Network Security Framework, Techniques, and Design for Hybrid Cloud

Sandesh Achar

Director of Cloud Engineering, Workday Inc., Pleasanton, California, **USA**

*Corresponding Contact:
Email: sandeshachar26@gmail.com

ABSTRACT

Network security is a framework that deals with issuing procedures and policies that will be used to establish and maintain security protocols in a particular organization. The functions related to the network security framework are oriented toward insulating the specific organization from external cyber threats and adversaries. On the other hand, a hybrid cloud is a type of cloud whose function is to allow the running and operating of different applications in various and different environments. The primary technique associated with developing hybrid clouds is the conjunctions between private and public clouds that will allow application portability and management for better and more efficient working of the clouds.

Key words:
Cloud, Security Framework, Hybrid Cloud, Network Security

12/30/2021 **Source of Support:** None, **No Conflict of Interest:** Declared

INTRODUCTION

The Network Security Framework is a comprehensive approach to security orchestration. The mixed Network Security Framework empowers information technology departments to enforce a consistent security posture across the entire digital attack surface while ensuring control, monitoring, and protection for all systems (Diamantopoulou et al., 2019). Decentralized networks, hybrid cloud environments, IoT and mobile devices, and other linked gadgets are again under the jurisdiction of information technology staff.

The core, implantation tiers, and profiles comprise the framework's three key components in a cyber security environment. The three main components of the Cybersecurity Framework are the Core, Implementation Tiers, and Profiles. The Framework Core provides an easy-to-understand list of necessary cybersecurity actions and outcomes. In addition, the core supports existing risk management and cybersecurity practices by assisting firms in managing and reducing their cybersecurity risks (Abimbola et al., 2019).

Organizations benefit from implementing the Framework Tiers because they provide context for how an enterprise views cybersecurity risk management. The Tiers are commonly used as a communication tool to discuss mission relevance, risk appetite, and investment plans. In addition, they provide organizations with a framework for determining the level of rigor acceptable in relation to their cyber security program.

The Framework Profile is the specific fit between an organization's risk tolerance goals, resources, and organizational needs, with the outputs of the Framework Core. Profile's major goal is finding and ranking opportunities to improve cybersecurity within an organization. A hybrid system can be built or operates relatively simply (Achar, 2016). A few on premise infrastructures and virtual assets occasionally link. A networking system makes connectivity easier. Some APIs are also available that enable operators to program or carry out actions at the consumer, employee, and management ends.

The hybrid system that is used the most frequently combines public cloud assets with on-premise computing resources. As the number of users rises, the company can transfer workloads to the public cloud more quickly. Again, you can minimize the workloads on the public cloud by moving data to on-premises if the number of users declines. Hybrid systems, which integrate public and private clouds, are occasionally possible. Sensitive workloads can be run in the private cloud while managed by a workstation on-premises. In addition, public cloud customers will primarily use your apps or services.

A technology that can combine summed-up data that moves from on-premises to the cloud and back will be required. Robust version control should also be a feature of that system, allowing you to maintain many versions of the same data or merge them all. The second requirement is network connectivity. It enables the transfer of data between environments. For private or public cloud interfaces, professionals rely more on VPNs and intranet networks than on raw internet. Thirdly, various central control interfaces are required for all hybrid systems. Here, the functionality from other business data centers and apps on the cloud infrastructure is called via APIs from your business apps (Perera et al., 2014).

TYPES OF NETWORK SECURITY PROTECTION

Device Security on Mobile

Since most workers use their mobile devices for work, many hackers target them due to their popularity. As a result, corporate apps are growing increasingly popular because, when utilized properly, they may significantly increase productivity. But it's crucial to keep these gadgets under control. Controlling access to these devices is one thing, but it's also vital to conFig connections so that data is private (Rodrigues et al., 2018).

Intrusion Prevention System (IPS)

Another network security approach is an intrusion prevention system or IPS. This model works by proactively scanning the traffic in and out of a network to help prevent attacks. Specific rulesets can be put in place that can run at specific intervals on their own or manually, depending on the need (Manavalan & Ganapathy, 2014).

Security for Email

Cybercriminals frequently exploit organizational networks by fooling users into responding to malicious emails; businesses must strengthen email security to protect their networks. Therefore, it is essential to use email security software that can filter suspicious data while scanning emails for malicious viruses. In addition, administrators might utilize these tools to prevent data loss by regulating the outgoing flow of communications.

Data Loss Avoidance (DLP)

DLP technology reduces the likelihood of employees disclosing company information to other parties, ensuring that enterprises can maintain data and resource confidentiality. By blocking websites and ports that provide printing, downloading, and forwarding operations, such technology prevents or limits employee access to data.

Network Access with Zero Trust (ZTNA)

ZTNA evaluates a user's access and rights before allowing them to continue using the network, just like network access control does. However, ZTNA is more precise since it concentrates on letting users access the applications they require to carry out their responsibilities. It frequently requires the appropriate software to carry out in-depth access control or SDP with zero trust network.

A network's segments

The process of employing software to establish locations where network traffic can be divided into different categories is known as network segmentation. These categories use IP addresses and the endpoint's identification as a starting point. This type of segmentation keeps out users who try to log in using dubious devices while allowing authorized users to access the network according to their role, location, and other factors.

Firewall

The organization's internal network is separated from the external network, such as the internet, by a firewall. It uses a set of default rules that administrators can build up to permit or deny traffic. Next-generation firewall use is crucial for network security since it considerably lowers the application risk (Achmadi et al., 2018).

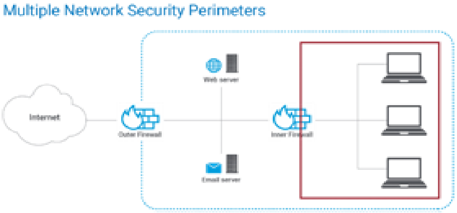


Figure 1: Firewall development

Network Access Management (NAC)

Thanks to NAC, you have control over which users can and cannot access parts of your network. However, before anyone may access the organization's network, network administrators typically implement password-protected accounts and authentication procedures. To verify users authorized to access the network, network access control checks to see if they meet the necessary requirements.

BASIC NETWORK SECURITY DESIGN PRINCIPLES

The vital orientation of a network security architecture, which also acts as the cornerstone of a firm's security architecture, covers the major areas of physical security, accountability, restrictions, and authentication access. Therefore, it is vital to take measurable steps in each area to protect network infrastructure from destruction, illegal access, and disclosure. Each of the network security core functions is built upon this.

Vulnerability analysis

Building the wall, checking for flaws, and structural reporting are the three primary stages of the DAM. To construct a strong defense at the architectural level, developing a model related to security in phase 1 that employs an IDPS and a firewall will be essential. To uncover weaknesses that put the network in danger, the monitoring activity will hire a new tool in phase 2 targeted at vulnerability analysis. Phase 3 entails creating a report, ranking the vulnerabilities, and applying the countermeasures suggested. Closing specific ports of the firewall that may be left viable, leading to improper configuration, is one of the most frequent actions that may be mentioned.

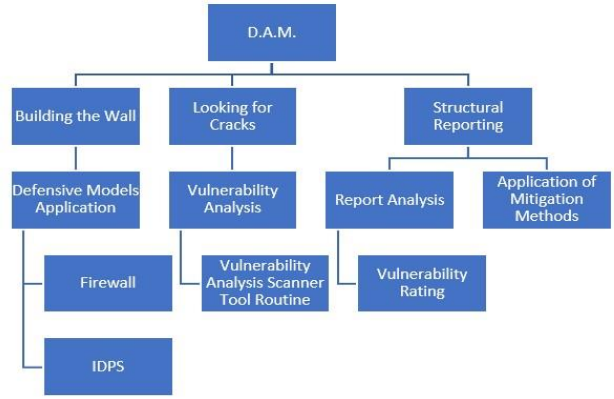


Figure 2: Vulnerability analysis

The following are the six core duties of network security:

Segmentation of Networks

Network segmentation, isolation, and compartmentalization are concepts to minimize an incident's impact on certain assets. Internal firewalls and internal rules regarding Access Control Lists VLAN and (ACLs) configurations are examples of traditional techniques for network segmentation. These techniques help lessen the harm cyberattacks cause to a specific area (Bruneliere et al., 2018). But not only are these implementations time- and money-consuming, but they also need to catch up in defending against threats.

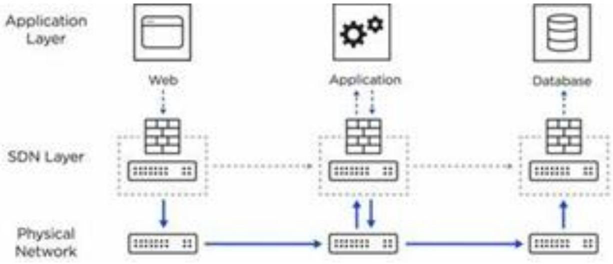


Figure 3: Segmentation of LAN network

Enforcement of Security Policy

Organizations can identify hostile conduct and persistent or unintentional policy violators by developing and enforcing security control regulations and policies. The complete task of implementing policy is divided into three sections:

- Making policy requirements based on crucial aspects and doing a design analysis of the system is part of the first step, including threat landscape, hardware, and software developments.
- To find violations is the second. It is simpler for network administrators to detect ambiguous activity, evaluate real-time incidents, and document such instances for use as evidence when the policy rules are clearly defined.
- The third step is to correct the infraction, which must follow local security policies, such as audit policies that outline the procedures for control and authentication.

Network Security Algorithm

A data encryption algorithm is a primary and most common avenue and method used in developing network security algorithms. This method incorporates the use of data conversion from one format to another. The raw data is usually transitioned from one data type, plaintext or readable, to encode generally unreadable information. This process is commonly known as ciphering. On the end receiver's side, the deciphering of the data occurs so that the raw data can be accessed and assessed at ease through a process known as decryption. The decryption function is done by a tool known as a decryption key, which is usually covert and secret so that it can be safe from unauthorized users that may tend to employ malicious activities.

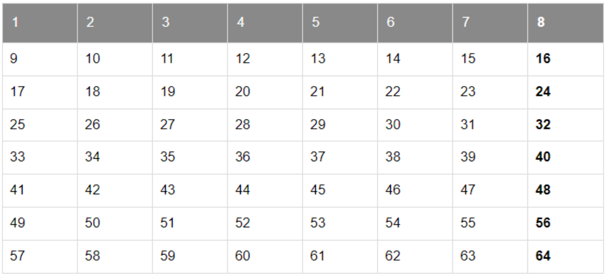
Data Encryption Standard (DES)

The Data Encryption Standard (DES) works as a symmetric block cipher. In their industry standard, the US previously used this and others to promote the encryption of sensitive data. When DES was abandoned in response to adversaries' more powerful brute-force capability, the Advanced Encryption Standard (AES) took its place.

Working Description of DES

The algorithm works under chunking, where the plaintext is taken and then divided into minute portions that usually have a 64-bit blockchain of data. The algorithm relates to the Lucifer cypher algorithm that constitutes transposition and substitution. The process involves the breaking down of data into smaller pieces of data. The main advantage of this is that it allows faster encryption and processing of data.

DES will employ using encrypted keys that will encrypt using 64-bit keys. The data will be encrypted into 64 bits of data. Eight of the 64 total bits are associated with error checking, thus giving them the name parity bits. After an error has been checked, the parity bits are then dropped.



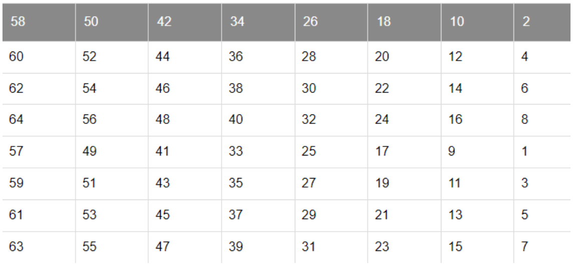
1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	**16**
17	18	19	20	21	22	23	**24**
25	26	27	28	29	30	31	**32**
33	34	35	36	37	38	39	**40**
41	42	43	44	45	46	47	**48**
49	50	51	52	53	54	55	**56**
57	58	59	60	61	62	63	**64**

Figure 4: bold font column shows the parity bits.

DES employs the use of permutations that constitutes initial permutation and final permutation that will deal with the rearranging of data

Initial Permutation

This specific permutation is usually done once and is the start of the encryption process. After the subdivision of the plaintext into smaller chunks and subdivisions into 64-bit blocks, initial permutation (IP) is carried out on them during the transposition process.



58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Figure 5: Initial Permutation example

A calculative and mathematical approach that can be deduced from the above figure is that the input of the 58th bit is the output of the first bit. In addition, the 50th-bit input corresponds to the 2nd-bit production, etc.

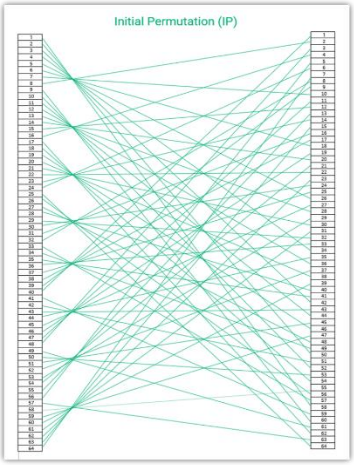


Figure 6: Input and Output placement of bits during initial permutation

The encryption relies on a function known as the Feisel function. The procedure operates by making rounds of encryption processes. These rounding operations are usually done several times. Before each round, the data is divided into the correct plain text and the left plain text, RPT and LPT, respectively.

The total 16 rounds of the Feisel function occur through the following:

- The IP's output is taken as the input for the process. If the process is substituted with x, it will occupy 64 bits.
- The LPT and RPT is the obtained by dividing x into two parts, each having 32 bits
- The original key then generates a subkey from k_1 to k_n, which is applied per round
- Using RPT, we obtain the result (f) of LPT and $K_2 – f(RPT, K_1)$

- An XOR function is performed on the results
- RPT is then swapped with L_1 so that the following function that will bring about L_2 will be done on RPT

Hybrid Cloud

A hybrid cloud is a type of cloud that integrates the combination of public clouds ad private clouds that compose a data center. This thus allows the sharing of data between the two public and private clouds and enables the sharing of applications.

Hybrid may be the ideal cloud choice for sectors that deal with compassionate data, like banking, finance, government, and healthcare. For instance, specific regulated sectors mandate the on-premises storage of types of data while permitting the cloud storage of less sensitive data. With this hybrid cloud architecture, businesses may still adhere to industry standards while gaining the flexibility of the public cloud for less regulated computing operations (Achar, 2018).

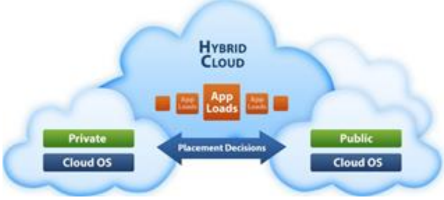


Figure 7: Working of a hybrid cloud

Many security features that organizations that employ hybrid cloud platforms can use currently include (SIEM) security information and event management capabilities. Due to characteristics like automated cybersecurity, disaster recovery, high availability, and data redundancy, some enterprises find that cloud hybrid security is preferable to their on-premises data center. However, networking between private and public clouds became possible thanks to the organized development of hybrid cloud theory and a few modern tools. As needed by the company operation, data can now travel effortlessly across on-premises, private, and public clouds.

The following contemporary tools play a significant role in this innovative cloud computing infrastructure:

- Virtualization of operating systems utilizing tools like Parallels, XenServer, VMware, VirtualBox, etc.
- You can access cloud assets from any location (VPNs) through virtual private networks.
- The container platforms needed to run containerized software include Podman, Containers, etc.

Advantages of the Hybrid Cloud Model

Businesses can move their front-end applications to the cloud using the hybrid cloud computing paradigm, then run other applications on virtual machines (Achar, 2020). Additionally, it enables you to preserve dated on-premises apps that you cannot shift to the cloud owing to legal or additional constraints.

Downtime is zero for upkeep.

When you improve your online apps or services, your customers only need to view a website or app that is still under construction. By copying its source code, you can upgrade existing software in a containerized environment. However, you need only publish the most recent app when ready.

IT workload reduction

LOB application owners and Developers can manage more queries via self-service thanks to hybrid cloud models. As a result, the repetitious chores associated with VMs or containers for IT workers are reduced.

Changes in Business that Are Flexible

You can quickly change company goals with hybrid systems. For example, you can boost a new workload whenever you alter the product or services while decreasing legacy workloads or moving them to on premise.

Limit ambiguity

The same OS is typically deployed across environments by hybrid systems, so the IT team can quickly upgrade, maintain, and troubleshoot the techniques. Additionally, a consistent, identical OS improves the compatibility of security protocols among various cloud assets.

Scalability on Demand

Many firms today start small and scale up as their operations expand. As a result, IT managers may expand storage capacity and performance following their changing needs thanks to the hybrid architecture.

Scalability on Demand

Many firms today start small and scale up as their operations expand. As a result, IT managers may expand storage capacity and performance following their changing needs thanks to the hybrid architecture.

How a Hybrid Cloud Is Built

Community, public and private clouds, and actual computer servers are all combined as part of the hybrid cloud computing strategy. When used together, these resources give total processing, storage, and memory power.

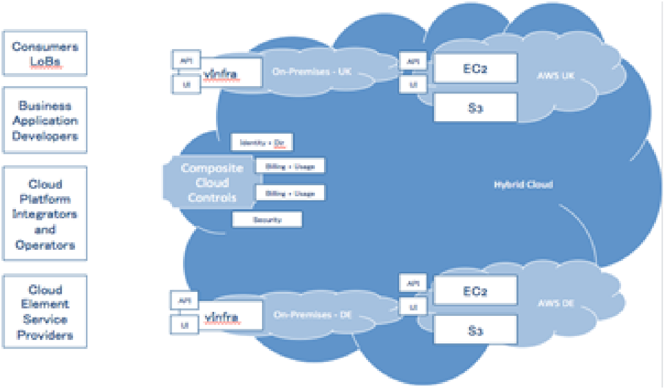


Figure 8: Deployment of a hybrid cloud

Although the architecture may change depending on the final application, typical combinations include the following:

- At least two public cloud platforms.
- Various assets for private clouds or virtual private clouds.
- Public and private clouds are synchronized with the physical server.
- Public cloud server or on-premises bare metal server linked to a public cloud

STRUCTURE DEVELOPMENT WORKING AND DESCRIPTION

They are different combinations of different hybrid cloud models. Consider the following elements that make up the overall hybrid structure:

Networking: Public, private, and on premise assets are connected through a secure network. When data and workloads move between local infrastructure and the cloud, VPNs are required to secure several tiers of data communication.

Complete Integration of Data and Workload: Workload and data version control are additional requirements of the hybrid paradigm. It accomplishes this by combining on-site, private, and public data.

Central Administration: Most of the time, a hybrid system's environments share the same operating system. Experts prefer Linux because it has the top security measures. Multiple operating systems in the hybrid system are subordinate to a centralized management tool with authority to modify their features.

Instant Resource Provisioning: The hybrid system uses a public cloud to easily access internet resources like email accounts, subscriptions, customer accounts, user profiles, etc.

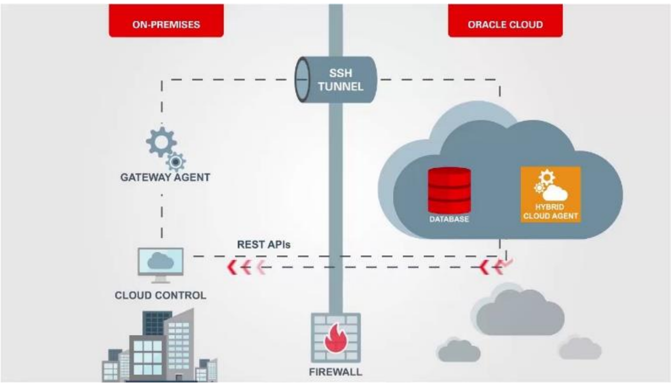


Figure 9: Hybrid cloud integration with other systems

HYBRID CLOUD SECURITY

The security of this computing platform is composed of separate assets such as on premise, a public cloud, and private cloud architecture. In addition, the business owner oversees safeguarding both on-site and cloud-based assets. In addition, they can handle workloads and data better, albeit.

However, the buyer and vendor of public cloud services work together to safeguard the cloud asset jointly. Typically, the customer installs software such as antivirus and security components on their cloud-based virtual computing asset. At the same time, the service provider's infrastructure is safeguarded, such as data centers.

USE CASES OF HYBRID CLOUDS

The Development of Applications

When a new application is launched, there is a lot of uncertainty about the workload. Even while these development organizations must assume some risk, utilizing a hybrid strategy helps to reduce it to some level. For example, they can forego the hefty upfront outlay. Companies can avoid paying a large upfront sum of money by implementing the new app in a hybrid model and just paying for the resources they use. However, they will only incur a significant loss if the development process is stopped in the midst (Paasivaara et al., 2014).

Regulatory Conformity

Industries that must secure sensitive data frequently choose a hybrid approach. Businesses operating in Since the EU passed the General Data Protection Regulation, data has started to be stored by those countries using a hybrid model (GDPR). It enables organizations to follow GDPR in the European Union while also following other laws overseas. Because not all data needs to be stored in a secure environment, hybrid cloud computing has become popular among these businesses. Therefore, the public cloud can be utilized by companies for everything else, and the private cloud to comply with rules.

High-Variability Workloads

Companies frequently need help because of the necessity for environmental scalability. For instance, an application may function successfully in the existing environment today but require more computational power tomorrow. Businesses may adapt to their dynamic workload requirements with shifting workload requirements while maintaining services by using hybrid cloud solutions. It functions like overdraft protection for your checking accounts to stop an unanticipated event.

Electronic Transformation

Several firms wish to upgrade their IT infrastructure by switching to a public cloud architecture. As a result, companies need to be able to shut down private data centers due to outdated applications or compliance requirements.

Emergency Recovery

Using a hybrid cloud strategy, businesses can duplicate their workloads on their on-premises and store the data on the cloud for backup purposes (Usak et al., 2020). As a result, cloud resources are used as needed to handle the demands in the case of an outage of a data center. Organizations should use caution throughout the installation to avoid issues like heavy bandwidth usage and challenging data management.

Processing Data in the Cloud

In businesses that process data, hybrid cloud computing is also used often. This infrastructure can be used as an alternative to public cloud services when doing query analysis on data stored locally (Bhuyan et al., 2017).

Hybrid Cloud Essentiality

Businesses frequently gain from using the hybrid approach over alternative solutions because it can match business needs with IT goals. It provides the most significant degree of flexibility of all the options, which is an essential quality for businesses that must comply with regulatory compliance or need to embrace digital transformation.

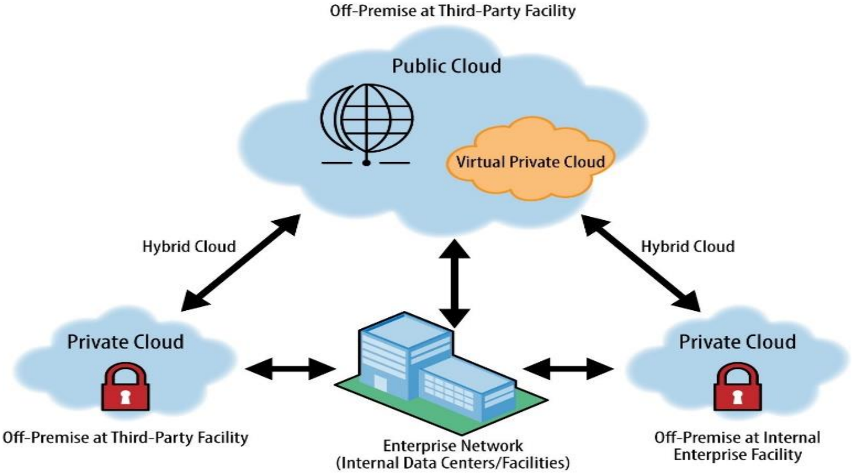


Figure 1: Incorporation of a hybrid cloud in a business

A hybrid cloud architecture is ideal for businesses that need to process large amounts of data quickly and have changing workloads (Adeniyi et al., 2021). Additionally, your business might pick the hybrid model if it wants to combine the capability of a public cloud with increased data protection or if it intends to use platform-as-a-service (PaaS) while using a private cloud architecture.

Conclusion

Organizations are just more productive with a hybrid cloud. You can use various solutions like current on premise infrastructure, a private cloud, and a public cloud for combined performance, security, and speed of data-based activities. One must use a straightforward strategy like the one listed below to handle data-related enterprises. Send duties, including internet apps, subscriptions, and marketing to a public cloud. Utilize a private cloud to host intranet websites, handle billing and customer service, and process sensitive data. Additionally, retain internal communication, ERP, inventories, business plans, and custom software on-site.

References

Abimbola, S., Keelan, S., Everett, M., Casburn, K., Mitchell, M., Burchfield, K., & Martiniuk, A. (2019). The medium, the message, and the measure: A theory-driven review on the value of telehealth as a patient-facing digital health innovation. *Health Economics Review*, *9*(1).

Achar, S. (2016). Software as a Service (SaaS) as Cloud Computing: Security and Risk vs. Technological Complexity. *Engineering International*, 4(2), 79-88. https://doi.org/10.18034/ei.v4i2.633

Achar, S. (2018). Security of Accounting Data in Cloud Computing: A Conceptual Review. Asian Accounting and Auditing Advancement, 9(1), 60–72. https://4ajournal.com/article/view/70

Achar, S. (2020). Cloud and HPC Headway for Next-Generation Management of Projects and Technologies. *Asian Business Review*, *10*(3), 187-192. https://doi.org/10.18034/abr.v10i3.637

Achar, S., & Tisuela, N. L. (2020). A Review of Hosting Enterprise SaaS with IaC on Multi-cloud Platforms. *International Journal of Reciprocal Symmetry and Physical Sciences*, *7*, 14–23. Retrieved from https://upright.pub/index.php/ijrsps/article/view/72

Achmadi, D., Suryanto, Y., Ramli, K. (2018). On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center. *2018 International Workshop on Big Data and Information Security (IWBIS)*, 149-157, https://doi.org/10.1109/IWBIS.2018.8471700

Adeniyi, E. A., Ogundokun, R. O., Awotunde, J. B. (2021). IoMT-Based Wearable Body Sensors Network Healthcare Monitoring System. In: IoT in Healthcare and Ambient Assisted Living. *Studies in Computational Intelligence*, vol 933. 103-121. https://doi.org/10.1007/978-981-15-9897-5_6

Bhuyan, M. H., Bhattacharyya, D. K., Kalita, J. K. (2017). Alert Management and Anomaly Prevention Techniques. In: Network Traffic Anomaly Detection and Prevention. *Computer Communications and Networks*. https://doi.org/10.1007/978-3-319-65188-0_5

Bruneliere, H., Al-Shara, Z., Alvares, F., Lejeune, J. and Ledoux, T. (2018). A Model-based Architecture for Autonomic and Heterogeneous Cloud Systems. In *Proceedings of the 8th International Conference on Cloud Computing and Services Science - CLOSER*, 201-212. https://dx.doi.org/10.5220/0006773002010212

Diamantopoulou, V., Tsohou, A., Karyda, M. (2019). General Data Protection Regulation and ISO/IEC 27001:2013: Synergies of Activities towards Organisations' Compliance. *Trust, Privacy and Security in Digital Business*. Lecture Notes in Computer Science, vol 11711. Springer. https://doi.org/10.1007/978-3-030-27813-7_7

Manavalan, M., & Ganapathy, A. (2014). Reinforcement Learning in Robotics. *Engineering International*, *2*(2), 113-124. https://doi.org/10.18034/ei.v2i2.572

Paasivaara, M., Behm, B., Lassenius, C. and Hallikainen, M. (2014). Towards Rapid Releases in Large-Scale XaaS Development at Ericsson: A Case Study. 2014 IEEE 9th International Conference on Global Software Engineering, 16-25. https://doi.org/10.1109/ICGSE.2014.22

Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Sensing as a service model for smart cities supported by internet of things. *Transactions on emerging telecommunications technologies*, *25*(1), 81-93. https://arxiv.org/abs/1307.8198

Rodrigues, J. J. P. C. et al. (2018). Enabling Technologies for the Internet of Health Things. *IEEE Access*, *6*, 13129-13141. https://doi.org/10.1109/ACCESS.2017.2789329

Usak, M., Kubiatko, M., Shabbir, M. S., Viktorovna Dudnik, O., Jermsittiparsert, K., Rajabion, L. (2020). Health care service delivery based on the Internet of things: A systematic and comprehensive study. *Int J Commun Syst.*, *33*(2). https://doi.org/10.1002/dac.4179

--0--