Assuring the Optimum Security Level for Network, Physical and Cloud Infrastructure

Ali T. Atieh

ORCID

EGM- IT Infrastructure Operation, Etihad Etisalat – MOBILY

Abstract

A robust and secure IT infrastructure ensures reliable security, high speeds and connectivity, employee support and accessibility, and a positive user experience for clients. It is hard to manage a modern firm without a secure and adaptable IT infrastructure. Technology, when properly set up and networked, can improve back-office processes, increase efficiency, and simplify communication. This research explores how an organization assure the optimum level of infrastructure security in in three domains: network infrastructure security, physical infrastructure security, and cloud infrastructure security. Running a network infrastructure model comes with a variety of difficulties. The findings suggest that there are few recommendations for assuring right security level for the network infrastructure, including: conducting a network security assessment, keeping user access privileges to a bare minimum for work, updating programs, investigating cybersecurity tools and Increasing cyber-awareness. Physical infrastructure security is also crucial. We divided he dangers are divided into the following categories and suggested for appropriated measure: threats by environment, threats by technical infrastructure, threats by humans, inappropriate humidity and temperature, Electrification, Electromagnetic Interference (EMI), Unauthorized physical access. Cloud security is necessitated by the widespread adoption of cloud technology, as well as an ever-increasing volume and sophistication of cyber attacks. To ensure the right level of cloud security, this research recommend to take some measures, including: Transit and Rest Protection, Asset Security. Securing User Management, Integration of compliance and security, Authentication and Identity, and Operational Safety and Security While no amount of security will ever stop all attacks, organizations can significantly minimize risk of suffering a breach and the fallout from such attacks by taking a few critical steps to secure business' network, physical and cloud infrastructure.

Introduction

Every business plan now includes IT infrastructure as a critical component. IT is used by everyone from multinational enterprises with mainframe systems and databases to tiny businesses with a single computer. The easiest way to figure out why computer technology is so widely employed in business is to look at how it is used in different industries. Information technology aids in the development and expansion of the commerce and commercial sectors, as well as the generation of maximum production. With advancements in information technology, the time it takes for diverse industries to produce business is now reduced. It offers electronic security, storage, and communication efficiency (Roche, 1992).

Data flow, storage, processing, and analysis are supported by information technology infrastructure, which is made up of physical and virtual resources (Liu et al., 2015). Infrastructure can be centralized within a data center or distributed among numerous data centers operated by the company or a third party such as cloud provider. As a company expands, so do its requirements. Through all of the changes that enterprises and their clients go through, an efficient IT infrastructure remains (Luftman, Lewis and Oldach, 1993).

The IT infrastructure of today's business is far more complex than it has ever been, and it often include both on-premises and cloud-based systems, as well as company-owned and employee-owned devices (such as laptops and smartphones) and Internet of Things (IoT) devices like cameras and industrial sensors (Sterk and Spruijt, 2013). Many of these devices were either not designed with security in mind or had a patchwork of security solutions done after the fact. Finally, the managing organization is responsible for securing all of these systems.

Infrastructure security, including critical infrastructure security, is essential for averting damage to technology assets and data as a result of an attack or disaster. It's also vital for limiting the amount of damage caused by a successful attack or a natural disaster. Similarly, the major purpose of infrastructure security is to reduce the organization's total risk level, which reduces the likelihood of a severe operational disruption and/or financial damage (Biringer, Vugrin and Warren, 2013).

Infrastructure security is the lynchpin of any company's overall security strategy because it sits at the heart of their technology operations. Infrastructure security can be thought of as the organization's master security plan, which underpins tactical strategies and everything else that is produced around it.

Traditional and cloud infrastructure are the two main forms of IT infrastructure. The typical hardware and software components of a traditional IT infrastructure include facilities, data centers, servers, networking hardware, desktop PCs, and corporate application software solutions (IBM, 2021). This infrastructure arrangement typically necessitates more power, physical space, and financial resources than other infrastructure kinds. A conventional infrastructure is often built on-premises for use by a single organization or in a private environment (IBM, 2021).

Cloud computing is a type of computing that uses the internet to traditional infrastructure is analogous to IT infrastructure (Atieh, 2021b). End users, on the other hand, can connect to the infrastructure over the internet and consume computing resources without having to install anything on their own thanks to virtualization. Virtualization connects physical servers that a service provider maintains in one or more locations. The system then splits and abstracts resources, like as storage, so that users can access them practically everywhere there is an internet connection.

Infrastructure security encompasses not only defense against classic cyberattacks, but also defense against natural catastrophes and other calamities. It also touches on the subject of resilience, which is concerned with how an organization recovers after an attack or other interruption (Lawson, 2011). The ultimate goal is to improve security and reduce downtime, as well as the accompanying customer attrition, brand and reputation damage, and compliance costs that enterprises incur. Fundamentally, infrastructure security refers to a high-level approach to safeguarding an organization's whole technological perimeter.

2. Securing a Network Infrastructure

Network infrastructure can be defined as the hardware and software assets of a whole network that allow network connection, communication, operations, and management of a corporate network are referred to as network infrastructure. It connects users, processes, applications, services, and external networks/the internet by providing a communication path and services (Garbis and Chapman, 2021).

Network-level infrastructure security occupies the majority of resources in most businesses' infrastructure security programs. When it comes to security risk, the network level is often considered the largest and most vulnerable of the company, and as a result, there are more methods available to safeguard the network level than at other levels (Andrés, Kenyon and Birkholz, 2004).

The firm must exercise the utmost caution when it comes to network infrastructure. Patches must be applied as soon as they are published, configurations must be double-checked to ensure they are right, and rules must be developed and followed to keep the network as secure as possible.

The goal of network infrastructure security is to prevent all of the problems mentioned above. Network infrastructure security monitors hardware and software, protects the network infrastructure from malicious attacks, enforces access control rules and ensures that only authorized users have access to network resources, detects and removes malware, and provides secure channels for remote users, such as a virtual private network (VPN) (Andrés, Kenyon and Birkholz, 2004).

Some Network Infrastructure Challenges

Running a network infrastructure model comes with a variety of difficulties. The following are three of the top three network infrastructure challenges (Kaeo, 2004) (Yeung, Yan and Leung, 2006) (Hansen, 1997) (Wong and Yeung, 2009):

1. Traffic Consolidation

There are frequently several subnets and locations or sites inside a company. Network visibility, monitoring, and management can become nearly impossible without a centralized hub. To better comprehend and manage the data transiting their networks, many firms deploy network

infrastructure solutions to centralize traffic. This improves their security posture while also assisting their network operations teams in resolving performance concerns (Bouchard, 2010).

2. Duplicate Data

Duplicate data can account for a large portion of network bandwidth in some circumstances. When it comes to the efficiency of network security measures, removing redundant data is crucial. Security solutions may be slower and less efficient in detecting threats if they receive too much duplicate data (Pawar and Anuradha, 2015).

3. Correct Information for the Correct Tool

Many businesses utilize a variety of cyber security solutions and service providers. Many security firms base their fees on the amount of data they must process. As a result, transmitting the appropriate data to the appropriate tool is an important part of infrastructure networking. Sending data from multiple sources to the same tool could be inefficient and costly, especially if one tool is better suited to one sort of data while another is more suited to another (Pawar and Anuradha, 2015).

Assuring right security level for the network infrastructure

1) Conducting a Network Security Assessment

A network security audit is, at its most basic level, a process through which a corporation investigates its network security rules and the many assets it has on its network in order to discover any potential flaws that could lead to a security compromise or breach. These audits are frequently done by a private entity, such as a managed security service provider (MSSP), but some larger firms with more strong budgets can also conduct such audits internally (Manzuik, Pfeil and Gold, 2006).

Multiple review processes are covered by a comprehensive audit, including:

- **Identifying assets:** Identifying what are the different types of assets on the network, and what software and operating system (OS) are they running. Knowing what's on network is critical for seeing potential flaws and addressing them, such as software that hasn't been updated with the latest security patch (Hu et al., 2019).
- **Security Procedures and Policies:** When it comes to keeping company's data secure, it is important to identify what criteria does each member of the team understand/follow. It can be a

BYOD (bring-your-own-device) policy in place at place of business (Disterer and Kleiner, 2013). It is also crucial to device what are the methods for enforcing security policies, and to check all of security rules and processes in order to keep data safe.

- Firewall configurations and architectures: Investigating what firewall solutions have in place, and where do they reside on network (at the perimeter, between specific servers/assets). Firewall configurations must be up to date and free of conflicts so that an attacker can not exploit (Fulp, 2007).
- Risk evaluation: Identifying the most serious dangers that are needed to address as soon as possible after identifying all of the assets on network and assessing security policies/procedures. Risk assessments assist in prioritizing cybersecurity activities so that the most serious flaws are addressed first.

This type of cybersecurity audit is an important initial step in defending a network infrastructure against future intrusion attempts since it allows to detect and correct major security gaps. It can also assist in determining which of the next few tasks security management team should prioritize based on the dangers have been discovered (Sabillon et al., 2017).

2) Keep user access privileges to a bare minimum for work.

Company can not avoid or mitigate insider attacks if three-quarters of them are malevolent, or carried out on purpose by users with legitimate access. Applying a policy of least privilege (POLP) to every user account on the network is one method.

Users on the network are limited to have only the level of access they require to fulfill their main job function. The main advantage is that it reduces the chance of an insider stealing data significantly—especially if network assets are completely isolated from one another. It is also possible to limit the amount of data an employee can compromise without breaching other defenses by limiting access, which offers intrusion detection system (IDS) a better chance of detecting odd activity (Ashoor and Gore, 2011).

3) Updating programs

Unpatched software on the network is another serious security risk. Companies are always looking for and repairing security weaknesses in their software and systems, flaws that allow hackers to get past supposedly impenetrable safeguards.

While many people are concerned about "zero-day" exploits—vulnerabilities that the original software creator is unaware of and which hackers can exploit with impunity—the truth is that the most commonly utilized exploits employ older, well-known security concerns for which remedies are already available (Wang et al., 2013).

So, after a security audit, one of first goals should be to review the list of software on each of network assets and ensure that they all have the most recent security patches—especially if the software version is years old. If software become such that the original creator no longer supports, it may be time to uninstall it and replace it with a newer program with up-to-date protection.

4) Investigating cybersecurity tools.

It is important to check if right tools in place to adequately manage the cybersecurity risks in network. While organizations don't need to buy every cybersecurity product on the market to safeguard company's network infrastructure, they need at the very least cover the essentials for lowering risks and meeting industry's regulatory duties. During the audit, IT tams should have made a list of all the assets on network, including the particular cybersecurity tools (firewalls, IDS/IPS, antivirus, remote backups, and so on) that can be employed to respond to most serious threats. (Jin et al., 2018)

5) Increasing cyber-awareness

Employees are frequently the weakest link in any organization's cybersecurity architecture, especially if those employees haven't received cybersecurity awareness training (Zwilling et al., 2020). Employees who aren't aware of the numerous online hazards may fall victim to phishing attacks, download viruses to their workstations, or choose passwords that are easy to guess, allowing others to take over their accounts.

Cybersecurity awareness training fills in the biggest knowledge gaps in staff, teaching them about the hazards and how to spot basic phishing efforts. This can assist protect workforce's human aspect from cyber-attacks.

Physical infrastructure security

Physical security protects the physical assets that facilitate the storage and information processing in information systems. Physical security necessitates the fulfillment of two requirements. First and foremost, physical security must protect the information system's physical infrastructure. In general, that infrastructure consists of the following:

- Hardware for the information system Data processing and storage equipment, transmission and networking infrastructure, and offline storage medium are all included. Supporting documentation can be included in this category.
- A physical location. The system and network components are housed in buildings and other facilities.
- Supporting infrastructure. The information system's operation is supported by these facilities. Electrical power, communication services, and environmental controls are all included in this category (heat, humidity, etc.).
- Employees. Control, maintenance, and use of information systems are all done by humans. (Amin, 2010)

Second, physical security must prevent physical infrastructure misuse that results in the misuse or harm of protected information. Misuse of physical infrastructure can be unintentional or intentional. The working position of the information system, which can be classified as static, mobile, or portable, has an impact on physical security. A mobile system is housed in a vehicle that acts as a support framework for the system. Portable systems do not require a single installation point and can be used in a range of environments, including buildings and open spaces. The nature and severity of risks of various categories, such as fire, roof leaks, unauthorized access, and so on, are determined by the nature and severity of the system's installation (Mikhalevich and Trapeznikov, 2019).

PHYSICAL SECURITY PREVENTION AND MITIGATION MEASURES

Inappropriate Humidity and Temperature

It's essentially a matter of having suitable environmental-control equipment and sensors to warn of thresholds being exceeded to deal with this problem. Aside from that, the main requirement is the upkeep of a power source (Hernández et al., 2012).

Threats from Technology

Each piece of important equipment should have an uninterruptible power supply (UPS) to deal with temporary power outages. The UPS is a battery backup system that can keep CPUs, displays, and other devices running for several minutes. Surge protectors, power noise filters, and automated shutdown devices can all be used with UPS units when the battery runs low. Critical equipment should be connected to an emergency power source, such as a generator, during lengthier blackouts or brownouts (Bey and Moecke, 2007). Management must address a variety of concerns, including product selection, generator siting, employee training, testing and maintenance schedules, and so on, in order to provide reliable service. A combination of filters and shielding can be employed to deal with electromagnetic interference (Gazizov et al., 2016). The technical specifications will be determined by the infrastructure design as well as the expected sources and nature of the interference.

Physical Threats Caused by Humans

Physical access control is the broad approach to human-caused physical risks. There are a variety of ways that can be utilized to limit access to equipment. These techniques can be used in conjunction with one another:

- Physical contact with a resource is limited by limiting access to the facility that houses the item. This method is designed to prevent outsiders from gaining access, but it does not address the issue of unauthorized insiders or workers.
- Physical interaction with a resource is limited by locking it away in a cabinet, safe, or room (Hurst, Merabti and Fergus, 2014).
- A machine can be accessible, but it is locked (perhaps permanently attached) to a difficult-to-move object. Theft will be deterred, but not vandalism, unlawful entry, or misuse.
- The power switch is controlled by a security device. A portable object is equipped with a tracking device so that its current location can be continuously monitored.

Cloud security:

1. Transit and Rest Protection

The data protection in transmission between (the end-user) and the provider is a vital feature of security when shifting to a cloud service. For both company and the provider, this is a two-fold responsibility. To avoid data interception, company will require network protection, as well as

encryption to prevent an attacker from accessing any data that is intercepted. Company should look for a security management team who can supply with a set of tools that will allow to easily encrypt data both in transit and at rest. This ensures the same level of security for any internal data transfers within the cloud service provider, as well as data transfers between the cloud service provider and other services that may expose APIs (Albugmi et al., 2016).

2. Asset Security

When choosing a cloud service provider, it's important to know where data is physically kept, processed, and maintained. This is especially critical now that government and industry laws such as GDPR have been implemented. To protect assets, a competent provider will have enhanced physical security in their data center to prevent illegal access to data. They'll also make sure the data assets are wiped before any resources are re-provisioned or discarded, so it doesn't end up in the wrong hands (Kemp, 2018).

3. Control and visibility

The capacity to see and control company's own data is an important aspect of security. A competent service provider will supply with a solution that gives complete insight over data and who is accessing it, no matter where it is or where company is. The supplier should provide activity monitoring so the company can keep track of changes to its ecosystem's setup and security (Yeluri and Castro-Leon, 2014).

4. A trusted security marketplace and a network of partners

It will take more than one solution or partner to secure cloud deployment. Through a marketplace, a good cloud service provider will make it simple for a company to identify and connect with various partners and solutions. It important to look for a provider that has a marketplace with a selected network of reputable partners who have a proven track record in terms of security. Security solutions that provide one-click setup and are complementary in securing data should be available in the marketplace, whether the company using a public, private, or hybrid cloud (Ali, Sabetta and Bezzi, 2013).

5. Secured User Management

A reputable cloud service provider would include solutions for secure user management. This will help to prevent unwanted access to management interfaces and procedures, ensuring the security of applications, data, and resources. The cloud provider should also have the ability to build

security measures that separate users and prevent any malevolent (or compromised) user from interfering with another's services and data (Muthurajkumar et al., 2015).

6. Integration of compliance and security

Security and compliance go hand in hand when choosing a cloud service provider. They must meet worldwide compliance norms that have been verified by a third party. A company should look for a cloud service provider that follows industry best practices for cloud security and, preferably, has a recognized certification. The Security, Trust, and Assurance Registry (STAR) program of the Cloud Security Alliance is a good indicator. The organization would also need to find a security management team with sector-specific accreditation if it is in a highly regulated field, such as healthcare, where HIPPA, PCI-DSS, and GDPR may apply (Shaheen, 2021c) (Shaheen, 2021b) (Shaheen, 2021a)(Joshi, Elluri and Nagar, 2020). The cloud service provider should allow the company to inherit their security measures into own compliance and certification procedures to guarantee that the compliance activities are both cost-effective and efficient.

7. Authentication and Identity

Access to any service interface should be limited to authorized and authenticated individuals only, according to cloud provider. When looking for a provider, seek for one that offers username and password authentication, two-factor authentication, TLS client certificates, and identity federation with current identity provider. Organizations may also want to be able to limit access to a dedicated line, an enterprise network, or a community network. To avoid interception, a good service only uses secure routes for authentication, such as HTTPS. Organizations should avoid services that use insecure authentication methods (Sharma, Gupta and Laxmi, 2014). This exposes the systems to unauthorized access, which could result in data theft, service modifications, or a denial of service.

8. Operational Safety and Security

Cloud providers who offer robust operational security to identify and prevent threats when choosing a cloud service should be chosen. robust operational security includes the following four elements:

- a) Management of Configuration and Change. The security management team should open about the assets that make up the service, such as any configurations or dependencies. They should notify of any modifications to the service that may affect security in order to avoid vulnerabilities. b)

Management of Vulnerabilities. To detect and mitigate any new threats to their service, security management team should have a vulnerability management procedure in place (Atieh, 2021a). These risks, their severity, and the anticipated threat mitigation schedule, which includes resolution, should all be maintained up to date. c) Monitoring for Safety. The security management team will have sophisticated monitoring mechanisms in place to detect any assault, misuse, or malfunction. They will respond to any incidents quickly and decisively, keeping the organization informed of the outcome. d) Management of Incidents. For common forms of assaults, security management team will have a pre-planned incident management approach in place. They will be prepared to use this procedure in the event of an attack. There will be a clear way to report any events, with a timeframe and manner that is acceptable (Ruo-xin et al., 2014).

The security management team, in addition to screening, must ensure that their members are aware of their security duties and receive frequent training. They should also have a policy in place to limit the number of persons who have access to the services and can influence them.

Conclusion

The process of putting safeguards in place to secure an enterprise's IT environment is known as IT infrastructure protection. An IT infrastructure includes all of a company's technology, including any networks, essential software, and hardware components such as servers and workstations. An organization's IT infrastructure includes anything that can link to the internal network, such as cloud resources or IoT devices, rather than just the technology inside its buildings.

Internal and external assaults aimed at stealing information, destroying data, or gaining control of resources continue to be a continual threat to IT infrastructures. Such catastrophic breaches can damage an organization, causing day-to-day activities to stall or stop, and causing severe damage to a company's reputation. Through countermeasures like as intrusion deterrence and identification, security surveillance, encryption techniques, and configuration management, IT infrastructure protection activities try to limit the danger of such assaults.

Companies can no longer simply depend on an ad hoc strategy to security as attackers change and their strategies become more advanced. With today's ever-changing threat landscape, businesses of all sizes must aim to be nimble, developing and refining security policies that are as diverse as the infrastructures they cover on a regular basis.

Enterprises can guarantee that their mission-critical data is appropriately safeguarded by developing a security strategy that includes plans, procedures, and a portfolio of compensating.

The best method to offer broad IT infrastructure defense, preventing attacks from both inside and outside of businesses, is to thoughtfully design security for every component of IT infrastructure, including: network, physical and cloud.

References

- Albugmi, A. *et al.* (2016) 'Data security in cloud computing', in *2016 Fifth international conference on future generation communication technologies (FGCT)*. IEEE, pp. 55–59.
- Ali, M., Sabetta, A. and Bezzi, M. (2013) 'A marketplace for business software with certified security properties', in *Cyber Security and Privacy Forum*. Springer, pp. 105–114.
- Amin, S. M. (2010) 'Electricity infrastructure security: Toward reliable, resilient and secure cyber-physical power and energy systems', in *IEEE PES General Meeting*. IEEE, pp. 1–5.
- Andrés, S., Kenyon, B. and Birkholz, E. P. (2004) *Security Sage's guide to hardening the network infrastructure*. Elsevier.
- Ashoor, A. S. and Gore, S. (2011) 'Importance of intrusion detection system (IDS)', *International Journal of Scientific and Engineering Research*, 2(1), pp. 1–4.
- Atieh, A. T. (2021a) 'Establishing Efficient IT Operations Management through Efficient Monitoring, Process Optimization, and Effective IT Policies', *Empirical Quests for Management Essences*, 1(1), pp. 1–12. Available at: <https://researchberg.com/>.
- Atieh, A. T. (2021b) 'The Next Generation Cloud technologies: A Review On Distributed Cloud, Fog And Edge Computing and Their Opportunities and Challenges', *ResearchBerg Review of Science and Technology*, 1(1), pp. 1–15. Available at: <https://researchberg.com/>.
- Bey, T. A. and Moecke, H. P. (2007) 'Electrical blackouts in hospitals and the need for reassessment of the electrical infrastructure and more powerful standby generation', *Prehospital and Disaster Medicine*, 22(S1), pp. S98–S98.
- Biringer, B., Vugrin, E. and Warren, D. (2013) *Critical infrastructure system security and resiliency*. CRC press.
- Bouchard, M. (2010) 'Network Security for 2010 and Beyond–The Impact of The Consumerization, Webification, Virtualization, and Consolidation of IT'. AimPoint Group.
- Disterer, G. and Kleiner, C. (2013) 'BYOD bring your own device', *Procedia Technology*, 9, pp. 43–

- Fulp, E. W. (2007) *Firewall Architectures for High-Speed Networks*. Wake Forest Univrsity.
- Garbis, J. and Chapman, J. W. (2021) 'Network Infrastructure', in *Zero Trust Security*. Springer, pp. 93–103.
- Gazizov, T. R. *et al.* (2016) 'New concept of critical infrastructure strengthening', in *AIP Conference Proceedings*. AIP Publishing LLC, p. 440007.
- Hansen, L. (1997) 'Network infrastructure security', *Network Security*, 1997(6), pp. 8–12.
- Hernández, L. *et al.* (2012) 'A study of the relationship between weather variables and electric power demand inside a smart grid/smart world framework', *Sensors*, 12(9), pp. 11571–11591.
- Hu, L. *et al.* (2019) 'Summary of research on IT network and industrial control network security assessment', in *2019 IEEE 3rd information technology, networking, electronic and automation control conference (ITNEC)*. IEEE, pp. 1203–1210.
- Hurst, W., Merabti, M. and Fergus, P. (2014) 'A survey of critical infrastructure security', in *International Conference on Critical Infrastructure Protection*. Springer, pp. 127–138.
- IBM (2021) *Why IT infrastructure is important*. Available at: <https://www.ibm.com/topics/infrastructure>.
- Jin, Y. *et al.* (2018) 'A secure container-based backup mechanism to survive destructive ransomware attacks', in *2018 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, pp. 1–6.
- Joshi, K. P., Elluri, L. and Nagar, A. (2020) 'An Integrated Knowledge Graph to Automate Cloud Data Compliance', *IEEE Access*, 8, pp. 148541–148555.
- Kaeo, M. (2004) *Designing network security*. Cisco Press.
- Kemp, R. (2018) 'Legal aspects of cloud security', *Computer Law & Security Review*, 34(4), pp. 928–932.
- Lawson, S. (2011) 'Beyond cyber-doom: Cyberattack Scenarios and the Evidence of History', *Mercatus Center at George Mason University*.
- Liu, Y. *et al.* (2015) 'Combination of cloud computing and internet of things (IOT) in medical monitoring systems', *International Journal of Hybrid Information Technology*, 8(12), pp. 367–376.

- Luftman, J. N., Lewis, P. R. and Oldach, S. H. (1993) 'Transforming the enterprise: The alignment of business and information technology strategies', *IBM systems journal*, 32(1), pp. 198–221.
- Manzuik, S., Pfeil, K. and Gold, A. (2006) *Network security assessment: from vulnerability to patch*. Elsevier.
- Mikhalevich, I. F. and Trapeznikov, V. A. (2019) 'Critical infrastructure security: Alignment of views', in *2019 Systems of Signals Generating and Processing in the Field of on Board Communications*. IEEE, pp. 1–5.
- Muthurajkumar, S. *et al.* (2015) 'Secured temporal log management techniques for cloud', *Procedia Computer Science*, 46, pp. 589–595.
- Pawar, M. V and Anuradha, J. (2015) 'Network security and types of attacks in network', *Procedia Computer Science*, 48, pp. 503–506.
- Roche, E. M. (1992) *Managing information technology in multinational corporations*. Barraclough Ltd.
- Ruo-xin, Z. *et al.* (2014) 'Model for cloud computing security assessment based on AHP and FCE', in *2014 9th International Conference on Computer Science & Education*. IEEE, pp. 197–204.
- Sabillon, R. *et al.* (2017) 'A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM)', in *2017 International Conference on Information Systems and Computer Science (INCISCOS)*. IEEE, pp. 253–259.
- Shaheen, M. Y. (2021a) 'Adoption of machine learning for medical diagnosis'.
- Shaheen, M. Y. (2021b) 'AI in Healthcare: medical and socio-economic benefits and challenges'.
- Shaheen, M. Y. (2021c) 'Applications of Artificial Intelligence (AI) in healthcare: A review'.
- Sharma, S., Gupta, G. and Laxmi, P. R. (2014) 'A survey on cloud security issues and techniques', *arXiv preprint arXiv:1403.5627*.
- Sterk, P. and Spruijt, R. (2013) 'Enterprise Mobility Management Smackdown'.
- Wang, L. *et al.* (2013) 'k-zero day safety: A network security metric for measuring the risk of unknown vulnerabilities', *IEEE Transactions on Dependable and Secure Computing*, 11(1), pp. 30–44.
- Wong, A. and Yeung, A. (2009) *Network infrastructure security*. Springer Science & Business Media.
- Yeluri, R. and Castro-Leon, E. (2014) *Building the Infrastructure for Cloud Security: A Solutions View*.

Springer Nature.

Yeung, K. H., Yan, F. and Leung, C. (2006) 'Improving network infrastructure security by partitioning networks running spanning tree protocol', in *International Conference on Internet Surveillance and Protection (ICISP'06)*. IEEE, p. 19.

Zwilling, M. *et al.* (2020) 'Cyber security awareness, knowledge and behavior: A comparative study', *Journal of Computer Information Systems*, pp. 1–16.