and Proxies**: To prevent students from bypassing filters, block access to known VPNs and proxy websites. Many advanced routers offer this feature by default.

1. **Firewalls with URL Filtering:**

Firewalls with URL filtering play a crucial role in controlling and securing internet access within educational environments, especially in schools adopting BYOD (Bring Your Own Device) models. A firewall acts as a barrier between a trusted internal network and external networks (such as the internet), and URL filtering is a key feature that enables it to block or allow specific websites based on their URLs. This method is often used to restrict access to inappropriate or distracting content, thereby maintaining a focused and safe online environment for students.

**How Firewalls with URL Filtering Work**

Firewalls with URL filtering operate by inspecting outgoing web requests from users within the network. When a student, teacher, or administrator tries to access a website, the firewall examines the URL and compares it to a list of rules or categories of URLs that are either allowed or blocked. This can be done in several ways:

1. **Static URL Lists:** These are pre-configured lists of URLs (domains or subdomains) that are blocked or allowed. For example, a school might block social media websites like "facebook.com" and "twitter.com."
2. **Category-Based Filtering**: URL filtering services often categorize websites into predefined groups such as "Education," "Social Media," "Adult Content," "Streaming Services," etc. The firewall can be configured to block entire categories based on the school's policy.
3. **Real-Time Analysis**: Some advanced firewalls use real-time analysis to evaluate URLs and dynamically classify or block access based on the content or behavior of the website. This is useful for catching newly created or unknown sites.
4. **Keyword-Based Filtering:** URL filtering can also operate based on specific keywords. If a URL contains certain forbidden words or phrases (e.g., “games,” “adult,” etc.), it will be blocked, even if it has not been explicitly listed.
5. **User or Group-Based Rules**: URL filtering can be applied differently based on user roles. For example, students may have strict restrictions, while teachers may have more lenient access to online resources.

**Advantages of Firewalls with URL Filtering:**

1. **Centralized and Scalable Control:** A firewall provides a centralized control point for URL filtering across the entire school network. Any device that connects to the network will automatically be subject to the firewall’s filtering rules without requiring individual configurations on each device.
2. **Customizable Policies:** URL filtering policies can be customized based on the needs of the school. Schools can choose to block certain categories of websites (such as gaming or adult content) while allowing educational or academic resources. This flexibility ensures that the filtering aligns with the curriculum and the school’s code of conduct.
3. **Improved Security**: URL filtering helps prevent students from accessing dangerous or malicious websites that may contain malware, phishing attacks, or other cybersecurity threats. By blocking known malicious sites, firewalls act as a security layer, protecting the school network and devices.
4. **User and Group Management:** URL filtering on firewalls can be user-specific, meaning different access rules can be applied based on user authentication. For example, teachers can be allowed to access educational YouTube videos, while students are restricted. This granular control is important in a school setting where students, teachers, and administrators need different levels of access.
5. **Low Maintenance for Basic Filtering:** Once configured, URL filtering can require minimal day-to-day maintenance. Most firewalls with URL filtering offer automated updates to filtering lists (e.g., lists of newly discovered malicious websites or inappropriate content categories), ensuring that the filtering rules stay current.
6. **Real-Time Blocking**: URL filtering can be done in real-time, meaning that as soon as a user attempts to visit a blocked website, they are immediately prevented from accessing it. This is critical for keeping students focused during lessons and for preventing inappropriate content from being viewed at any time.
7. **Monitoring and Reporting:** Firewalls often provide detailed logs and reports on user activity. Administrators can see which websites were attempted, who tried to access them, and whether the attempt was blocked. This reporting is helpful for ensuring compliance with school policies and identifying patterns of misuse**.**

**Limitations of Firewalls with URL Filtering:**

1. **Granularity Issues:** Although URL filtering can be applied based on categories, it sometimes lacks the granularity to allow specific pages on a website while blocking others. For example, a school may want to block entertainment videos on YouTube while still allowing access to educational content. However, URL filtering at the firewall level might block the entire site.
2. **Potential for Overblocking:** URL filtering can lead to overblocking if categories are too broad or if the filtering system misclassifies a legitimate educational resource. For example, blocking "games" might inadvertently block educational gamification platforms that are part of the learning experience.
3. **Bypassing Filters: Tech**-savvy students can sometimes bypass URL filtering by using VPNs, proxies, or alternative DNS servers. This can be a significant challenge for administrators, especially in a BYOD environment where students have more control over their personal devices.
4. **Difficulty with Encrypted Traffic (HTTPS):** Many modern websites, especially major platforms like Google and social media, use HTTPS encryption. URL filtering systems must either decrypt the traffic to inspect it, which can raise privacy and performance concerns, or rely on basic domain-level filtering, which is less effective. Some advanced firewalls include HTTPS inspection capabilities, but this can slow down the network and is resource-intensive.
5. **Maintenance of Blacklists and Whitelists:** While many firewalls come with pre-configured URL lists, they still require some level of manual maintenance. Schools may need to create custom whitelists to ensure that certain educational resources are not blocked, or update blacklists to block new threats or inappropriate content.
6. **Cost:** Advanced firewalls with sophisticated URL filtering capabilities can be costly, both in terms of initial investment and ongoing subscription fees for real-time updates and support. Schools with limited budgets may find it difficult to justify the cost, especially if additional features such as deep packet inspection or intrusion detection are needed.
7. **Bandwidth Overhead:** Implementing URL filtering can introduce some overhead to network bandwidth, especially if real-time content inspection is enabled or if HTTPS traffic is being decrypted and inspected. This can slow down the overall network performance, particularly in schools with a high number of connected devices.
8. **User Identification Challenges:** While firewalls can enforce URL filtering rules for the entire network, identifying individual users can be difficult if the system isn’t integrated with a directory service or other authentication mechanism. Without user identification, the same filtering rules apply to all users, regardless of role (student, teacher, or administrator).

**Best Practices for Effective URL Filtering with Firewalls:**

To ensure that URL filtering is both effective and manageable in a school environment, the following best practices should be considered:

* **Use Category-Based Filtering:** Start with broad categories to block inappropriate content (e.g., adult content, gaming, streaming services). Fine-tune the rules over time by adding or removing specific sites based on feedback from teachers and students.
* **Enable User Authentication**: Integrate the firewall with a user authentication system (such as LDAP, Active Directory, or RADIUS) to apply different filtering rules for students, teachers, and staff. This ensures that teachers have access to resources they need while students remain restricted.
* **Combine with Other Tools:** URL filtering should not be the only line of defense. It works best when combined with other content control tools, such as endpoint security software, browser-based filtering, or classroom management systems that give teachers real-time control over student access.
* **Implement HTTPS Inspection with Caution:** If the firewall supports HTTPS inspection, consider enabling it for high-risk categories like "malware" or "phishing" to increase security. However, ensure that the performance impact is manageable and that privacy concerns are addressed.
* **Regularly Review and Update Policies:** URL filtering policies should be regularly reviewed and updated to reflect the evolving needs of the curriculum, new online threats, and feedback from teachers and students. Ensure that any blocked legitimate educational content is whitelisted promptly.
* **Monitor and Report:** Utilize the reporting features of the firewall to track blocked attempts and network usage patterns. This data can help in refining policies, identifying potential security issues, and ensuring that the filtering system is effective without being too restrictive.

**3.Network Access Control (NAC):**

Network Access Control (NAC) is a comprehensive approach used by organizations to enhance the security of their internal network by managing how devices and users access the network. In a school environment with BYOD (Bring Your Own Device) policies, NAC becomes especially important for controlling and monitoring student and teacher devices that connect to the school’s network. It allows administrators to define and enforce policies governing device access, ensuring that only authorized users and compliant devices can connect to the network.

**How Network Access Control (NAC) Works:**

NAC solutions typically combine several functions to ensure that only secure and authorized devices can connect to the network. The process often follows these steps:

1. **Authentication:** When a device attempts to connect to the school’s network (wired or wireless), the NAC system verifies the identity of the user. This can be done through several methods such as usernames and passwords, multi-factor authentication (MFA), or certificates issued by the school’s IT department.
2. **Endpoint Compliance Check:** Once the user is authenticated, the NAC system checks the device for compliance with the school’s security policies. This might include verifying that the device has up-to-date antivirus software, security patches, or a specific firewall enabled. Devices that fail to meet these criteria may be denied access or placed into a restricted area of the network (e.g., guest network).
3. **Access Control:** After the device is authenticated and compliance is verified, NAC grants access to the network based on predefined policies. These policies can be as granular as needed, controlling which parts of the network users can access. For example, students may only have access to educational resources, while teachers have access to administrative systems.
4. **Continuous Monitoring:** NAC systems do not just check the device at the point of entry but can continuously monitor the behavior of connected devices. If a device's security status changes (e.g., a malware infection is detected), NAC can dynamically adjust the device's network permissions or remove it from the network entirely.
5. **Role-Based Access Control (RBAC):** NAC allows administrators to apply different access levels based on the user’s role (e.g., student, teacher, or guest). A student’s device might be restricted to educational websites, while a teacher’s device might have more flexibility. This ensures a secure, role-specific access policy across the school.
6. **Guest Management:** NAC also provides features for managing guest devices. For example, visitors or temporary users might be granted access to a separate guest network that is isolated from the main school network. NAC solutions can provide a temporary password or authentication method for these guests.

**Advantages of Network Access Control (NAC):**

1. **Improved Network Security:** NAC ensures that only authorized and compliant devices can access the school’s network, reducing the risk of malware, viruses, and unauthorized access. By enforcing security policies, NAC reduces the attack surface and protects sensitive data from potential threats.
2. **Control Over BYOD:** With more schools allowing students to bring their own devices, NAC provides a way to control and monitor these devices without having to manage them directly. This helps ensure that personal devices adhere to the school’s security standards before they are granted access to the network.
3. **Granular Access Control:** NAC allows for fine-grained control over which resources different types of users can access. By segmenting the network, schools can prevent unauthorized access to sensitive systems (e.g., administrative databases or test servers) while allowing general network access for students.
4. **Enforcing Security Policies:** NAC solutions enforce compliance by ensuring that all devices connecting to the network meet specific security requirements. For example, devices must have updated antivirus software, current operating system patches, or specific configuration settings like firewalls or encryption. This helps reduce vulnerabilities in the network.
5. **Real-Time Monitoring and Remediation:** NAC provides continuous monitoring of connected devices. If a device becomes non-compliant or suspicious activity is detected (such as unusual traffic patterns or malware infection), the NAC system can isolate the device, limit its access, or disconnect it from the network entirely. This allows for real-time responses to potential threats.
6. **Guest and Third-Party Management:** NAC allows schools to securely manage guest users, contractors, or temporary staff. These individuals can be given limited, time-based access to certain parts of the network, ensuring they do not have unrestricted access to sensitive data or systems.
7. **Simplified User Authentication:** NAC often integrates with authentication systems such as LDAP, Active Directory, or RADIUS, enabling single sign-on (SSO) or certificate-based authentication. This simplifies access for students and teachers, while also allowing for more secure and consistent authentication processes.
8. **Reporting and Auditing:** NAC systems generate detailed reports and logs on network access, device compliance, and user behaviour. This helps administrators track who is accessing the network, when, and from which device. It can also be used to identify and address policy violations or potential security incidents.

**Limitations of Network Access Control (NAC):**

1. **Complexity in Implementation**: NAC systems can be complex to implement, particularly in large schools with many different devices and user types. Configuring and fine-tuning the policies to ensure that legitimate devices can access the network while keeping unauthorized devices out can be challenging.
2. **Compatibility Issues**: Not all devices may be fully compatible with NAC solutions, particularly older devices or those that do not support modern authentication methods. Ensuring that all devices (including smartphones, tablets, and laptops) can be seamlessly integrated into the NAC system may require additional resources.
3. **User Friction**: While NAC improves security, it can also introduce some friction for users, particularly in BYOD environments. Students or teachers may be frustrated if their devices are denied access due to non-compliance, especially if they are not tech-savvy or if the school’s IT support is slow to respond.
4. **Resource-Intensive:** NAC systems can be resource-intensive to operate and maintain. They often require regular updates to security policies, monitoring of device compliance, and troubleshooting of access issues. Schools with limited IT staff may struggle to fully manage and benefit from NAC.
5. **Cost:** NAC solutions, especially advanced ones, can be expensive to purchase and deploy. Schools with limited budgets may find it difficult to justify the costs, particularly when also considering the need for ongoing maintenance, updates, and staff training.
6. **Potential for Network Bottlenecks**: As NAC continuously monitors devices and enforces security policies, it can introduce some performance overhead. If not properly optimized, this could result in slower network performance, particularly during high-traffic periods (e.g., when multiple students are connecting to the network simultaneously).
7. **Evasion Techniques**: Skilled users may attempt to bypass NAC restrictions by using techniques such as MAC address spoofing, unauthorized network adapters, or VPNs. While NAC systems are generally effective at detecting and blocking such attempts, these evasion techniques remain a potential vulnerability.

**Best Practices for Effective NAC Deployment:**

To ensure that NAC solutions are deployed effectively in schools, certain best practices should be followed:

1. **Start with Clear Policies**: Define and document network access policies that outline which devices are allowed to connect, what security standards must be met, and what resources different user roles can access. Clear policies are essential to ensure that NAC works smoothly and meets the school’s security needs.
2. **Segment the Network**: Use network segmentation to isolate different types of devices and users. For example, place student devices on a different VLAN than teacher or administrative devices. This limits the potential for unauthorized access or security breaches.
3. **Regular Compliance Checks**: Ensure that NAC systems perform regular compliance checks on devices, not just during initial connection but throughout the session. This helps detect devices that may become non-compliant after gaining access (e.g., due to malware infection or outdated software).
4. **Integrate with Authentication Systems:** Use existing directory services (such as Active Directory or LDAP) to manage user authentication. This makes it easier to apply role-based access control and ensures that only authenticated users are allowed onto the network.
5. **Provide Clear Instructions for BYOD Users:** Provide students and teachers with clear instructions on how to configure their devices to meet the school’s security requirements (e.g., installing antivirus software or enabling firewalls). Offer IT support to help users troubleshoot any access issues.
6. **Use a Layered Security Approach:** NAC should be part of a larger security strategy. Combine it with other security tools such as firewalls, intrusion detection/prevention systems (IDS/IPS), and endpoint protection to create a comprehensive defence-in-depth strategy.
7. **Monitor and Optimize Performance:** Regularly monitor the performance of the NAC system to ensure it does not create bottlenecks or slow down the network. Optimize policies and adjust thresholds to balance security and performance needs.

**4.Cloud-Based Web Filtering Services (e.g., Cisco Umbrella, Zscaler):**

Cloud-based web filtering services provide a flexible and scalable approach to controlling and monitoring internet access, particularly in educational environments where BYOD (Bring Your Own Device) is increasingly common. These solutions, such as **Cisco Umbrella** and **Zscaler**, enable schools to filter online content, protect against web-based threats, and enforce internet usage policies, all without the need for significant on-premise infrastructure.

Cloud-based filtering services operate by routing internet traffic through their cloud servers, where they apply filtering policies and security controls before allowing access. These services offer granular control over what websites students and staff can access, helping to ensure that online activity aligns with the educational goals and safety policies of the institution.

**How Cloud-Based Web Filtering Services Work:**

1. **DNS and Proxy-Based Filtering**: Cloud web filtering solutions often rely on DNS or proxy-based filtering to block access to malicious, inappropriate, or non-educational websites. Instead of the school’s network directly resolving domain names, DNS queries are routed through the cloud provider (e.g., Cisco Umbrella or Zscaler), which checks them against a database of categorized websites.
   * **DNS Filtering**: The service intercepts DNS requests from the school’s network and decides whether to allow or block access based on predefined policies. This method is lightweight and doesn’t require significant changes to network infrastructure.
   * **Proxy-Based Filtering**: In this approach, all web traffic is routed through the cloud service’s proxy server, which inspects and filters traffic based on URL categories, content, and security policies. This method offers more detailed control but can add more overhead than DNS-based filtering.
2. **Customizable Content Categories**: Most cloud-based web filtering solutions provide a broad range of content categories that administrators can enable or block. These categories typically include:
   * Adult content
   * Social media
   * Streaming media (YouTube, Netflix)
   * Online gaming
   * Malware and phishing sites
   * Educational resources Administrators can create custom policies for different groups, such as students, teachers, and administrative staff, allowing tailored access based on their roles.
3. **Threat Intelligence and Malware Protection**: In addition to content filtering, cloud services like Cisco Umbrella and Zscaler provide robust security features. They use global threat intelligence networks to identify and block access to malicious websites, phishing attacks, and sites hosting malware. This adds an additional layer of security, preventing students and teachers from accidentally accessing harmful content or falling victim to online threats.
4. **User and Device Identification**: Cloud-based filtering services typically integrate with existing directory services (such as Active Directory or LDAP) to apply policies based on user identity. This allows the school to enforce different filtering policies for students, teachers, or guests. Some services also support device-level filtering, enabling the enforcement of rules based on whether the device is a school-issued laptop, personal phone, or tablet.
5. **Reporting and Monitoring**: Detailed reporting is another core feature of cloud-based web filtering services. Schools can monitor internet usage, identify trends, and detect violations of internet use policies. Reports may include information on the most accessed websites, blocked requests, attempts to access restricted content, and potential security threats. Administrators can use these reports to ensure that students stay focused on educational activities and comply with the school's internet usage policies.
6. **BYOD and Off-Network Protection**: One of the significant advantages of cloud-based web filtering is its ability to protect devices even when they are not on the school network. Whether students or teachers are using personal devices at home or in a coffee shop, their internet traffic will still be routed through the cloud service, ensuring consistent filtering and protection across all environments.
7. **Easy Deployment and Scalability**: Cloud-based solutions require minimal on-premise hardware, making them easy to deploy and scale. Schools do not need to invest in or manage large firewalls or filtering appliances. As the number of users and devices grows, the service can scale to accommodate them without significant changes to the network infrastructure.

**Advantages of Cloud-Based Web Filtering Services:**

1. **Scalability**: Cloud-based filtering services are highly scalable, making them ideal for schools of all sizes. Whether a school has hundreds or thousands of students, the service can handle the increase in traffic and devices without additional hardware or complicated setup.
2. **Off-Network Protection**: Since cloud filtering is not tied to the school’s physical network, it can extend protection to devices used outside the school. Students’ personal devices or school-issued laptops will still be filtered regardless of location, ensuring compliance with school policies both on and off campus.
3. **Comprehensive Threat Protection**: Providers like Cisco Umbrella and Zscaler have robust security mechanisms to block access to known malware, phishing sites, and other web-based threats. These services often use global threat intelligence databases, providing real-time protection against emerging online threats.
4. **Easy Policy Management**: Administrators can easily create and manage internet usage policies using a cloud-based dashboard. Different groups (students, teachers, guests) can have different filtering rules, and these rules can be updated and applied instantly across the network.
5. **No On-Premise Infrastructure**: Cloud-based web filtering eliminates the need for schools to invest in and maintain expensive filtering hardware. All traffic is routed through the cloud, and policy enforcement occurs off-site. This not only saves costs but also simplifies management, especially for schools with limited IT staff.
6. **Real-Time Updates**: Cloud providers regularly update their databases of categorized websites and known threats. This ensures that schools are always protected against the latest malicious content or inappropriate material without requiring manual updates from the IT staff.
7. **Detailed Reporting and Insights**: Cloud-based services provide comprehensive reporting tools, giving schools deep insights into internet usage patterns. This helps in identifying inappropriate or non-educational behaviour, tracking attempts to access restricted sites, and generating reports for compliance or auditing purposes.
8. **Global Reach and Availability**: Cloud filtering services are available across different geographical locations and networks. This is particularly useful for international schools or students and teachers who may travel but still need to adhere to the institution’s policies.

**Limitations of Cloud-Based Web Filtering Services:**

1. **Dependence on Internet Connectivity**: Since these services are cloud-based, they rely on constant internet connectivity. Any disruptions in the internet connection may result in loss of filtering capabilities or delays in applying policies.
2. **Privacy Concerns**: Cloud-based filtering services inspect all internet traffic, which might raise privacy concerns, especially in environments where students and staff use personal devices. Schools must be transparent about how data is being monitored and stored by the cloud service provider.
3. **Latency**: Routing all internet traffic through a cloud-based filtering service can introduce additional latency, particularly in schools with slower internet connections or high traffic loads. This could potentially impact the user experience, especially during peak usage times.
4. **Costs**: While cloud-based services eliminate the need for hardware, they typically operate on a subscription model. Over time, these recurring costs can add up, particularly for larger schools or districts with many devices and users.
5. **Limited Customization**: Cloud-based filtering services may not offer the same level of granular control as on-premise solutions, such as firewall-based filtering. Some advanced or niche filtering requirements may not be fully supported in the cloud.
6. **False Positives and Overblocking**: There’s always the risk of overblocking, where legitimate educational content is mistakenly blocked by the filtering service. Similarly, false positives can prevent students from accessing research materials or useful information, impacting their learning experience.
7. **Bypass Techniques**: Tech-savvy students may find ways to bypass cloud-based filtering services, such as using proxy servers, VPNs, or Tor networks. While many cloud services offer mechanisms to block these tools, it’s an ongoing challenge to stay ahead of these evasion tactics.

**Best Practices for Deploying Cloud-Based Web Filtering:**

1. **Define Clear Policies**: Schools should have clear internet usage policies that are communicated to both students and staff. The cloud filtering system should be configured to enforce these policies while providing enough flexibility for legitimate educational activities.
2. **Enable Off-Network Protection**: Ensure that filtering policies apply to devices both on and off the school network. This is critical for maintaining consistent protection for BYOD devices and school-issued laptops.
3. **Monitor and Adjust Policies**: Regularly review internet usage reports to identify trends or potential issues. Adjust filtering policies as needed to balance security with educational access.
4. **Provide Transparent Communication**: Schools should inform users about what is being monitored, how data is used, and how filtering policies are applied. Transparency helps mitigate privacy concerns and fosters trust.
5. **Ensure Proper Bandwidth**: Given that all traffic is routed through the cloud service, ensure that your school has sufficient internet bandwidth to handle the additional load without causing performance issues.

**Layered Security Approach**: While cloud-based filtering is a powerful tool, it should be combined with other security measures such as firewalls, antivirus software, and user training to create a comprehensive security strategy.

**5.DNS-Based Filtering (e.g., OpenDNS):**

**DNS-based filtering** is a method of controlling and restricting internet access by filtering web traffic at the DNS (Domain Name System) level. It is widely used in schools, businesses, and homes to block inappropriate, malicious, or non-educational websites. One of the popular examples of this filtering technology is **OpenDNS** (now part of Cisco Umbrella), which allows administrators to block access to specific categories of websites based on DNS queries.

**How DNS-Based Filtering Works:**

DNS is the system that translates human-readable domain names (like [www.google.com](http://www.google.com)) into IP addresses that computers use to communicate with each other. DNS-based filtering works by intercepting and inspecting DNS requests made by a user's device before allowing or blocking access to the corresponding website.

When a user types a URL into their browser:

1. The browser sends a DNS request to resolve the domain name (e.g., "[www.example.com](http://www.example.com)") to its corresponding IP address.
2. The DNS-based filtering service (e.g., OpenDNS) intercepts the request and checks if the domain is categorized as allowed or blocked according to pre-configured policies.
   * If the website is allowed, the service returns the correct IP address, and the user can access the website.
   * If the website is blocked, the service either returns a blocked page or simply does not resolve the domain, preventing the user from accessing the content.

DNS-based filtering is particularly lightweight and easy to deploy, as it does not require installing hardware or software on individual devices. Instead, administrators need only configure the network’s DNS settings to use a filtering service like OpenDNS.

**Key Features of DNS-Based Filtering:**

1. **Content Categorization**: DNS filtering services categorize websites into different types (e.g., adult content, social media, gambling, malware, phishing). Administrators can block entire categories or allow exceptions for specific sites based on the institution’s needs.
2. **Custom Blacklists and Whitelists**: In addition to predefined content categories, administrators can create custom blacklists (blocked websites) and whitelists (allowed websites) to fine-tune their filtering policies.
3. **Threat Protection**: Many DNS filtering services, including OpenDNS, offer protection against known malware and phishing websites. They use threat intelligence databases to identify and block requests to malicious sites, adding an extra layer of security to the network.
4. **Policy Enforcement Across Networks**: DNS-based filtering can be applied at various levels, including the entire school network, specific subnets, or even individual devices. It is commonly used to enforce different policies for different groups, such as students, teachers, and guests.
5. **DNS Encryption**: To improve privacy and prevent DNS-based attacks like DNS spoofing, many DNS filtering services now support encrypted DNS queries via protocols like DNS over HTTPS (DoH) or DNS over TLS (DoT).
6. **Off-Network Filtering**: DNS-based filtering can also protect devices that are outside the school network. By using a roaming client or manually configuring devices to use the DNS service provider’s DNS servers, the filtering policies can be applied regardless of the device’s location.
7. **Detailed Reporting and Analytics**: DNS filtering services provide comprehensive reporting tools that allow administrators to monitor DNS requests, track blocked websites, and generate insights into browsing habits. This is especially useful in educational environments to ensure compliance with acceptable use policies and to identify inappropriate online behavior.

**Advantages of DNS-Based Filtering:**

1. **Simplicity of Deployment**: DNS-based filtering is easy to deploy, requiring only a change in the DNS settings on the school’s routers or DHCP servers. There’s no need for hardware appliances or endpoint software, making it a cost-effective solution for schools.
2. **Low Resource Overhead**: Because DNS filtering occurs before a web page is even loaded, it has minimal impact on network bandwidth and performance. This is especially important in large school environments with multiple devices accessing the network simultaneously.
3. **Network-Wide Protection**: DNS filtering can apply to all devices connected to the school’s network, including personal student devices (BYOD) and school-owned computers. It ensures uniform enforcement of internet access policies across the entire network.
4. **Cloud-Based Management**: Services like OpenDNS offer cloud-based dashboards, allowing administrators to manage filtering policies, monitor DNS traffic, and view reports from any location. This is especially useful for multi-campus schools or districts.
5. **Protection Against Malware and Phishing**: DNS-based filtering provides an additional layer of defence against cyber threats. By blocking access to known malicious websites, it helps prevent malware infections, phishing attacks, and other cyber threats.
6. **Customizable Filtering**: Administrators can create custom filters based on the specific needs of their school. For example, they can block social media during school hours or allow access to YouTube for educational purposes only.
7. **Off-Network Protection**: Many DNS-based filtering services offer the ability to extend protection beyond the school network. For example, OpenDNS allows the installation of a client agent that enforces filtering policies on devices even when they are off-campus.

**Limitations of DNS-Based Filtering:**

1. **Limited Granularity**: DNS filtering can only block entire domains (e.g., [www.facebook.com](http://www.facebook.com)), not individual web pages. This means that if an educational website shares a domain with non-educational content, blocking the entire domain might limit access to useful resources. It lacks the ability to block specific parts of websites, unlike more advanced URL-based filtering.
2. **No Content Inspection**: DNS-based filtering does not inspect the content of websites, such as images, videos, or file downloads. It operates solely on domain names, which may limit its ability to filter specific types of content that exist on allowed domains.
3. **Bypass Risks**: DNS-based filtering can be bypassed if users manually configure their devices to use alternative DNS servers. While some solutions provide mechanisms to block this behavior (e.g., forcing devices to use specific DNS servers), tech-savvy students may still find ways around the filtering.
4. **No SSL Inspection**: DNS-based filtering does not decrypt or inspect SSL-encrypted traffic. This means that if a blocked website is hosted on HTTPS, the DNS filter will block access to the entire domain, but it cannot examine the specifics of the request.
5. **Depends on DNS Servers**: DNS filtering is only effective if all DNS traffic goes through the configured DNS servers. If users or devices use other DNS resolvers, the filtering policies won’t apply, potentially leaving gaps in protection.
6. **Lack of Advanced Reporting**: While DNS-based filters offer basic reports on blocked websites and user activity, they may not provide as detailed insights as other filtering methods, such as proxy-based or firewall solutions. This can limit an administrator’s ability to analyze browsing behaviour in depth.
7. **No Real-Time Filtering**: DNS-based filtering may not be as fast in identifying and blocking newly emerging threats. Since it relies on DNS databases to categorize domains, there might be a delay before new malicious or inappropriate domains are added to the blocklist.

**Best Practices for Deploying DNS-Based Filtering:**

1. **Regularly Update Policies**: Ensure that filtering policies are regularly reviewed and updated to reflect the evolving needs of the school. This includes adjusting blocked categories, adding new sites to blacklists, and allowing exceptions for legitimate educational content.
2. **Monitor Bypass Attempts**: Use tools or network settings to prevent users from bypassing DNS filtering by manually changing DNS settings. For example, firewall rules can be configured to enforce the use of specific DNS resolvers.
3. **Combine with Other Filtering Methods**: While DNS-based filtering is effective for basic content control, it should be combined with other filtering technologies, such as firewalls or proxy-based filters, to provide more comprehensive protection. This ensures that inappropriate or malicious content is blocked even if it comes from an allowed domain.
4. **Educate Users**: Educate students, teachers, and staff about the school’s internet usage policies and the role of DNS filtering in maintaining a safe and productive online environment. This can help reduce attempts to bypass the filter.

**Use DNS Encryption**: Enable DNS encryption protocols such as DNS over HTTPS (DoH) or DNS over TLS (DoT) to prevent DNS queries from being intercepted or tampered with by malicious actors.

**6.Browser-based filtering extensions:**

**Browser-based filtering extensions** are software tools or plugins installed directly in web browsers (like Chrome, Firefox, Edge, etc.) to control and manage internet access. These extensions can filter, block, or restrict access to specific websites, categories of content, or online activities. They are often used by schools, parents, and organizations to ensure a safe and productive browsing experience by controlling what users can access on the web.

**How Browser-Based Filtering Extensions Work:**

These extensions function by intercepting and inspecting web requests directly within the browser. When a user tries to access a website, the extension checks the site against pre-configured filtering rules. If the site matches any blocked categories or blacklists, the extension either prevents the website from loading or displays a warning page to the user.

The filtering rules can be based on various parameters, such as:

* **URLs** (specific websites or domains)
* **Content categories** (social media, adult content, gaming, etc.)
* **Keywords** (blocking sites based on specific terms found in URLs or page content)

Since browser-based filtering operates at the browser level, it only affects traffic within that specific browser, making it easy to target control for individuals or specific devices.

**Key Features of Browser-Based Filtering Extensions:**

1. **Website Blacklisting/Whitelisting**: Administrators or users can create customized lists of websites to either block (blacklist) or allow (whitelist). This allows granular control over which websites are accessible.
2. **Content Filtering Categories**: Most browser extensions come with predefined content categories (such as adult content, gambling, social media, or gaming) that can be blocked. Users can toggle these categories on or off based on their specific needs.
3. **Time-Based Restrictions**: Some extensions offer time-based controls, allowing users or administrators to block access to certain types of content during specific hours (e.g., blocking social media during school hours).
4. **Content Blocking at Page Level**: Unlike DNS-based or firewall-based filtering, browser-based filtering can inspect and block content at the page level. This means that it can filter specific elements within a webpage, such as images, scripts, or specific sections of a site.
5. **Parental Control Features**: Many browser filtering extensions, particularly those designed for home use, offer features aimed at parental control, such as setting daily time limits for browsing or blocking access to inappropriate content based on the child's age.
6. **Password Protection and Bypass Prevention**: To prevent users from uninstalling or disabling the extension, many filtering extensions come with password protection or administrative controls. Only authorized users can change settings, uninstall the extension, or disable it.
7. **Activity Monitoring and Reporting**: Some filtering extensions include reporting features that allow parents, teachers, or administrators to monitor web usage. They can generate reports on browsing activity, blocked websites, and time spent on different online activities.
8. **Customizable Filters and Alerts**: Administrators can configure custom filtering rules based on keywords or domain patterns. Alerts can be set up to notify when specific websites are accessed, or when an attempt to bypass the filter is detected.

**Advantages of Browser-Based Filtering Extensions:**

1. **Easy to Install and Use**: These extensions are easy to install from browser extension stores and require minimal configuration. Most users can set up basic filtering rules without technical expertise.
2. **Fine-Grained Control**: Browser-based filters provide detailed control over content at a page level, unlike network-level solutions like DNS filtering or firewalls, which can only block entire domains. This allows users to block specific parts of a site while still allowing access to useful content.
3. **Platform Flexibility**: Because they are browser-specific, filtering extensions can be installed on any device that supports modern web browsers, including Windows, macOS, Linux, and even Chrome OS. This makes them flexible solutions for environments with a mix of devices.
4. **Customizable for Individual Users**: Extensions can be customized for individual users, making them ideal for schools or families where different filtering rules might be needed for different groups (e.g., stricter filters for students and lighter filters for teachers).
5. **No Need for Network Configuration**: Unlike firewall or router-based solutions, browser extensions don’t require changes to the school’s or home’s network setup. This makes them easier to deploy in environments where users are spread across multiple locations.
6. **Real-Time Filtering**: Browser-based filters operate in real-time, meaning they can instantly block new or inappropriate content based on updates from their filtering databases.
7. **Portability Across Networks**: Since these extensions work within the browser, they apply filtering policies regardless of which network the device is connected to. This makes them effective for laptops or mobile devices that might be used in different environments (school, home, public networks).
8. **Low-Cost or Free Options**: Many browser filtering extensions are free or have low-cost premium versions, making them accessible for small schools or families without a large IT budget.

**Limitations of Browser-Based Filtering Extensions:**

1. **Browser-Specific**: One major limitation is that these filters only work within the specific browser in which they are installed. If a student uses a different browser or installs a new one, the filtering policies will not apply, potentially allowing them to bypass the restrictions.
2. **Easy to Bypass**: Tech-savvy students may find ways to disable or uninstall the browser extension, especially if the extension lacks strong administrative controls. They could also use incognito/private browsing modes or switch to another browser to bypass filtering.
3. **Device-Specific**: These filters only protect the browser on the specific device where the extension is installed. They cannot apply network-wide protection, meaning other devices (like smartphones, tablets, or different computers) won’t be filtered unless the extension is installed on all of them.
4. **No SSL Inspection**: Similar to DNS filtering, browser-based filters cannot inspect encrypted (HTTPS) traffic unless the extension is specifically designed to do so. This may limit the ability to block specific content on HTTPS websites, as the filtering might be restricted to blocking entire sites.
5. **Limited Control Over Non-Web Traffic**: Since browser extensions only control web traffic within the browser, they cannot manage or filter non-web traffic such as email clients, file-sharing services, or other applications that use internet protocols outside of the browser environment.
6. **Performance Impact**: Depending on the complexity of the filtering rules, browser-based extensions can sometimes slow down browsing performance. This is because they must intercept every web request and compare it against the filtering rules before allowing the page to load.
7. **No Centralized Management**: Managing browser-based filtering across multiple devices can be challenging, especially in larger schools. Without centralized control, administrators may need to manually install and configure the extension on each device, and tracking which devices have the extension installed becomes difficult.
8. **Lack of Comprehensive Reporting**: While some browser extensions offer reporting features, they are typically more limited compared to enterprise-level solutions like network-based filters or firewalls. Schools or organizations that need detailed activity logs and analysis might find the reporting insufficient.

**Best Practices for Using Browser-Based Filtering Extensions:**

1. **Use Password Protection**: To prevent students from tampering with the extension, ensure that administrative controls and password protection are enabled. This will stop users from disabling or uninstalling the extension.
2. **Combine with Other Filtering Methods**: Browser-based extensions should ideally be used in combination with other filtering techniques, such as DNS-based or firewall-based filters, to provide multi-layered protection. This ensures that even if students switch browsers, internet filtering remains enforced.
3. **Regularly Update Extension**: Ensure that the browser extension is kept up to date to benefit from new filtering rules, security patches, and performance improvements. Outdated extensions may leave vulnerabilities open.
4. **Educate Users**: It’s important to educate users, especially students, about the reasons for internet filtering and the potential risks of visiting inappropriate or harmful websites. This can encourage responsible internet usage and reduce attempts to bypass filters.
5. **Enforce Usage of a Single Browser**: Schools or parents can enforce policies to only allow the use of a specific browser (like Chrome) on school-issued devices. By ensuring that students cannot install or use alternative browsers, administrators can guarantee that the filtering policies are applied consistently.

**CHAPTER-3**

**RESEARCH GAPS OF EXISTING METHODS**

* Web filtering technologies, such as URL filtering, keyword blocking, and category-based filtering. However, the effectiveness of these methods on current educational system is unexplored​
* Wireless access points cannot be implemented as school is a public area with many users causing Network congestion​
* Teachers having full access to student's device may lead to threat to confidentiality and cause compliance and privacy concerns​
* Scalability of number of devices and data under wireless access points

​

* Working ability of web portal across different devices ​
* Security risks from shared devices with acquaintances without proper security measures increases the risk of unauthorized access, which could lead to security breaches, exposure of sensitive information, and potential data loss​
* Maintaining integrity of learning materials, preventing unauthorized modifications or error​

**CHAPTER-4**

**PROPOSED METHODOLOGY**

Software used:

* Software - Visual Studio code ​
* URL filtering - ASA cisco​
* keyword blocking - cisco umbrella ​
* category based filtering - cisco umbrella​
* firewall Implementation - Next-Generation Firewalls (NGFWs)​
* Cloud Platform - Google Cloud Platform​

**Technology stack components**

* Frontend Technologies: HTML, CSS, React.js, Scripting language​
* Backend Technologies: Java, Node.js​​
* Database: MongoDB, Google Cloud Storage​
* Tools& AP: Cisco Umbrella, ASA Cisco, Google text-to-speech, Amazon Polly, Dialog flow ​
* Collaboration Tools: Google Workspace (Google Docs, Sheets, Classroom)​
* Cloud Services: GCP **(**e2-micro VM**,** Google Fire cloud for storage, Pub for integration, tools, and Monitoring for data analysis)​
* Security appliance: Next Gen Firewalls (NGFWs)​

**DESIGN PROCEDURE**

1. Developing a web application for user registration system where students and teachers create individual accounts with unique credentials and having Role-Based Access Control to access the web application and using responsive designs for it to be device friendly.​
2. Making a detailed terms and conditions for user compliance.​
3. Deploying Google cloud platform for students which can be used for accessing study materials, reference books and videos as educational content and by using cloud platform services for access control, Monitoring, hosting web application and scalability functions making it cost efficient and using Google Workspace tools which are specially designed for educational settings increasing productivity.​
4. Building a firewall around school’s network and using monitoring software for detecting intrusion against cyber threat and integrating with web filtering software’s like (URL filtering, keyword blocking, and category-based filtering) for restricting web content improving productivity.​
5. Using Google dialog flow which is a cloud-based NLU platform as responsive chat box for interacting with students and answer their queries.​

**CHAPTER-5**

**OBJECTIVES**

**1.Develop a Comprehensive Web Portal Interface**:  
Create a user-friendly web portal that enables teachers to easily manage and filter website access for students based on their names or classes. This interface should support functionalities such as adding/removing students from specific filter groups, viewing current access logs, and customizing filtering options to align with the curriculum.

**2.Implement Real-time Monitoring and Filtering Mechanisms**:  
Design and implement a system that collects device and username information from student devices via wireless access points. This system should enable real-time monitoring of online activities and enforce the filtering policies set by teachers, ensuring that students can only access approved content during class.

**3.Evaluate the Impact of Website Filtering on Learning Outcomes**:  
Conduct research to evaluate how effective website filtering and access control influence student engagement and learning outcomes in the classroom. This could involve analyzing students' academic performance, their usage patterns of online resources, and their feedback regarding the filtering system.

**4** **.Integrate Firewall Solutions for Enhanced Security**

Explore and integrate appropriate firewall technologies that can support the filtering of websites based on the customized policies set by teachers. The research could focus on assessing different firewall solutions' effectiveness, scalability, and ease of implementation in a school environment.

**CHAPTER-6**

**SYSTEM DESIGN & IMPLEMENTATION**

**1.Develop a Comprehensive Web Portal Interface**:

Create a user-friendly web portal that enables teachers to easily manage and filter website access for students based on their names or classes. This interface should support functionalities such as adding/removing students from specific filter groups, viewing current access logs, and customizing filtering options to align with the curriculum.

**2.Implement Real-time Monitoring and Filtering Mechanisms**:

Design and implement a system that collects device and username information from student devices via wireless access points. This system should enable real-time monitoring of online activities and enforce the filtering policies set by teachers, ensuring that students can only access approved content during class.

**3.Evaluate the Impact of Website Filtering on Learning Outcomes**:

Conduct research to evaluate how effective website filtering and access control influence student engagement and learning outcomes in the classroom. This could involve analysing students' academic performance, their usage patterns of online resources, and their feedback regarding the filtering system.

**4.Integrate Firewall Solutions for Enhanced Security:**

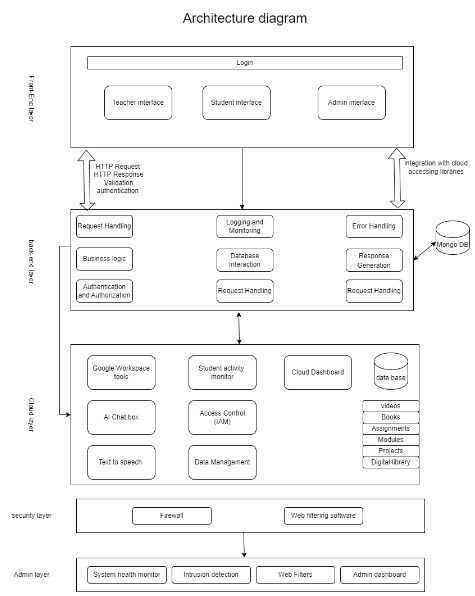
Explore and integrate appropriate firewall technologies that can support the filtering of websites based on the customized policies set by teachers. The research could focus on assessing different firewall solutions' effectiveness, scalability, and ease of implementation in a school environment.

**INPUT DESIGN**

Input design is a critical aspect of system development that ensures accurate, efficient, and secure data collection and processing. For BYOD (Bring Your Own Device) classrooms, input design focuses on facilitating secure access to systems, monitoring device usage, and enabling productive learning experiences. This section outlines input mechanisms tailored to the dual goals of security and productivity in BYOD environments.

**OUTPUT DESIGN**

Output design focuses on how data and insights are presented to users to ensure effective communication, usability, and decision-making. In BYOD classrooms, outputs should be designed to support both security monitoring and productivity enhancement. This section outlines various output mechanisms and their alignment with the dual goals of secure and productive BYOD environments.



**CHAPTER-7**

**TIMELINE FOR EXECUTION OF PROJECT**

**(GANTT CHART)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Tasks​ | Review 0​ | Review 1​ | Review 2​ | Review 3​ | final​ |
| Tittle Finalizing​ | ​ | ​ | ​ | ​ | ​ |
| Literature Survey and analysis of project statement​ | ​ | ​ | ​ | ​ | ​ |
| Finalizing objectives and deciding methodology​ | ​ | ​ | ​ | ​ | ​ |
| Finding existing GAPS in the project​ | ​ | ​ | ​ | ​ | ​ |
| Referring research papers for better insight ​ | ​ | ​ | ​ | ​ | ​ |
| Designing and developing web portal and registering users and storing in MongoDB​ | ​ | ​ | ​ | ​ | ​ |
| Developing a cloud environment for uploading educational content and videos and Implementing access control through cloud dashboard​ | ​ | ​ | ​ | ​ | ​ |
| Implementing firewall using (NGFWs)​ | ​ | ​ | ​ | ​ | ​ |
| 50% Implementation with live demo and report​ | ​ | ​ | ​ | ​ | ​ |
| Developing a web page to monitor firewall for intrusion detection​ | ​ | ​ | ​ | ​ | ​ |
| Integrating the firewall with web filtering technologies and restricting content using web filters​ | ​ | ​ | ​ | ​ | ​ |
| Integrating cloud with Dialogflow tool for handling student queries ​ | ​ | ​ | ​ | ​ | ​ |
| 100% implementation with live demo and report (hardcopy)​ | ​ | ​ | ​ | ​ | ​ |
| Plagiarism report on project report​ | ​ | ​ | ​ | ​ | ​ |
| Publication of project report​ | ​ | ​ | ​ | ​ | ​ |
| Patent on project report​ | ​ | ​ | ​ | ​ | ​ |

**CHAPTER-8**

**OUTCOMES**

1. **Enhanced Classroom Management**: Teachers can manage and restrict student access to online content, reducing distractions and improving focus.
2. **Improved Learning Outcomes**: Filtering relevant educational content aligns with the curriculum, fostering deeper engagement and understanding among students.
3. **Data-Driven Insights**: Analytics will provide insights into student internet usage, helping educators tailor instruction and assess the effectiveness of filtering policies.
4. **Increased Accountability**: Activity logs promote responsible online behavior among students and ensure compliance with school internet usage policies.
5. **Support for Diverse Learning Needs**: Customizable filtering allows teachers to address individual student needs, facilitating differentiated instruction.
6. **Strengthened Cybersecurity**: The integrated firewall enhances network security and protects students from accessing harmful content.
7. **Scalability for Future Needs**: The system can evolve with technological advancements and expand to accommodate more users and features.
8. **Increased Teacher Confidence**: With control over internet access, teachers feel empowered to incorporate technology into their lessons, promoting innovative teaching practices.

**CHAPTER-9**

**RESULTS AND DISCUSSIONS**



The analysis shows a fluctuating trend in pass percentages across assessments. Initially, there was strong performance (80%) in Unit Test 1, followed by a significant decline, reaching the lowest point (40%) in Unit Test 3. However, a steady recovery began with Unit Test 4 (75%) and continued into subsequent assessments, eventually returning to the initial performance level. This U-shaped trend highlights challenges during the mid-phase, likely due to increased difficulty or other factors, and demonstrates successful recovery through interventions. Sustained improvement suggests resilience and effective strategies, with a focus on maintaining consistency in future assessments.

**CHAPTER-10**

**CONCLUSION**

The proposed web portal is designed to help teachers manage internet access in BYOD classrooms. It creates a controlled digital environment where students can use their personal devices productively, free from distractions and harmful content. This ensures better focus and improved learning outcomes.

In the future, the system will include advanced features like **AI monitoring** to detect inappropriate behaviour (e.g., trying to bypass filters) and **analytics** to measure how effective the filtering policies are. These tools will give teachers and schools valuable insights to make the system even better.

The system will also adapt to real-time classroom activities using **automation and machine learning**, allowing filtering rules to change dynamically based on what the class is doing. For example, during a group project, collaboration tools can be enabled while non-educational content stays blocked.

Additionally, the project will involve continuous feedback from teachers, students, and school administrators to ensure the system evolves to meet new challenges. By leveraging **cloud-based technologies**, it will be cost-effective, scalable, and easy to manage, making it suitable for schools of all sizes.

In short, the web portal will provide a secure, distraction-free, and productive digital environment, helping schools effectively balance technology and education in BYOD classrooms.

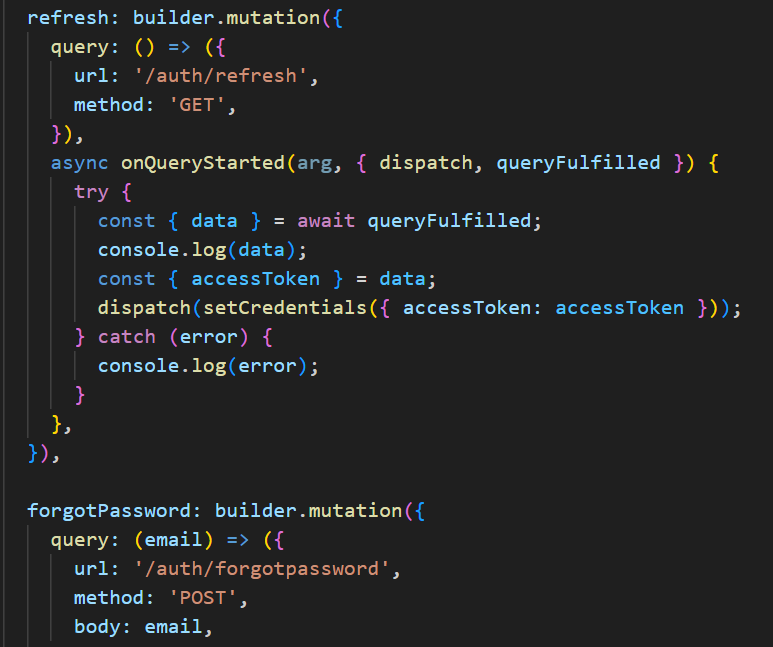
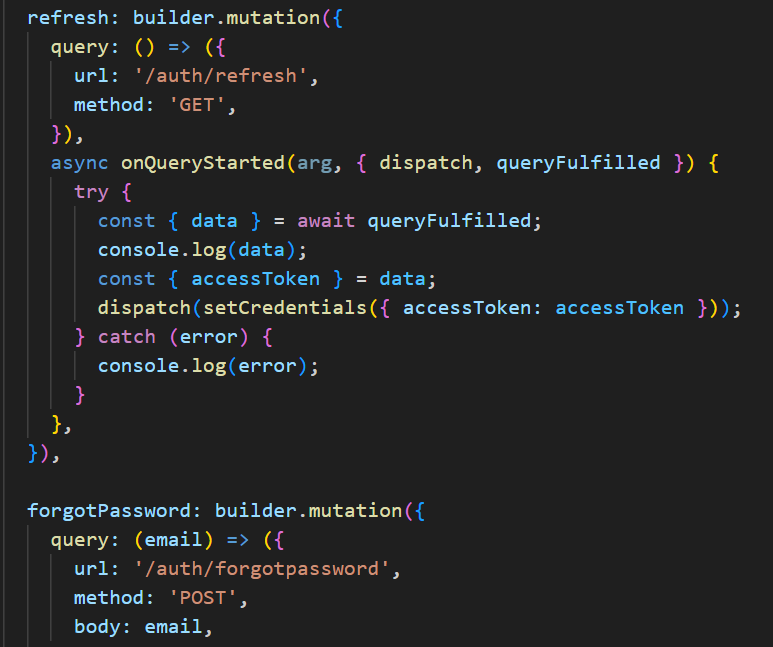
**REFERENCES**

1. [https://www.researchgate.net/profile/Deepshikha-Aggarwal/publication/334130255\_Bring\_Your\_Own\_Device\_BYOD\_to\_the\_Classroom\_A\_technology\_to\_promote\_Green\_Education/links/6656dba40b0d28457461c946/Bring-Your-Own-Device-BYOD-to-the-Classroom-A-technology-to-promote-Green-Education.pdf](file:///C:\Users\Murthy\AppData\Local\Microsoft\Windows\INetCache\IE\2NR7KGPB\Rev1.pptx)
2. [https://www.researchgate.net/profile/Rahat-Siddiqui/publication/261136229\_Bring\_Your\_Own\_Device\_BYOD\_in\_Higher\_Education\_Opportunities\_and\_Challenges/links/54e2dc520cf296663797c13d/Bring-Your-Own-Device-BYOD-in-Higher-Education-Opportunities-and-Challenges.pdf](file:///C:\Users\Murthy\AppData\Local\Microsoft\Windows\INetCache\IE\2NR7KGPB\Rev1.pptx)
3. <http://www.library.must.ac.ug/bitstream/handle/123456789/2789/Enhancing%20Bring%20Your%20Own%20Device%20Security%20in%20Education.pdf?sequence=1&isAllowed=y>
4. [https://files.eric.ed.gov/fulltext/EJ1099110.pdf](file:///C:\Users\Murthy\AppData\Local\Microsoft\Windows\INetCache\IE\2NR7KGPB\Rev1.pptx)
5. <https://www.researchgate.net/publication/318921194_Bring_Your_Own_Device_in_Education_A_Review_of_Challenges>​
6. <https://computerresearch.org/index.php/computer/article/view/606/6-Improving-Network-Security-Next-Generation_JATS_NLM_xml>
7. <https://smoothwall.com/resources/web-filtering-and-byod>
8. <https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2016.01739/full>
9. <https://www.mdpi.com/2504-3900/82/1/10>
10. <https://computerresearch.org/index.php/computer/article/view/606/6-Improving-Network-Security-Next-Generation_JATS_NLM_xml> ​

<https://www.researchgate.net/publication/381306880_An_Overview_of_Web_Content_Filtering_Techniques>

**APPENDIX-A**

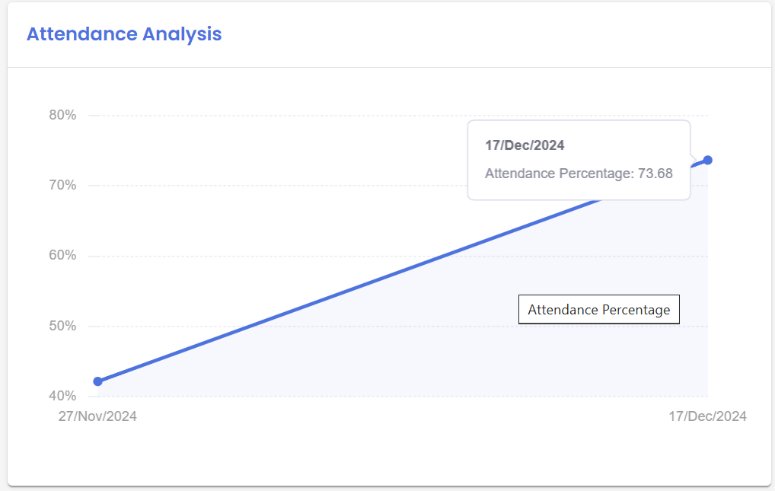
**PSUEDOCODE**



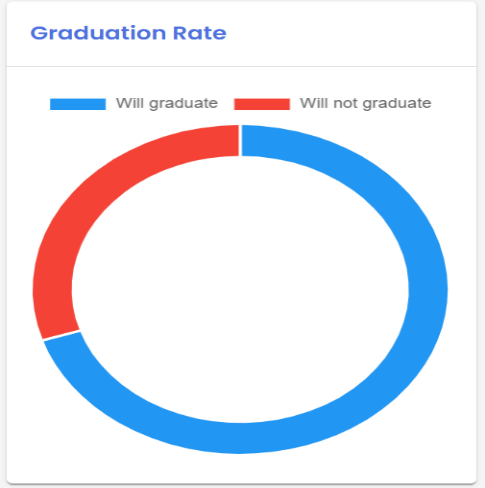
**APPENDIX-B**

**SCREENSHOTS**

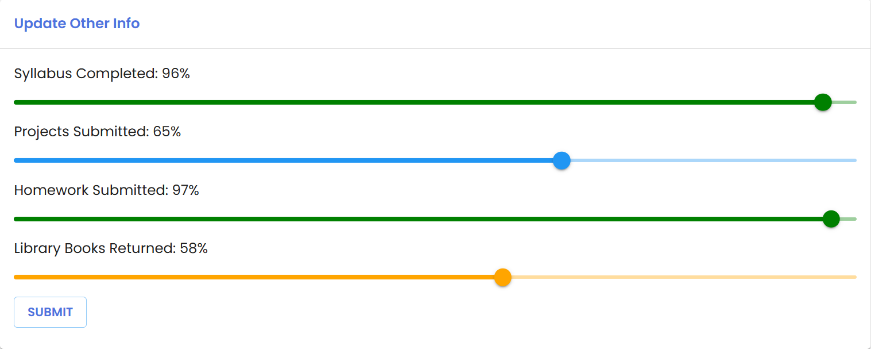
“Fig 1 Teacher Dashboard”



“Fig 2 Teacher Dashboard”



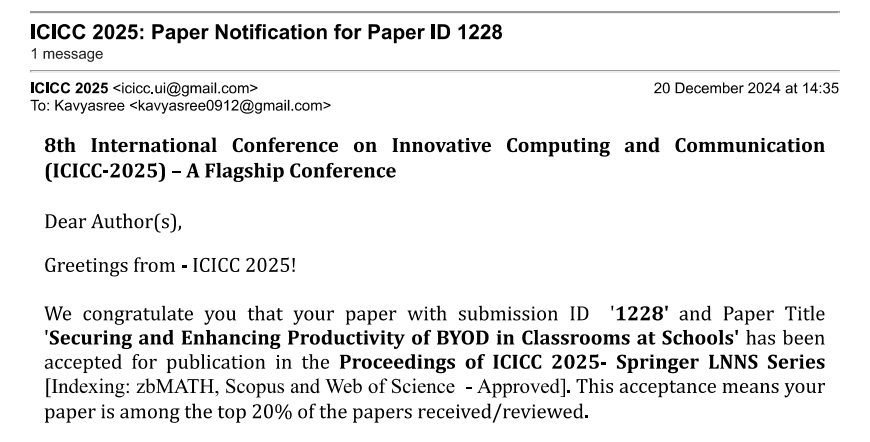
“Fig 3 Teacher Dashboard”

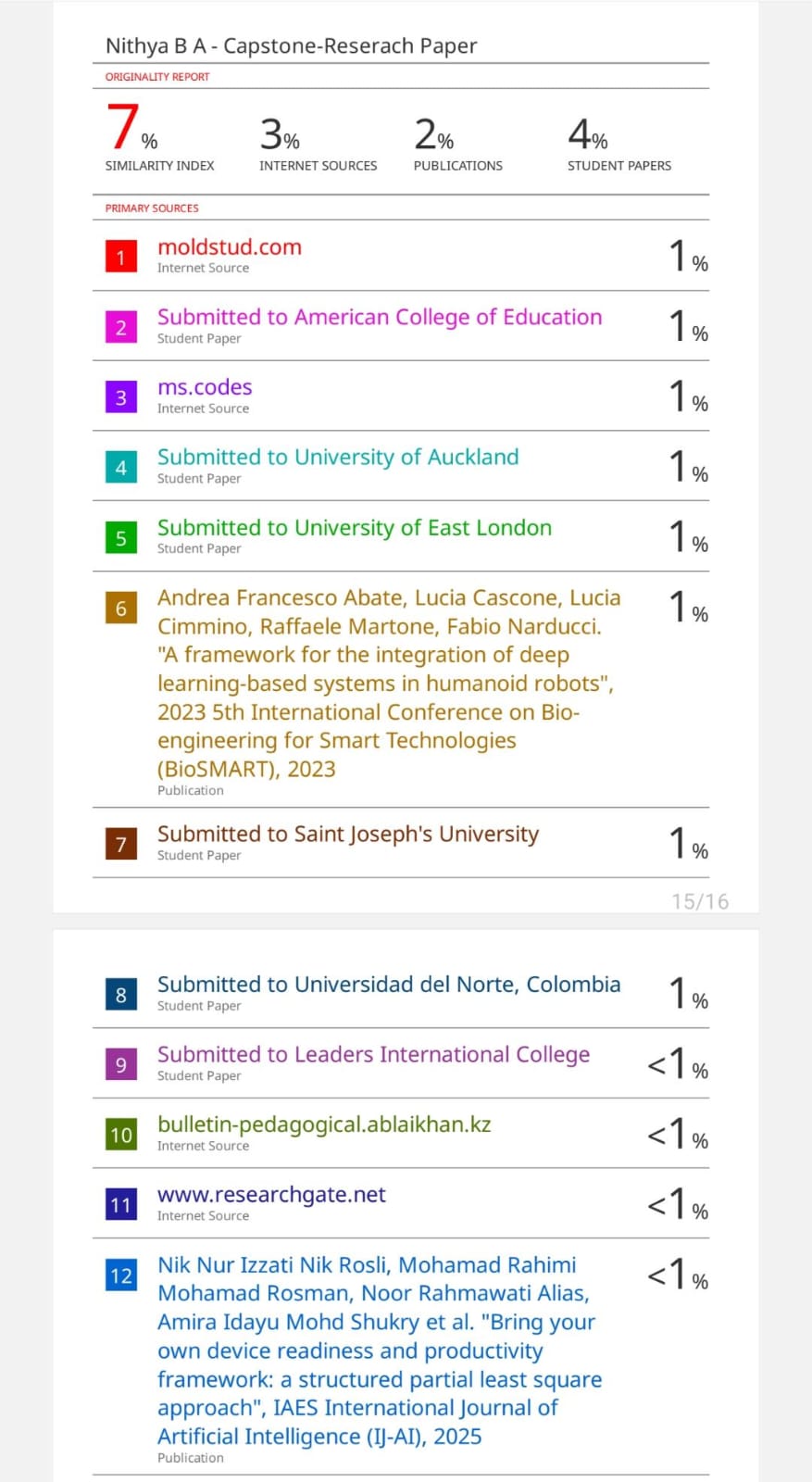


“Fig 4 Teacher Dashboard”

**APPENDIX-C**

**ENCLOSURES**

****

****

**"**Securing and Increasing Productivity of BYOD in Classrooms at Schools,**"** aligns with multiple United Nations Sustainable Development Goals (SDGs). It supports **Goal 4: Quality Education** by enhancing the learning experience through secure and productive use of personal devices, ensuring access to appropriate educational resources. By leveraging cloud services and advanced cybersecurity measures, it contributes to **Goal 9: Industry, Innovation, and Infrastructure,** fostering innovative and scalable digital infrastructure for modern classrooms. The emphasis on privacy compliance and safeguarding sensitive data aligns with **Goal 16: Peace, Justice, and Strong Institutions**, promoting trust and accountability within educational institutions. Furthermore, the use of collaborative cloud-based solutions highlights **Goal 17: Partnerships for the Goals**, reflecting the need for cooperation between schools, technology providers, and stakeholders to achieve shared educational and technological advancements.

****