CONTENTS

Task 01

Information assurance is one of the key factors to consider in an organization. It is the practice of protecting against security attacks or vulnerabilities and managing risks related to data process, transmission and storing. When we talk about information security, we must consider the CIA triad. They are confidentiality, integrity and availability.

Title

Mobile security and risk management

Affiliation 01: amaathil@std.appsc.sab.ac.lk
Correspondence: aathilmohamed98@gmail.com; Tel: (+94)764706791

Editor: Mohamed Aathil
E-mail:
amaathil@std.appsc.sab.ac.lk
Contact No: +94764706791
Postal-code: 30190

Received date: 19/10/2021
Accepted date: 22/10/2021
Published date: 26/10/2021

Abstract:
IT provides diverse technological solutions to ensure the security of day-to-day life, IT solutions become vulnerable to threats, so security for IT came to the subject. The knowledge gap of cryptography is one of the major dropping parts of security. The cryptographic algorithms were originally used as an encryption technique during civil wars. Earlier, IT security was referred only to the protection of desktops, laptops and servers. Now it has been quiet for a long time, and today's trending topic is mobile security.

Keywords: #security, #mobile, #risk, #cryptography, #hashing, #CIA

Introduction

Nowadays mobiles are everywhere. Mobile security is one of the most important parts that users to be considered to protect their privacy. There are a bunch of security issues are out there. In this article, I want to highlight a little bit about it. Data breaching, phishing attacks, Network spoofing, broken cryptography are some of them.

A data breach is an event where a piece of information is taken by a third party without the knowledge of the proprietor. Stolen data may include sensitive, proprietary, or confidential information such as credit card numbers, customer data, trade secrets, or matters of national security. If one of this sensitive information seeped into an anonymous person, the holder of this information will be worried and sometimes it can be a major effect on his life too. Phishing is a type of social engineering attack. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

Publishers Note:
This review article was published on SECURITY Journal on26/10/2021

For Further Networking and Cyber-Security articles: Scan the QR code that shown top of the paper

Network spoofing is a precise type of cyber-attack in which someone attempts to use a computer, device, or network to trick other computer networks by masked as a legitimate entity. This can be called IP spoofing. IP spoofing is the formation of Internet Protocol (IP) packets that have an adapted source address to either hide the uniqueness of the sender, to imitate another computer system. Broken Cryptography or unconfident usage of cryptography is mostly common in mobile apps that influence encryption. The use of a broken or risky cryptographic algorithm is a needless risk that may result in the exposure of sensitive information. The use of a non-standard algorithm is unsafe because a strong-minded attacker may be able to break the algorithm and compromise whatever data has been protected.

Discussion

In the discussion part, I want to discuss the solution for this security issue and the knowledge gap in this massive technical domain area. And also, what are the remaining problems in the security and risk management domain that we have not discussed earlier.

- **Solutions for the problems and the knowledge gap.**

  Malware can be industrialized and deployed as malicious apps that users unsuspectingly install on their devices. Mobile security answers should be able to detect and block downloads of these malicious apps. So, a well-informed user, / must knowledge about the prevent to downloading malicious apps from the software stores. If a user downloads an app from the web, he must download the apps from the legitimate and verified by SSL certificate given websites.

  Mobile devices and the genuine apps that run on them can be targeted at the network level. Man-in-the-Middle, phishing, and other attacks take advantage of network connectivity to steal data or bring malicious content. Mobile security includes blocking these network-level attacks.

  relationships between each of these sections within the information privacy and security settings, as well as the gaps that exist between privacy and security, as well as between knowledge and opinions. In the mobile environment, protecting an individual's information security and/or privacy needs actual conduct to be enacted. Prior research has suggested that intending to protect one's information privacy or security is not sufficient; one needs to use information protection practices to be protected.

  The research papers did great research on mobile security and risk management. They explained each security problem in detail. I agree with their research method and the way they handle explaining each security issue. Even though, there will be some remaining issues are out there. DDOS attacks are one of the famous attacks nowadays. They are very simple, but they can cause very serious problems to victims. Social engineering attacks, the man in the middle attacks,

viruses, spyware and adware are some other kinds of attacks. Ransomware is also important. It is a kind of attack that happens in mobile users, the attacker can ransom money or something from the victim to lease the acquired information.

Conclusion

So Mobile security requires a different method not absorbed on malware. Dripping apps that store or transmit sensitive personal and commercial data in an unconfident manner are of far greater concern at this point. Even legitimate apps without deliberately malicious functionality that are downloaded from official app marketplaces can comprise high-risk security issues. Mobile security requires classifying and remediating security issues in device OSs and configurations, the apps installed on those devices, and the network connections those devices make each day.

References

Kaspersky. (2021, April 26). *Top 7 Mobile Security Threats in 2020*. Www.Kaspersky.Com. Retrieved October 26, 2021, from https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store

Palter, J. (n.d.). *5 Critical Mobile Security Challenges & How to Solve Them*. Real Time Network. Retrieved October 26, 2021, from https://www.realtimenetworks.com/blog/5-critical-mobile-security-challenges-how-to-solve-them

RM Studio Team. (2019, January 15). *Mobile Devices and Information Security Risk Management*. Risk Management Studio. Retrieved October 26, 2021, from https://www.riskmanagementstudio.com/mobile-devices-and-information-security-risk-management/

What is Mobile Security? (2021, July 26). Check Point Software. Retrieved October 26, 2021, from https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-mobile-security/

Task 2

1.

The basics of all security systems are the moral values and practices and the professional standards of all employees of the association. These are some of the ethical issues related to Information Security.

User privacy

Privacy has developed legal insinuations, but there are also ethical thoughts. Do people know how their accounts are monitored? To what extent is such monitoring happening? Privacy worries can easily become a slippery slope, slowly corroding an individual's right to privacy entirely.

Security Liability

Security systems for digital networks are computerized to defend energetic information and important assets. However, this amplified security comes with the increased investigation. Eventually, IT professionals want to balance risk with independence to create a security system that is active and ethical at the same time.

Access costs

The matter even spreads to private Internet repetition since the cost of ability in some areas may be cost-prohibitive. The greater ethical question is whether or not digital exchange is now a universal right. The cost of access can obstruct business growth, entrepreneurial spirit and individual look.

Digital proprietorship or intellectual property

Digital mediums have permissible information to flow more easily than before. This exchange of thoughts comes with a lawful and ethical reaction. How can ownership be recognized in the digital realm? Things can be easily copied and pasted online, which makes intellectual property hard to control. Legal notions such as copyright have struggled to keep up with the digital era.

2.

Communities of interest must reflect preparations as the aim for all data security activities. Security methods are the least costly controls to execute however most hard to objectify and shape the policy. Data Security Policy, Standards and Practices Management from all groups of plotting must consider approaches as the aim for all data security arranging, plan, and organization.

Quality security agendas start and end with a method. As data security is an administration as opposed to a specialized issue, strategy guides the workforce to work in a way that will add to the security of its data resources.

Organizing SETA programs are a good path to teach employees about security. SETA is a program intended to help organizations to alleviate the number of security breaches produced by human error. It can be a very real and organized method to train, educate, and raise awareness of everything having to do with security and protecting their data. This can then result in people becoming more security-aware. Thus, lessening security incidents due to people thinking and being alert of security issues. Which would protect the organization and any data or information that is allied with the user or group.

3.

Intellectual property (IP) denotes to makings of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce.

First, the creator must control, if an originator has rights to the intellectual property in a specific country. Patents and trademarks are regional and must be listed in each country where defence is required.

The current intellectual property legal government in Sri Lanka is ruled by the Intellectual Property Act, No. 36 of 2003 which makes supplies for a variety of intellectual property rights and their achievement, organization and implementation. The National Intellectual Property Office of Sri Lanka recognized under this law is the only Government Department, which is accountable for the management and control of the intellectual property system in Sri Lanka.

References

5 Legal and Ethical Issues in IT – Best Computer Science Degrees. (n.d.). Best Computer Science Degrees. Retrieved October 26, 2021, from https://www.bestcomputersciencedegrees.com/lists/5-legal-and-ethical-issues-in-it/

Naveengupta40, A. (2017, October 12). *Discuss how an organization institutionalizes its policies, standards, and practices using education, training, and awareness programs?* Site Title. Retrieved October 26, 2021, from https://naveengupta40.wordpress.com/2017/10/11/discuss-how-an-organization-institutionalizes-its-policies-standards-and-practices-using-education-training-and-awareness-programs/

Security Education Training and Awareness (SETA) – IT Living Lab. (n.d.). IT Living Lab. Retrieved October 26, 2021, from https://livlab.org/seta/

What is Intellectual Property (IP)? (n.d.). WIPO. Retrieved October 26, 2021, from https://www.wipo.int/about-ip/en/

Task 03

1)

An Intrusion Detection System (IDS) is a network security technology initially built for detecting vulnerability feats against a target application or computer. An IDS is a device or software application that monitors a network or systems for malicious action or policy defilements. Any intrusion activity or violation is classically stated either to an administrator or collected centrally using a security information and event management system.

Categories of IDS

1. Host-based IDS

It is used at the system level. The system traffic is monitored for any malicious events. Such an IDS can take system snapshots whenever there is any alteration or alert. A host-based IDS is that monitors the computer infrastructure on which it is connected, examining traffic and logging malicious conduct.

Host-based intrusion detection systems (HIDSs) are applications that function on the information composed from individual computer systems. This vantage point lets a HIDS analyze actions on the host it monitors at a high level of part, it can frequently control which processes and/or users are involved in malicious activities. Furthermore, unlike NIDSs, HIDSs are privy to the outcome of a tried attack since they can straight admission and monitor the data files and system processes targeted by these attacks.

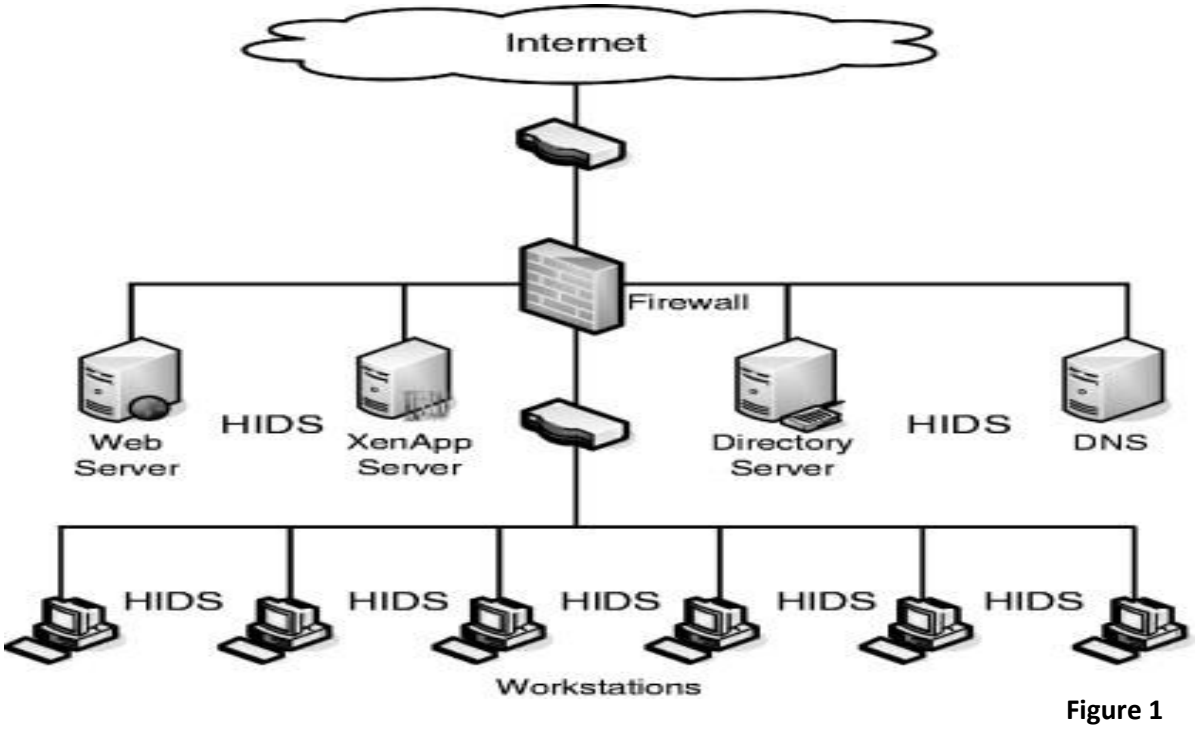


Figure 1

2. Network-based IDS

A network-based intrusion detection system is intended to help administrations monitor their cloud, on-premise and hybrid environments for suspicious actions that could designate cooperation. This includes policy violations and port scanning, plus unknown source and destination traffic.

IDS is a technology or application built for safeguarding networks from vulnerability feats to deliver you with the competence to quickly respond to and stop spoofed, illegal network packets from contaminating your target systems. An efficient IDS program logs all incoming and outgoing traffic, keeping an eye on information packets being conveyed across the network and subjects an alert if the traffic deviates from the usual pattern. This way, you're warned about possible intrusion threats early on, enabling you to reply to such threats proactively.

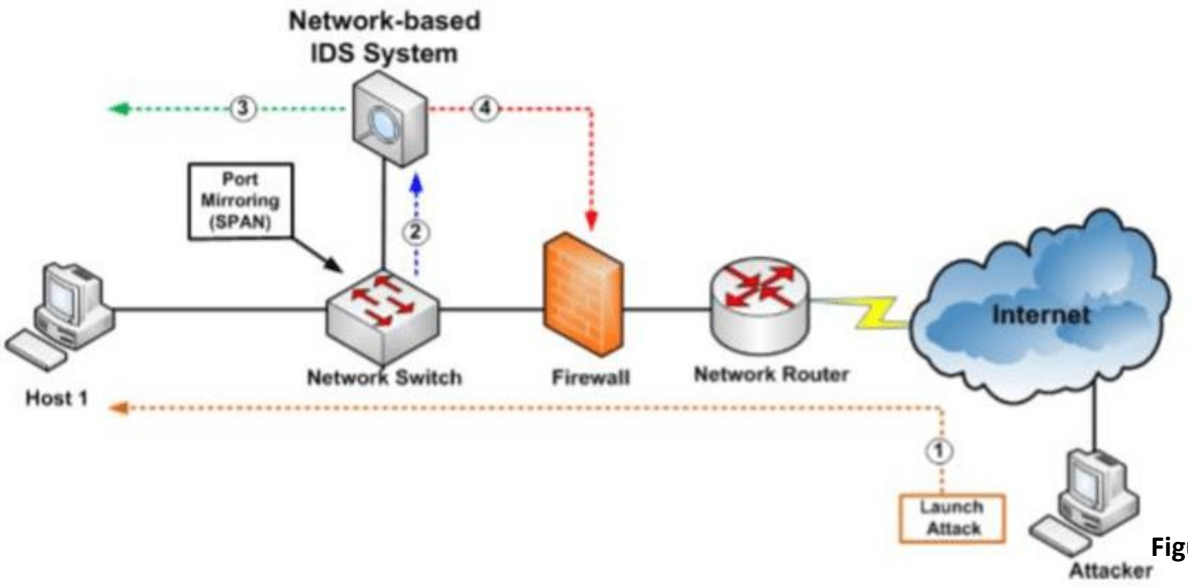


Figure 2

3.

Anomaly-Based Intrusion Detection System (AIDS)

This type of IDS is based on a technique or an approach where the program monitors your continuing network traffic and examines its pattern against predefined norms or baseline. It then classifies and alerts the management to unusual behaviour across network bandwidth, devices, ports, protocols, etc.

Anomaly-based IDSes classically work by taking a baseline of the normal traffic and activity taking place on the network. They can amount the present state of traffic on the network against this baseline to notice patterns that are not present in the traffic usually.

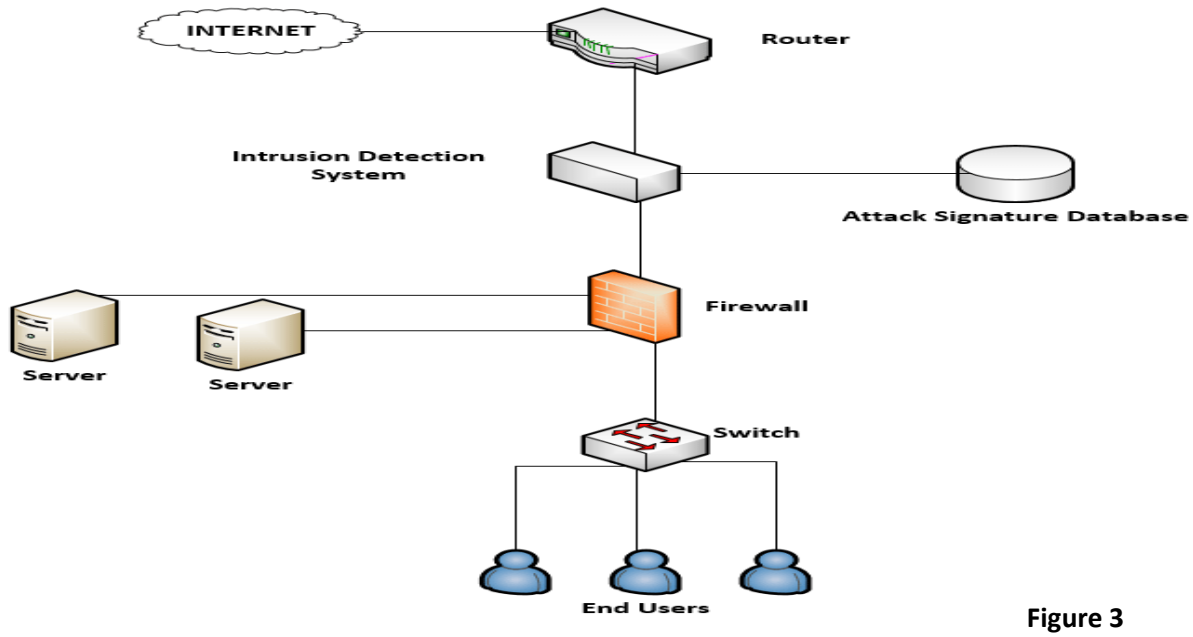


Figure 3

2)

A firewall is a kind of cybersecurity tool that is used to filter traffic on a network. Firewalls can be used to distinguish network nodes from outside traffic sources, internal traffic sources, or even specific applications. Firewalls can be software, hardware, or cloud-based, with the respective type of firewall having its sole pros and cons. The prime goal of a firewall is to block malicious traffic needs and data packets while allowing legitimate traffic through.

Firewall types can be separated into several different classes based on their overall construction and technique of operation. Here are eight types of firewalls:

- Packet-filtering firewalls
- Circuit-level gateways
- Stateful inspection firewalls
- Application-level gateways (a.k.a. proxy firewalls)
- Next-gen firewalls
- Software firewalls
- Hardware firewalls
- Cloud firewalls

Packet-Filtering Firewalls

As the most "basic" and oldest type of firewall architecture, packet-filtering firewalls essentially create a checkpoint at a traffic router or switch. The firewall achieves a simple check of the data packets coming through the router reviewing information such as the terminus and beginning IP address, packet type, port number, and other surface-level information without opening up the packet to examine its insides.

Circuit-level gateways

As an additional unsophisticated firewall type that is meant to quickly and easily favour or deny traffic without overwhelming significant computing resources, circuit-level gateways work by confirming the transmission control protocol (TCP) handshake. This TCP handshake check is designed to make sure that the session the packet is from is legitimate.

Stateful Inspection Firewalls

These firewalls syndicate both packet review technology and TCP handshake verification to create a level of defence greater than either of the preceding two architectures could provide alone.

Proxy Firewalls (Application-Level Gateways/Cloud Firewalls)

Proxy firewalls function at the application layer to filter incoming traffic between your network and the traffic source hence, the name "application-level gateway." These firewalls are brought via a cloud-based solution or additional proxy device. Rather than letting traffic connect straight, the proxy firewall first creates a connection to the source of the traffic and checks the received data packet.

Next-Generation Firewalls

Numerous of the most recently-released firewall products are being advertised as "next-generation" architectures. However, there is not as much agreement on what makes a firewall truly next-gen.

Software Firewalls

Software firewalls comprise any type of firewall that is installed on a local device rather than a distinct piece of hardware (or a cloud server). The big benefit of a software firewall is that

it's highly useful for creating defence in depth by isolating separate network endpoints from one another.

Hardware Firewalls

Hardware firewalls use a physical application that acts in a manner alike to a traffic router to interrupt data packets and traffic requests before they're connected to the network's servers. Physical appliance-based firewalls like this excel at perimeter security by making sure malicious traffic from outside the network is interrupted before the company's network endpoints are unprotected to risk.

Cloud firewall

Whenever a cloud solution is used to deliver a firewall, it can be called a cloud firewall, or firewall-as-a-service (FaaS). Cloud firewalls are considered identical with proxy firewalls by many since a cloud server is frequently used in a proxy firewall setup.

3)

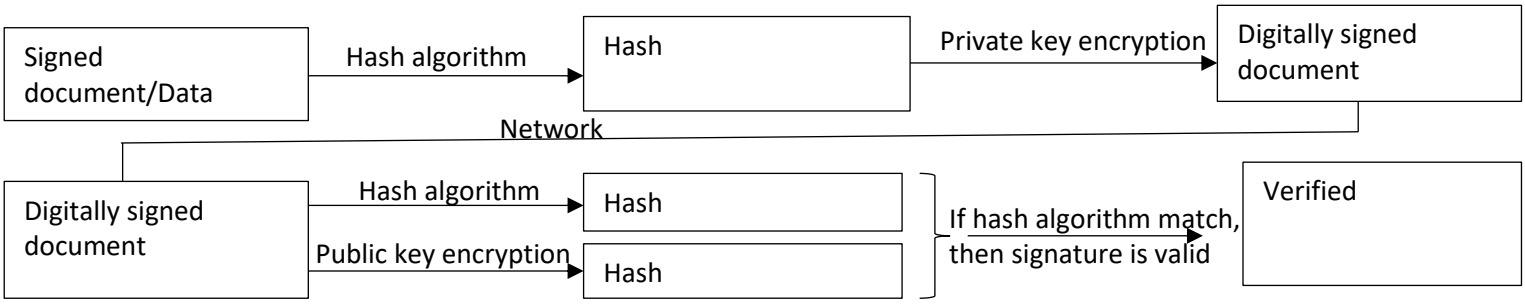
A digital signature is a mathematical method used to authenticate the authenticity and integrity of communication, software or digital text. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more essential security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.

Digital signatures can deliver an indication of the source, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge informed consent.

Digital signatures are founded on public-key cryptography, also known as asymmetric cryptography. Using a public key algorithm, such as RSA (Rivest-Shamir-Adleman), two keys are generated, creating a mathematically linked pair of keys, one private and one public.

Digital signatures work through public-key cryptography's two equally validating cryptographic keys. The individual who creates the digital signature uses a private key to encrypt signature-related data, while the only method to decrypt that data is with the signer's public key.

Digital signature process



The value of a hash is sole to the hashed data. Any alteration in the data, even an alteration in a single charm, will result in a different value. This attribute allows others to use the signer's public key to decrypt the hash to authenticate the integrity of the data.

If the decrypted hash matches a second calculated hash of the same data, it shows that the data hasn't changed since it was signed. If the two hashes don't match, the data has also been interfered with in some way and is cooperated or the signature was created with a private key that doesn't agree to the public key obtainable by the signer and matter with verification.

References

Dosal, E. (2019, November 26). *What is a Firewall? The Different Firewall Types & Architectures*. COMPUQUIP. Retrieved October 26, 2021, from https://www.compuquip.com/blog/types-firewall-architectures

Host-Based Intrusion Detection Systems - an overview | ScienceDirect Topics. (n.d.). ScienceDirect. Retrieved October 26, 2021, from https://www.sciencedirect.com/topics/computer-science/host-based-intrusion-detection-systems

Lutkevich, B., Brunskill, V., Loshin, P., & Cobb, M. (2021, February 5). *digital signature*. SearchSecurity. Retrieved October 26, 2021, from https://searchsecurity.techtarget.com/definition/digital-signature

NIDS | Network Intrusion Detection System. (2021, August 10). Redscan. Retrieved October 26, 2021, from https://www.redscan.com/services/managed-intrusion-detection-system/nids/

What is an Intrusion Detection System (IDS) & How does it work? (2020, June 19). TekTools. Retrieved October 26, 2021, from https://www.tek-tools.com/security/what-is-an-intrusion-detection-system-ids

Task 4

The COVID-19 pandemic has pretentious school teaching universal, foremost to the near-total closures of schools. Most governments about the world have provisionally closed schools in an attempt to cover the feast of the COVID-19 epidemic. School ends impression not only students, teachers, and families, but carry high social and economic costs for people across communities.

Through the growth of distance teaching technologies, particularly online education, the project aimed to upsurge access to post-secondary education in Sri Lanka while refining the quality and relevance of learning by introducing both blended learning programmers and fully-online programmers. Online culture helps students to create and interconnect new ideas. You get the chance to upheaval your skills and gain knowledge separately from school education. One of the prime rank of e-learning is that it helps students and teachers develop progressive services.

In order to examine the transmission of COVID-19, we accepted the Vulnerable Exposed Infectious–Recovered (SEIR) model with control events practical to the high-risk zones in the country. Since the incubation period for the disease is 2–14 days as reported, there is a high option of transmission prior to the onset of symptoms and without showing symptoms [11], which justifies the adoption of the SEIR model. In the classical SEIR model, a population of size in the th region is divided into vulnerable exposed infected, and recovered components. We extended the model by including an extra compartment as hospitalized. This involved all those entering hospitals and quarantine centers. The susceptible class consists of individuals who can possibly get infected by the disease. If the susceptible person is bare to the virus, the individual is moved to the exposed compartment at the rate of . Let be the change rate of the exposed individuals to the infected class. Infected individuals, those who are hospitalized, are moved to the newly added compartment hospitalized at the rate of. Infected persons in compartments and are enthused to the healthier section after the infectious period, and the persons in the recovered class are assumed to have permanent immunity against the disease.

Coldness education is here to stay in approximately form or the other, at least in the foreseeable future. Ensuring effective remote education is chiefly challenging for TV broadcasts as opposed to online teaching, where programmer design has to ensure steadiness in the face of the central teacher. Given that TV is the most possible way of attainment less-privileged students in Sri Lanka, is it crucial to address existing pedagogical and logistical issues.

A learning organization system (LMS) is a processer program application for the organization, documentation, following, announcing, robotization and conveyance of educational courses, preparing programs, or education and improvement agendas. The erudition administration system concept developed specifically from e-Learning. In spite of the fact that the primary LMS showed up within the advanced training segment, the larger part of the LMSs now center

on the corporate market. Knowledge Administration Agendas make up the largest section of the learning framework market.

References

Erandi, K. K. W. H. (2020, September 22). *Effectiveness of the Strategies Implemented in Sri Lanka for Controlling the COVID-19 Outbreak.* Hindawi. Retrieved October 26, 2021, from https://www.hindawi.com/journals/jam/2020/2954519/

Pozo, J. (n.d.). *Teaching and Learning in Times of COVID-19: Uses of Digital Technologies During School Lockdowns*. Frontiers. Retrieved October 26, 2021, from https://www.frontiersin.org/articles/10.3389/fpsyg.2021.656776/full

Situation Analysis on the effects of and Responses to COVID-19 on the Education Sector in Sri Lanka. (2021, March 1). UNICEF Sri Lanka. Retrieved October 26, 2021, from https://www.unicef.org/srilanka/reports/situation-analysis-effects-and-responses-covid-19-education-sector-sri-lanka