Well Designed Data Centers

Paul Farri

Liberty University

System Administration, CSIS-352 B02

February 21, 2023

Table of Contents

**Introduction2**

Required Features and Efficiencies3

Preserving Data Integrity via Smart Data Center Design5

**Important Hardware, Software, and Data Aspects7**

Conclusions8

References10

**Introduction**

Data is one of the core aspects of everyday life that humans encounter in a variety of environments, and with that significance also includes the important responsibility of keeping that data stored and protected from threats abroad. This is where data centers are established to fulfill that role. Data centers are one or multiple buildings in which dedicated computer systems and their associated equipment are localized at. They provide services such as such as data storage, backup and recovery, productivity applications, high volume e-commerce transactions, powering online communities, artificial intelligence, and machine learning for a large variety of businesses, enterprises, and companies that cooperate for their services. Data centers are used by millions of businesses and many governments across the world, in which they can either build their own from the ground up or borrow the services of an existing data center. Data centers must be as secured and protected as the data it holds, and this can be achieved with an efficient design. Designing data centers from the ground up with the idea of security in mind provides the facility with a strong foundation for security. The architectural design of data centers can greatly impact the overall performance of the facilities (Wu et al, 2012). This security can then be built upon further as installations are made inside the facility. With this protective layering, stored assets inside data centers shall enjoy far more protection and contribute to warding off attacks and cyber threats.

**Required Features and Efficiencies**

Data centers require certain features and efficiencies that are vital in order to keep themselves functioning to necessary capacities and maintain fast performance for the services that they provide to companies and businesses. Three major traits that data centers should maintain a clear and consistent focus on are scalability, flexibility, and high availability (Arregoces & Portolani, 2003). Other factors to take into consideration are energy consumption, cost, heating, technology usage, and capacity. Data centers must be able to perform their operations quickly in short-term scenarios and have the structure to grow seamlessly sustain a consistent and rapid growth rate for its clients, as well as being able to dynamically adopt new services without conducting major changes or overhauls to its infrastructure. Successful scalability also means that data centers, especially data centers using network architecture, must be able to quickly make way for new additions such as more ports for servers, firewalls, switches, routers, IDSs, and SSL off-loaders to the facility without interruption of operations so that it can carry out bigger tasks. They must also be capable of performing day and night for seven days per week as much as they can. Companies and businesses require consistent support each day and sometimes even require increased support depending on the circumstances. This means that if the data center is temporarily out of commission and cannot perform the duties it sets out to perform, then the clients that benefit from its services will suffer risk and potential losses from it, such as network outages, hard drive failures, and data endangerment.

Data center network architecture is considered to be one of the more important factors that determine network performance (Wang et al, 2015). Network architecture with high level fault tolerance, large capacity, reduced latency, low cost, and low energy consumption not only make data centers waste less resources, but also grant it the fast performance it needs to complete operations with little to no delay. Even a little bit of delay or latency can cause services to be interrupted, and that will create greater problems for both the client and the data center providing the services. Delays and waste of electricity can even be caused by performance gaps inside the data centers themselves. CPUs for data centers have advanced extensively over the years, but because their growth has overtaken other technologies in computing, these fast CPUs are unable to perform at an optimal level due to them being forced to wait for other technologies present to complete their operations. As the CPUs wait, more and more power inside the data center is being consumed as a result of them always running ahead of their partnered equipment. This increase in power usage causes costs to spike, and this causes data centers to take a financial hit. Attempting to fix the problem by adding more servers to divert CPU power merely increases power output and makes cost increase even further (Glowka, 2013). Power costs for data centers are already their dominant financial burden, and heating from increased power usage makes it worse. Heat generated from server operations also cause costs to increase because it results in excessive usage the data center’s cooling systems. Inefficient technology means increased slower performance and increased heat output, and increased heat output means increased costs for the data center as a whole (Glowka, 2013).

The solution to this problem can be solved by using the correctly-sized equipment needed for the job, enhancing the air distribution on the floor layout and aisle designs, making sure server racks are placed in the best locations for optimal cooling potential. A Bell Business Markets data center in Ottawa back in 2013 overcame its heating issues by renovating the design of the facility. This included lessening the use of copper through single-step electricity transformations, decreasing the consumption of water through air cooling with an A/C backup included, lowering power consumption costs by maximizing free cooling instead of mixed cooling, retaining and redistributing heating generated by the servers inside the facility, and decreasing the usage of lead via flywheel technology instead of relying on batteries. All these options combined together can make data centers open to more cost-effective solutions and conserve resources while keeping their systems fast in performance and operations running smoothly.

**Preserving Data Integrity via Smart Data Center Design**

Data integrity can be preserved better simply by utilizing smart data center design. It is an factor of data centers that might seem unnecessary at first but will potentially make a major difference for companies in the long term. The overall design of a data center may depend on what the center’s purpose is, and as a result of advancing technology and design approaches, the design may change over time even once the main infrastructure of the facility is finished being built. As mentioned before, a Bell Business Markets data center in Ottawa back in 2013 changed its designs to adopt a new smart approach so that it can perform better and avoid wasting resources (Glowka, 2013). Data integrity can also be a benefit from data centers adopting new and innovative design formats, even once the actual facility has been fully constructed. One method that data integrity can be achieved in data centers through smart design is with cloud computing. With cloud storage, data can be stored to a remote location in which there will be less data stored on the client’s end but still allowing them to have just as much access to their data. The cloud serves as a solution in providing successful ways to keep data protected and unmodified for long periods of time. It also provides greater economic benefits to data centers and uses up far less resources. This encourages data centers to utilize a cloud computing design approach and for their partnered companies and businesses to embrace cloud-based services (Kumar et al, 2011).

Cloud storage services must be both fast and reliable in keeping up with its users and keeping all that it stores completely protected from outside interference. The cloud storage service must also be able handle very large quantities of data coming in from multiple clients at one time, as well as demonstrate the ability to detect incoming threats and alert the service provider that a hostile entity has infiltrated the system. Letting the owner of the data to be able to quickly access the cloud server itself and examine their data that is stored directly allows them to see if their data has been modified in any way, shape, or form. However, it would also be an even better solution for both parties if the cloud storage service produces a form of data integrity proof without the client being required to access their entire file or sets of files on the storage. It is also important that access to the cloud storage can be conducted on a wide variety of platforms and devices. Sometimes a client or individual user may have a low-powered device such as a personal digital assistant or a small mobile phone that does not have large amounts of CPU processing power or bandwidth connection, and attempting to access large sized files on devices with low capabilities can cause heavy usage of bandwidth. This makes the development of light-weight and widely available cloud storage services very important for clients. Many storage services, including certain cloud-based storage services, encrypt the data that is stored inside the system and provide an encryption key generated for future access so that all data inside remains completely protected from anybody trying to access it that is not the owner of the data (Kumar et al, 2011)

**Important Hardware, Software, and Data Aspects**

Data centers work around the clock day and night while expanding in scale, and this job is best performed by using powerful components and secured, performance-friendly software. Maintaining a pursuit in the usage and maintenance of balanced hardware, efficient software, and data stored in storage that maintains consistent daily protection from modifications is very important as a whole for data centers and can mean the difference between success and failure. If a technical component is far too advanced compared to the partnered equipment being used inside a data center, then operations will be slowed down since the other equipment cannot keep up. The servers must be accommodated with a design that allows for maximum cooling potential so that excessive heating inside the data center does not use up additional wattage and increase unnecessary costs. Data center software must be secure, reliable, and trusted in being able to meet the needs and security concerns of the facility. If the software used by the data center is unreliable or lacks any form of security, then the facility will be left completely open to security breaches from the inside. Client data stored inside the systems must also be under complete encryption while at the same time providing total accessibility to the clients who own the data. This maintains both security and trust between the data center and the business or company it partners with for the flow of services.

The hardware, software, and data of a data center must be “synchronized” or balanced together in which they all work with each other in full compatibility without hinderance or delay. This can be influenced based on the way they are set up, the way they are used by the facility, and the way they are maintained inside the facility by its employees. The hardware cannot be too advanced over its partnered equipment or generate heat from excessive power usage, and it cannot be too underperforming. The software cannot be too complex, and it cannot so simple or small in scale to the point where it is no longer reliable. And the data stored cannot be locked behind one big digital door, but at the same time it cannot be so exposed or accessible to the point where anybody can go inside and modify it. If these three important components work consistently with each other to fulfill the data center’s operations, then the speed, efficiency, and smoothness in services to the clients and partners will work dynamically and allow for maximum potential even in quickly-changing environments or scenarios where new architecture has to be installed alongside existing systems. It will also indirectly aid in cushioning the data center from losses if an issue were to arise.

**Conclusion**

Building successful smart data center designs as well as maintaining the sufficient operations of data centers are some of the more important ways of keeping vital data and internal system operations protected from all sorts of threats and cyber-attacks from malicious organizations and individuals, or even just providing a cushion against natural inconveniences like excessive heating, waste of resources, or socially engineered problems from untrained employees. They also are necessary to maintain and constantly improve upon due to their importance to other companies that they provide services for, as data centers such as Microsoft Azure and Amazon’s EC2 platform are the primary backbone for things such as e-commerce, social networking, web-hosting (Kant, 2009). This objective will also help keep employees alert at all times of threats and remind them of the importance of utilizing innovative data center designs to stay ahead of threats that will typically come without warning. Sometimes security software and employee training are not enough to keep important data, servers, network operations, and data storage systems protected. The design of data centers themselves can play a major role in providing a good fight against these threats. It is not simply just the employees or the company that are at risk of being affected by such problems, but the people and companies that they provide their services for are also at major risk. If there is no efficient shielding carried out through things such as creating a protective and efficient data center design, then the risk for the companies increases, and such risk will very likely lead to their personal data being in danger of being stolen or damaged, and their services from the data centers being slowed down or even halted altogether. Regardless of how small a threat or problem may be, it is always better to prepare ahead of time than to take the dangerous risk and assume they will not be affected. Once a problem has entered the system or facility, the damage will already be inflicted whether its big or small. The primary goal for data centers must be to keep themselves ahead in the strategy of defense and act before the damage is done.

**References**

Arregoces, M., & Portolani, M. (2003). *Data center fundamentals*. Cisco Press.

Glowka, J. (2013). TIM lecture series – energy efficiency and data security in modern data centres.*Technology Innovation Management Review, 3*(2), 41-44. <https://doi.org/10.22215/timreview659>

Kant, K. (2009). Data center evolution: A tutorial on state of the art, issues, and challenges. *Computer Networks*, *53*(17), 2939-2965.

Kumar, R. S., & Saxena, A. (2011, January). Data integrity proofs in cloud storage. In *2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011)* (pp. 1-4). IEEE.

Wang, T., Su, Z., Xia, Y., Muppala, J., & Hamdi, M. (2015). Designing efficient high performance server-centric data center network architecture. *Computer Networks*, *79*, 283-296.

Wu, K., Xiao, J., & Ni, L. M. (2012). Rethinking the architecture design of data center networks. *Frontiers of Computer Science*, *6*, 596-603.