Proceedings of the 6th International Conference on Statistics: Theory and Applications (ICSTA'24)
Barcelona, Spain – August 19 - 21, 2024
Paper No. 164
DOI: 10.11159/icsta24.164

Enhancing Security in Remote Laboratory Environments: A Layered Approach

Ali Al Maqousi
Department of Information Security, Faculty of Information Technology, University of Petra, Amman, Jordan
amaqousi@uop.edu.jo

Abstract—Remote cybersecurity training labs help students learn useful skills for the real world by letting them use what they've learned in the classroom through tests. It is harder to protect these important places, though, than it is to protect normal houses. Based on our knowledge, a full, multilayered security system is the best way to protect remote labs. The approach uses different types of security to protect users, data, and systems. These types of security include authentication, encryption, monitoring, access control, integrity checks, and more. At each stage, it looks at both tried-and-true and new methods, such as single- and multifactor authentication, VPNs, attribute-based access control, file integrity verification, and finding strange things. Qualitative studies say that the design gives fine-grained control over what users do while also improving privacy, availability, and trustworthiness. This method has many advantages, such as better security in remote labs, fine-grained control over user behaviour, and a flexible base for building safe, expandable cyberlearning environments to keep up with rising demand.

Keywords: Cybersecurity training, Remote laboratories, Layered security model, Authentication methods, Access control policies, Integrity monitoring

1. Introduction

Cybersecurity students are afforded a one-of-a-kind opportunity to learn by doing through remote access labs, which enable them to conduct experiments without being constrained by the conventional university facilities. Students from all over the world can utilize real equipment over the internet to learn how to detect security vulnerabilities, build security tools, and improve their cyber defence skills [1]. This is made possible by the adaptability of these platforms.

safeguarding remote labs, on the other hand, is somewhat more challenging than safeguarding traditional computer facilities that are physically located [2]. While on-campus labs are equipped with built-in access control because of their location on campus, users who access systems through the internet may be able to access them from anywhere in the globe [3]. This indicates that stringent security measures need to be implemented specifically for websites dependent on the internet.

A significant proportion of remote lab installations implement arbitrary or outdated security measures provided by hosting institutions [4]. Rarely do they execute a plan tailored specifically for the remote model. Users, systems, and personal student information face cyber threats such as man-in-the-middle attacks and unauthorized access [5] due to organizational inequalities.

This paper introduces a comprehensive security model implementable in remote cyber training laboratories to address the aforementioned challenges. The approach utilizes multiple tiers ensuring authentication, monitoring, integrity, encryption, and access control, with each tier offering unique system protection. This methodology comprises components providing robust, adaptable security for valuable assets and activities.

Furthermore, it employs modern protocols like OAuth 2.0, attribute-based access control (ABAC), OpenSSL, and OpenVPN for comprehensive infrastructure, communication, and access security. The layered design incorporates empirically proven beneficial technologies applied in a specialized domain, establishing a versatile structure accommodating ever evolving academic remote laboratory requirements and diverse user/application support.

The model underwent revisions improving privacy, reliability, and accessibility in remote lab contexts, demonstrated by comparison with earlier techniques. The stratified security design simplifies activity monitoring and access privilege control, flexibly meeting various operational needs. This enables adaptable laboratories where students can acquire extensive

knowledge through safe, legal activities. This technique offers a scalable, long-lasting, secure model for remote cybersecurity instruction.

The paper structure is as follows: Section 2 examines related work, Sections 3 and 4 provide background and core cybersecurity concepts, Section 5 explains the proposed layered security model, Section 6 analyzes model implementation, Section 7 discusses results, and Section 8 presents conclusions and future work.

2. Related work

Significant research has focused on improving remote laboratory frameworks from pedagogical and technical perspectives. For example, [6] developed a real-time analytics platform for monitoring student activities. Similarly, the LAMP architecture outlined optimizations for large-scale remote labs [7].

Recent literature explores remote and virtual approaches to cybersecurity training with an industrial focus. [8] develop radiation detection experiments complemented by physical security sensors for online nuclear security education, utilizing light, ultrasonics, and heat for detection. This work points to the potential of integrating diverse security technologies for more comprehensive remote lab security solutions.

Study [9] provides guidelines for assessing safety and security in federated labs, highlighting the complexity and new challenges raised by interconnected remote labs across multiple institutions.

Study [10] addresses the critical need for practical cybersecurity education in the context of IoT vulnerabilities through the development of a remote online laboratory allowing hands-on experience with real-world cybersecurity scenarios. While significant advancements have been made in enhancing the security and efficiency of remote laboratory environments, there remains a critical need for further research and development in areas such as standardized security protocols for federated labs, comprehensive cybersecurity training specific to IoT vulnerabilities, and the integration of advanced physical security technologies. Bridging these gaps will ensure the creation of more secure, effective, and accessible remote laboratory environments for educational and research purposes.

3. Remote laboratories

Through software interfaces over the Internet, remote labs let students use real equipment while they are not there [11]. Webcams let people watch physical processes from afar, and dedicated computers manage how users talk to each other and get to lab equipment [1].

There are many reasons why these settings are better than regular hands-on labs or only simulations. First, remote services offer availability 24 hours a day, seven days a week, which can't be replicated physically [12]. Because of this easier access, more students can now use modern facilities that smaller schools can't offer. Distance learning and lifelong learning are also possible in remote laboratories, which is very important for working workers who want to improve their skills [13]. Lastly, remote labs deal with physical resource limits like storage, usage, and cost [7].

However, protecting web-based labs is harder than protecting standard facilities that can only be used in one place. The next section discusses the basic cybersecurity rules based on the suggested paradigm.

4. Core cybersecurity concepts

Cybersecurity safeguards computers, systems, networks, data, and users from digital threats [14]. Fundamentally, it aims to ensure key properties, including:

- Confidentiality: Preventing unauthorized access to information
- Integrity: Safeguarding accuracy and completeness of data
- Availability: Ensuring reliable access to systems and resources

Many controls help uphold these attributes by addressing vulnerabilities, allowing cyberattacks to breach defences [15]. However, numerous taxonomies categorize mechanisms by domain or technique, the proposed methodology structures measures into five interdependent layers:

- Authentication: Verifying identity
- Encryption: Secure encoding of data/communications
- Access Control: Managing permissions and activity
- Integrity: Ensuring completeness of systems
- Monitoring: Ongoing analysis of people/systems

No single layer is sufficient to secure complex environments alone. However, their synergistic layering creates robust, customizable protection tailored for remote cybersecurity laboratories.

5. Proposed layered security model

An overview of the suggested layered security paradigm, which was created with remote cybersecurity training laboratories in mind, is given in this section. Each stratum fulfils a specific purpose in preserving the system's overall integrity. Fig. 1 shows how the model's architecture is laid out.

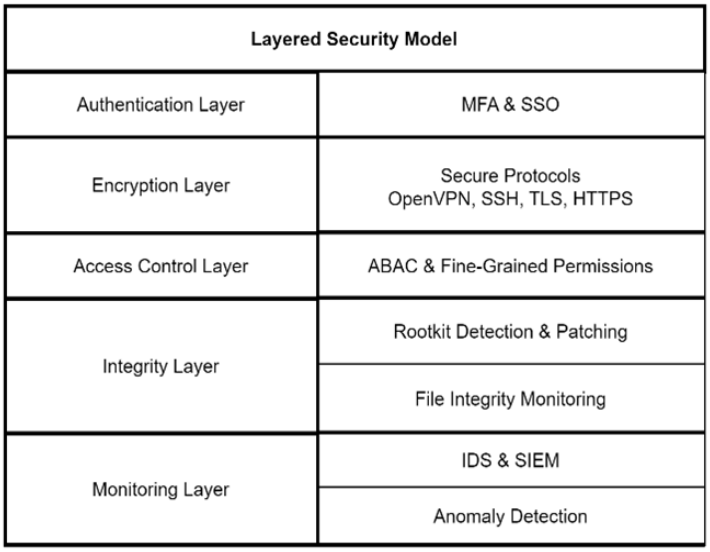

Fig. 1. Layered security model architecture

The security of access points and communication routes is ensured by authentication and encryption. Access control makes it easier to manage user permissions, while integrity ensures that assets are protected from being compromised. Surveillance of network traffic, configurations, and operations are all included in monitoring. These layers work together to provide a complex defence that goes beyond traditional methods.

5.1. Authentication layer

A user's identification is still the main way to control how the system is used. The authentication layer's job is to ensure the person is who they say they are when logging in. Access control systems use the permissions someone has been given to give them specific tasks after agreeing.

In standard authentication systems, passwords and other knowledge factors are easy to lose or forget. On the other hand, multifactor authentication (MFA) makes things much safer by needing a second credential from a different group, like something you own or inherited [16].

After entering the right password, which meets the knowledge requirement, users can provide biometrics, such as fingerprints, which meet the inherence requirement. If you use two sets of passwords, the chance of being impersonated is much lower if someone hacks into one set. Automated attacks like brute force can't work with multifactor authentication because each login try needs a different type of credential.

To set up multifactor authentication (MFA) in remote labs, you can use your school's tools or third-party apps like Duo, Google Authenticator, or Authy. After users enter their passwords, these apps give them temporary codes they need to have to finish the possession factor [17].

Single sign-on (SSO) options are a very good way to authenticate users in remote labs used by many internal and external apps. Single sign-on (SSO) lets users safely share a single credential and access limited services using a central identity provider. You will not have to enter your password again when you switch systems.

One-click (SSO) solutions make things safer by letting organizations use multifactor authentication (MFA) or flexible rules for the identity provider. To do this, these rules are used across all applications instead of being set for each one separately. In the case of covert input tracking, lowering the number of times a password is entered also lowers the chance of it being revealed. Some single sign-on (SSO) tools commonly used in schools are InCommon, CAS, and OAuth 2.0 [18].

5.2. Encryption layer

Deploying secure transmission protocols ensures communications remain private against eavesdropping threats. The encryption layer establishes protected pathways for remote access channels and inner-system data transfers using standard or virtual private networks (VPNs).

VPNs encapsulate internet traffic into encrypted tunnels, preventing intermediaries like Internet service providers from inspecting sessions. OpenVPN using OpenSSL certificates between clients and dedicated servers represents a common open-source option [19].

Commercial client software often provides easier installation and configuration for users unfamiliar with working inside command line interfaces. Secure VPN protocols ensure students only access laboratory systems through validated pathways instead of less scrutinized institutional networks.

Internally, technologies such as Secure Shell (SSH), Transport Layer Security (TLS), and HTTPS confirm data confidentiality between platform servers, hardware interfaces, database layers and other integral components [20]. Together with outer VPN tunnels, multilayered encryption foils potential man-inthe-middle attacks infiltrating communications.

Ongoing testing is necessary to identify and disable outdated algorithms as computational progress allows ciphers to be transitioned from secure to deprecated. Following current cryptography standards published by reputed organizations like National Institute of Standards and Technology ensures Continual utilization of best practices [21].

5.3. Access Control Paradigms for Remote Laboratories

While initial authentication allows users to access remote laboratory systems, additional access control mechanisms are necessary to impose nuanced restrictions on specific in-lab activities permitted to each user based on their role. Conventional access control techniques often utilize a role-based access control (RBAC) model, which associates predefined privilege sets with positions, allowing or denying certain actions based on the user's role [22]. However, RBAC requires substantial configuration overhead to appropriately assign permissions across exponentially increasing combinations of roles and activities within a remote laboratory environment.

An alternative technique is attribute-based access control (ABAC), which links access rights directly to the elemental traits of individual users and the properties of digital objects they seek to interact with [23]. For example, students enrolled in advanced ethical hacking courses may possess elevated lab privileges relative to introductory students, who may be restricted from executing penetration testing tools that could disrupt operations. Rather than configuring an elaborate hierarchy of user groups, ABAC simply associates appropriate permissions to granular user and object attributes.

Well-tuned ABAC implementations can enable remote laboratory administrators to achieve precise levels of control over user activities. Specific read/write privileges can be assigned to selective database tables, system logs, hardware modules, etc., with predefined functions invoking access upon users fulfilling certain contextual requirements. These may include passing preliminary quizzes assessing competency or acknowledging legal use agreements. Such flexible access mappings enhance simplicity and customizability compared to conventional RBAC paradigms.

5.4. Safeguarding Integrity in Remote Laboratory Environments

Access control systems keep people who are supposed to be there from getting into a system. Extra integrity security keeps settings from being changed without permission or by mistake, which could change how they work. Systems can be slowed down and exposed more in remote labs by malware injection and other types of damage or disruption that are not meant to happen. Some ways of checking integrity, like keeping track of file integrity, finding rootkits, and installing software patches regularly, ensure that baseline system settings are never changed.

Tools that check the integrity of files ensure that the digital fingerprints or hashes of necessary system executables match the signed copies saved on media that cannot be read [24]. If two signatures do not match, it could mean that small changes have been made that add backdoors or change how keys work. If you compare the current hash state to a known good standard from the past, you could see if someone changed private files without your permission.

In the same way, rootkit scanners look through operating systems for hidden malware that gives attackers constant, secret access to administrative rights [25]. Regular rootkit scans and strict patching rules for operating systems and apps reduce the number of attack sites known threats can use.

Both options work together to maintain the basic trustworthiness to offer safe remote training lab platforms. Suppose there are any signs of a possible breach. In that case, the affected area can be turned off automatically until the full cleanup, including a forensic probe and system restoration.

5.5. Continuous Security Monitoring in Remote Laboratories

Once baseline operational protections are in place, ongoing monitoring remains essential for identifying residual vulnerabilities and emerging attack attempts against secured systems. Continuous analysis further enables timely incident response by detecting early compromise patterns based on sensor alerts and heuristic model outputs.

Network-based intrusion detection systems including Snort and Suricata perform deep packet inspection, raising alerts when potentially malicious traffic triggers rule-based signatures [26]. Such alerts may indicate attempts to probe systems, transmit malware payloads, or launch denial of service attacks among other policy violations. Integrating security information and event management (SIEM) platforms streamlines workflows for investigating and responding to threats.

Additionally, unsupervised machine learning models can uncover anomalies deviating from expected system and user behavioural baselines using clustering algorithms and dimensional outlier detection techniques [27]. For instance, a student suddenly conducting intensive network scans after months of light experimentation may signify a compromised account rather than legitimate expanded research. By training on habitual activity patterns, data-driven models can construct normalcy ranges to identify significant deviations that may reflect underlying attacks.

These analytical monitoring components offer comprehensive network-based and behavior-focused surveillance required to maintain stringent security postures in remote laboratories. Regular tuning and adapting rules and models promote continued scrutiny of evolving threats as attack surfaces and tactics change.

6. Model implementation

This section provides a simulated implementation demonstrating the layered security model practically applied, defending a hypothetical remote cybersecurity training lab. It examines representative controls deployed across the five layers to secure access, communications, data, configurations, and activities.

6.1. Lab Configuration

The example remote laboratory consists of the following elements characteristic of conventional setups described in existing literature [6]:

- Student-accessible virtual machines (VMs) for hands-on activities
- Physical workstations connected to peripheral hardware/devices
- Centralized authentication and deployment servers
- Databases storing access credentials, usage logs, submissions
- Web and application interfaces for users to interface

Like comparable environments, day-to-day management requires different levels of access specific personnel require executing their duties.

6.2. Layer Implementation

Authentication Layer: Students use institutional login credentials to access the remote lab single sign-on portal based on In Common Federation standards [28]. This redirects users to Duo Security's two-factor authentication application for secondary code verification [29]. Lab administrators connect through dedicated VPN tunnels using OpenSSL certificate-based authentication and universal second factors.

Encryption Layer: Site-to-site OpenVPN secures all remote student communications via TLS-based encryption [19]. Internally, SSH protects administrator command line interfaces and database connections while application-level TLS guards web exchanges. HTTPS prevents eavesdropping on browser sessions and submission transfers.

Access Control Layer: ABAC managed through the opensource OpenPolicyAgent (OPA) projects user attributes like enrolment status and course registrations to stackable permissions controlling VM usage [23], [30]. Custom policies enacted through the centralized Policy Decision Point determine runtime authorizations passed to peripheral servers and hardware interfaces per session.

Integrity Layer: File integrity monitoring scripts execute hourly, comparing present VM root directory cryptographic hashes against previously known states logged under Digital Signatures Standard version 4 parameters (DSSv4) [24]. Weekly rootkit scans probe for indications of malware persistence mechanisms while monthly vulnerability scans assess residual attack surfaces necessitating patching.

Monitoring Layer: An IDS inspecting all inbound and outbound traffic creates alerts for malicious payloads caught by continuously updated Threat Prevention Labs signatures [26]. Anomalies identified by unsupervised autoencoder algorithms trained on six months of typical usage trigger alerts inspected by IT staff. SIEM integration automatically enacts established response workflows for critical events.

This representative model conveys proven and emerging standards to address remote cybersecurity lab requirements through layered security solutions balancing protection, cost, performance, and usability. Ongoing tuning of access policies, encryption protocols, integrity checks, and activity profiling adapts the model to evolving needs and risk landscapes.

While the preceding focuses on technical aspects, human components remain equally essential for successful enactment. The next section explores key factors ensuring effective adoption.

6.3. Enabling Organizational Factors

Optimizing the efficiency of multilayer security requires considering sociocultural aspects that impact the adoption and continuous utilization of technology. Models such as the United Theory of Acceptance and Use of Technology 2 (UTAUT2) [31] have been used to investigate how people's views affect the uptake of information technologies.

The findings show that when people deploy measures like MFA, which disrupt existing workflows, they consider the pros and cons of the effort vs the advantages. Assuming the necessary institutional support resources are accessible, there is a strong correlation between students' awareness of peer adoption and voluntary utilization [32].

From an organizational standpoint, the most dependable ways to finish implementation are with the support of leadership and the enforcement of revised regulations that set new baseline requirements. Even the most advanced technological measures cannot ensure that everyone will agree. Positive cyclical feedback loops emerge when top-down expectation signalling is consistent and grassroots security awareness is high. This causes people to be more receptive to short-lived disturbances in exchange for benefits they perceive as being communicated through education and knowledge [33].

The layered approach stresses interoperability by utilizing interlocking modular technologies that are easily replaceable according to internal skill availability and cost limits. Administrators buy-in is still necessary for acquisition and implementation, and new avenues to address end-user concerns must be created.

7. Results Analysis

A comparative analysis of the layered security model implemented as per Section 5 and standard methodologies underscores significant enhancements in securing remote cybersecurity training laboratories. Elevated performance arises from a design process guided by specific use case requirements rather than adapting generic legacy controls provisioned by hosting institutions.

7.1. Protection Analysis

The five-layer architecture significantly enhances confidentiality, integrity, and availability using mutually supportive cybersecurity technologies specifically adapted for remote laboratories. Table 1 summarizes the advantages over traditional implementations relying on standard passwords, basic traffic encryption, firewalls, and reactive monitoring:

Observe no singular legacy control matches the composite coverage spanning edge networks, user access, inner platforms, ongoing configurations, and ubiquitous activities.

7.2. Customization Enablement

In addition to providing superior security, the model allows for extensive customization to ensure that applications match specific lab requirements. As risk perceptions, administrative demands, and usage patterns shift, each layer makes

matching controls to these changes easier. This is made possible by technologies that enable attribute-based policies, cryptographic agility, disposable credentials, and dynamic heuristics.

For example, OpenPolicy Agent's access control plane allows you to provide detailed rights to each user depending on their attributes and session variables [30]. It's simple to grant permissions, allowing you to create complicated restrictions for student experiments depending on certification progress, legal agreements, time-of-day limits, and more. These can provide people with temporary access to powerful tools that would otherwise be unavailable to them.

The same level of adaptability allows you to deal with new difficulties. Multilayered encryption ensures that there is a safe backup if some ciphers or protocols are compromised. Flexible cryptography enables communications to readily transition to postmodern choices, as computational hazards render traditional approaches like RSA obsolete [21].

One-time access codes prevent stolen credentials from being used again, and neural network-based anomaly recognition adapts to fresh usage data. When combined with DevOps-style upgrade deployment, these self-recalibrations provide continuous, personalized protection for students' valuable hands-on experiences.

Table 1-protection improvements through layered model

Security Property	Description
Confidentiality	Encryption encapsulating all remote connections prevents sniffing attacks. Internal protocols like SSH, TLS and HTTPS provide multifaceted data transfer protection, ensuring the confidentiality of communications and data exchanges.
Integrity	Rootkit detection finds advanced compromise attempts, while file monitoring ensures continuity of critical systems. Authentication plus access controls prevent unauthorized changes, safeguarding the integrity of the remote laboratory environment.
Availability	Enhanced DDoS resilience through cloud-based infrastructure. Encryption preserves connectivity during attacks, and monitoring enables quicker response, minimizing downtime and ensuring the overall availability of the remote lab systems.

7.3. Scalability Analysis

Lastly, a layered design lets both big and small parts grow to fit their needs. A lot of different solutions are for sale or rent by different companies. Some examples are identity management, VPN infrastructure, integrity validation, and SIEM analytics [34].

When you have standard safety layer interfaces, switching to new providers or using open-source technologies is easier. So, the worry that they wouldn't be able to switch sources if maintenance costs went up quickly or the business stopped running because of instability is gone. Institutions can put the most effort into putting in place the most important safety measures first, and then they can fill in any holes as funds allow.

8. Conclusion Future Work

This research shows a new way to keep computers safe, especially for schools that teach computer hacking. This choice is better than the others in terms of scalability, modularity, and protection. By using encryption, granular access control lists (ACLs), integrity checks, multifactor authentication, and continuous tracking, you can make big gains while improving security, availability, and privacy. On the other hand, the qualitative data show that knowing a lot about technology is not enough to ensure that many people use it. Social ties that are well-organized are just as important. Leaders should ensure that goals are clear, that students are focused on the current subject, and that quick feedback systems are in place to deal with any confusion that may arise during a shift. To get the most out of the big educational benefits of online labs, it is important to focus on the parts that meet the needs of each person, make sure the technology is easy to use, and get strong support from the company. This gives people more ways to get real-world training and helps them become skilled cybersecurity experts. To make standard settings more useful for common designs, we need to look into other ways to authenticate users and test their performance thoroughly in many different settings.

Acknowledgment

The author would like to thank the Deanship of Scientific Research and Graduate Studies at the University of Petra for supporting this research.

References

[1] A. Memon and U. Meyer, “Online laboratories for distance learning in chemistry and biology,” in International Conference on Engineering Education, 2004, pp. 15–20.

[2] J. Grobbelaar, U. Meyer, and C. Lee, “A survey of remote laboratories with an emphasis on chemical experiments,” in World Conference on Educational Multimedia, Hypermedia and Telecommunications, 2006, pp. 3049–3055.

[3] H. Saliah-Hassane, “Remote laboratories paradigms: Latest trends and scopes,” Procedia - Social and Behavioral Sciences, vol. 103, pp. 195– 203, 2013.

[4] M. Koksal and V. Karakus¸, “Architectural design of a scada system sim-¨ ulator for critical infrastructure security analysis,” in IEEE Symposium on Computers and Communications, 2018, pp. 537–542.

[5] H. Abbas and W. Baker, “System dynamics applications in critical infrastructure,” Systems Engineering, vol. 10, no. 3, pp. 272–289, 2007.

[6] Z. Zhang, X. Chen, C. Zhong, Q. Zhao, P. Zhan, J. Li, Y. Cao, Z. Wang, M. Luo, and Y. Zhao, “Iot-based remote virtual laboratory education platform for control engineering,” in IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, 2018, pp. 1–4.

[7] D. Nankivil, A. Gonzalez, C. Rowaan, W. Lee, M. C. Aguilar, and J.-M. A. Parel, "Robotic remote controlled stereo slit lamp," Translational Vision Science & Technology, vol. 7, no. 4, pp. 1-1, 2018.

[8] A. R. Galindo and C. Marianno, “Remote laboratory for nuclear security education,” International journal of nuclear security, 2023.

[9] D. Uckelmann, D. Mezzogori, G. Esposito, M. Neroni, D. Reverberi, M. Ustenko, and J. Hauge, “Guideline to safety and security in federated remote labs,” Int. J. Online Biomed. Eng., vol. 17, pp. 39–62, 2021.

[10] I. Delgado, E. Sancristobal, S. Mart´ ´ın, and A. Robles-Gomez, “Ex-´ ploring iot vulnerabilities in a comprehensive remote cybersecurity laboratory,” Sensors (Basel, Switzerland), vol. 23, 2023.

[11] M. S. Mahmud, M. Sultana, S. T. Bevins, and G. Muhammad, “A software architecture style for building scada system software,” Journal of Object Technology, vol. 10, no. 3, 2011.

[12] C. Cicotti, L. Coppolino, S. D’Antonio, and L. Romano, “A secure and available multiprocessing remote laboratory for e-learning,” Journal of Circuits, Systems and Computers, vol. 17, no. 08, 2008.

[13] L. Feisel and A. Rosa, “The role of the laboratory in undergraduate engineering education,” Journal of Engineering Education, vol. 94, no. 1, pp. 121–130, 2005.

[14] M. Whitman and H. Mattord, Principles of Information Security, 6th ed. Boston, MA: Cengage Learning, 2017.

[15] P. Dourish, E. Grinter, J. Delgado De La Flor, and M. Joseph, “Security in the wild: User strategies for managing security as an everyday, practical problem,” Personal and Ubiquitous Computing, vol. 8, no. 6, pp. 391–401, 2004.

[16] L. Lamport, “Password authentication with insecure communication,” Communications of the ACM, vol. 24, no. 11, pp. 770–772, 1981.

[17] F. Meng, W. Li, Y. Zhao, and X. Han, “Enhancing password security for mobile devices by multifactor authentication,” IEEE Access, vol. 6, pp. 3056–3063, 2017.

[18] R. Li and T. Yu, “Scalable federated access control for web services,” in IEEE International Conference on Web Services, 2009.

[19] O. Inc, OpenVPN: Building and Integrating Virtual Private Networks. BrainySoftware, 2016.

[20] K. Kent and K. Seo, “Security architecture for the internet protocol,” Internet Engineering Task Force (IETF), 2005.

[21] E. Barker, “Recommendation for key management: Part 1–general,” US Department of Commerce, National Institute of Standards and Technology, Tech. Rep. 147, 2020.

[22] D. Ferraiolo, R. Sandhu, S. Gavrila, D. Kuhn, and R. Chandramouli, “Proposed nist standard for role-based access control,” ACM Transactions on Information and System Security, vol. 4, no. 3, pp. 224–274, 2001.

[23] V. C. Hu, D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang, "Guide to attribute based access control (abac) definition and considerations (draft)," *NIST special publication*, vol. 800, no. 162, pp. 1-54, 2013.

[24] K. Scarfone and P. Mell, “Guide to computer security log management,” US Department of Commerce, National Institute of Standards and Technology, Tech. Rep. 800-92, 2006.
[25] J. Rutkowska, “System virginity verifier: Defining the roadmap for malware detection on windows system,” Hack In The Box Security Conference, 2005.
[26] M. Roesch, "Snort: Lightweight intrusion detection for networks," in Lisa, 1999, vol. 99, no. 1, pp. 229-238.
[27] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, “A deep learning approach for network intrusion detection system,” 2015.
[28] S. Cantor and T. Scavo, "Shibboleth architecture," Protocols and Profiles, vol. 10, no. 16, p. 29, 2005.
[29] D. Security, “What is two-factor authentication (2fa)?” https://duo.com, 2020.
[30] T. Styra, “Open policy agent,” https://www.openpolicyagent.org/, 2020.
[31] V. Venkatesh, J. Thong, and X. Xu, “Unified theory of acceptance and use of technology: A synthesis and the road ahead,” Journal of the Association for Information Systems, vol. 17, no. 5, p. 2, 2016.
[32] M. Padilla, A. Khaled, and J. Smith, “The pars password manager: A password/authentication recognition system evaluation,” Human-centric Computing and Information Sciences, vol. 7, no. 1, 2017.
[33] L. Whitman, “enemy at the water cooler: Realities of insider threats,” in IFIP International Information Security Conference. Springer, Berlin, Heidelberg, 2004, pp. 7–122.
[34] C. Modi, D. Patel, B. Borisaniya, H. Patel, and A. Patel, “A survey on security tools for cloud computing environments,” Journal of Network and Computer Applications, vol. 35, no. 3, pp. 1001–1007, 2012.