Navigating the Legal and ethical issues faced by companies in implementing an IT infrastructure

Surendar venkatachalam(A20525010)
ITMS 585, Legal and ethical issues in Information Technology
svenkatachalam@hawk.iit.edu

Abstract : The establishment of a strong IT infrastructure is crucial as businesses continue to rely more and more on information technology (IT) to run their operations. Companies must negotiate some legal and ethical problems that come with this deployment, though. Companies must take into account their social and ethical obligations as well as legal and ethical problems like privacy, security, and data protection legislation. Implementing IT infrastructure runs the risk of causing data breaches, legal action, and reputational damage. Therefore, before putting in place an IT infrastructure, it is crucial for businesses to properly evaluate and negotiate these legal and ethical challenges. The many legal and moral dilemmas that businesses have when putting in place an IT infrastructure are examined in this article along with advice on how to handle them. Although there are many different types of firms in the commercial and enterprise sectors, each with its own unique business model and product offerings, if we take a deeper look, we can find that they all have one thing in common: an IT infrastructure. Businesses are built on this unnoticeable architecture, which also enables them to provide their services. In the modern day, centralized, decentralized, and distributed systems have solidified their positions as the main frameworks that support every enterprise firm and application.

Keywords : centralized infrastructure, decentralized infrastructure, distributed infrastructure, cybersecurity, cyber threats

1. Introduction

1.1 Centralized infrastructure

A computing system with centralized IT infrastructure enables remote access to all resources, including hardware, software, and data, which are all stored in a single location or data center. Consolidating IT resources such as servers, storage devices, and networking equipment to establish a consolidated platform for controlling and

delivering IT services is the goal of this method. This enables more effective resource management and control, improved security, and simpler scaling.

This is a more conventional strategy that works best for organizations that need more network control and use a vertical coordinating style. One advantage of this technique is that it gives a more uniform procedure, resulting in consistent outputs, less training and resource consumption, and much easier and faster reporting. In a centralized architecture, decision-making and change management are simple, with seamless, continual improvements in short feedback loops. Internet service providers, File systems, Organizational networks, and Application Development Servers are some of the well-known implementations of centralized infrastructure.

The centralized model was one of the earliest types of systems to emerge and is widely utilized today, especially on the Internet. This form of network has a fundamental issue with its reliance on a central server, which serves as a single point of failure and a prime target for adversaries. The management and decision-making authority in a centralized management infrastructure is concentrated at the top of the organizational hierarchy for the goal of synchronizing financial, human, and other company resources.

1.2 Decentralized infrastructure

A technique for setting up and administering digital infrastructure networks that doesn't rely on a single centralized model or service provider is known as decentralized infrastructure. Each department has autonomy in a decentralized infrastructure. Instead of using a single centralized server, a decentralized architecture makes use of several servers. These servers can each function as a separate master server, with the required workloads being split among them for load balancing. Decentralization is a viable option when various departments in a company have varied IT expectations and ambitions. It lets each business unit run its server and choose hardware and software based on its individual needs. The decision-making authority is split among each node. The system's final behavior is the sum of the decisions of the various nodes. This system has the advantage of having no single point of failure; each department has its internal infrastructure for handling, analyzing, and managing data. They are no longer reliant on a single central server to handle all of their administrative needs. They can solve cost, risk, and scalability issues associated with traditional centralized networks while also eliminating barriers to access and participation. Because they circumvent many of the drawbacks of a centralized network, decentralized networks are by far the most prevalent kind.

1.3 Distributed infrastructure

All network services and coordinating responsibilities are dispersed equitably over the whole company network in a distributed

network. A dispersed network does not have a centralized server or a cluster of domain controllers. Nodes spread geographically and logically throughout the company network and share all data processing, computing resources, and network management tasks. Some dispersed networks go even further by crowdsourcing computing power from client computers, using the fact that many of these devices are overpowered and unused. A major firm with thousands of people and systems geographically dispersed among branch offices and data centers is an example of a distributed network.

A distributed system, like a decentralized one, does not have a single central owner. However, it goes a step further and eliminates centralization. Users have equal access to data in a distributed system, although user rights can be enabled as necessary. The internet is the greatest illustration of a large, dispersed system. The distributed system allows users to share data ownership. Hardware and software resources are also shared across users, which can increase system performance in some instances. A distributed system is immune to component failure, which can significantly increase its uptime.

2. Centralized infrastructure

2.1 Definitions and characteristics

Client/server architecture systems with one or more client nodes directly connected to a central server are known as centralized systems.In this type of system, a client submits a request to a corporate server and receives an answer, it is most typical in many firms. Less powerful nodes linked to the central server can forward process requests to the server machine instead of processing them directly. A single server that conducts all important administration and data processing is the center of a centralized network. This approach allows for better control and coordination of IT resources, as well as improved security and cost savings (Ghosh & Chakraborty, 2018). Other servers can connect to this master server and administer certain functions, but they cannot function independently of it. Client systems and users must first go via the centralized master server in order to access resources or services on several servers directly. The entire network collapses if the main server crashes.

Another meaning of centralization is an organizational system in which only a few people have decision-making authority. Unexpectedly, centralization affects us more than you might imagine. You use a centralized system when you use social media platforms like Facebook. YouTube and other prominent internet sites are likewise centralized. The entire system will depend on a single centralized clock so it is easy to monitor and update.

2.2 Advantage of using centralized infrastructure

- **Simplified management** : A single central server may be set up quickly and easily since there

is only one configuration to handle—neither load balancing nor orchestration are necessary. They are excellent for small commercial applications, centralized databases, or testing environments because of their simple architecture and well defined responsibilities in the system, which considerably reduces the time required for decentralized systems to be deployed.

- **Improved efficiency** : Centralized infrastructure enables organizations to manage IT resources more efficiently by using standardized hardware, software, and processes. With this strategy, economies of scale are enabled, which eliminates the demand for duplicate resources and boosts efficiency.

- **Low setup cost** : Centralized networks are very affordable since all servers and networking equipment are housed in a single location. Extra or duplicate equipment is required when deployed across many sites. Increasing redundancy, in a nutshell, raises expenses. It is simpler to negotiate software licensing and support contract costs for a complete firm rather than individual divisions. Better contract conditions and even complementary integration or support services may come as a result of this.

- **Enhanced Security** : A centralized structure improves IT staff supervision and simplifies mundane chores. Software installs, upgrades, and security patches, for example, may all be accomplished from a single site. Centralized infrastructure provides enhanced security through better control and monitoring of security measures (Ghosh & Chakraborty, 2018). It is simpler to monitor and update security measures like firewalls, intrusion detection systems, and antivirus software due to the centralized location.

- **Data consistency** : Centralized IT systems aid in the prevention of data silos. Data and information may be shared swiftly between departments, leading in better knowledge sharing and collaboration. Using a centralized cloud-based CRM system, for example, will allow all staff to access client information from any location.

- **Simplified management** : Centralized infrastructure simplifies IT management by consolidating IT resources and operations into a single location or data center. This approach eliminates the need for multiple IT staff at different locations, reducing complexity and

increasing efficiency.The top-down nature of centralized systems makes it simple to standardize the interaction between the server and the client nodes, allowing businesses to give a more uniform and simplified experience to end customers. Furthermore, because the system has clearly defined responsibilities, it is very straightforward to track and gather data, making the identification of deviant user behavior more efficient.

These benefits make it desirable to many enterprises, particularly those with limited IT resources and a need for increased efficiency and security.

2.3 Disadvantage of using centralized infrastructure

- **Single point of failure** : A single master server presents a single point of failure on the network, such as a power outage or network failure, can put the entire system to a halt. Client nodes will be unable to send, receive, or process user requests as a result. Furthermore, maintenance and upgrade operations will almost certainly require a period of outage during which users will be unable to utilize the company's services.

- **More vulnerable** : All of your important and sensitive data is kept and accessed from a single server in a centralized network, posing a security risk. If hackers gain access to your one DC, they can access everything from that single location rather than having to bounce between numerous systems and servers to obtain what they need. Another source of concern is that data is only stored on the central server, which increases privacy threats and the possibility of data loss if the server becomes corrupted.

- **Scalability** : A system's computational power can't be upgraded after a certain limit and that is the main limitation of centralized infrastructure. Only vertical scaling is possible with centralized systems, which means that the central server can be upgraded with greater hardware components. The difficulty is that the performance of the hardware components on the market is sometimes insufficient for technological enterprises that require a huge pool of processing power to handle their task.

- **Reduced responsiveness** : When your network traffic exceeds the capabilities of a single node, a central server can create bottlenecks. Outside of small

enterprises and specialized LANs, proper centralized network administration is rarely employed since it simply cannot handle the volume of network traffic and computer power required in an enterprise context. Certain users can encounter higher delay and be unable to access information or services if the system's capacity is exceeded.

Overall, centralized infrastructure can be an efficient approach for firms trying to improve IT efficiency, control, and security. Before implementing this strategy, the organization's objectives and resources must be thoroughly examined because it may not be the best fit for many businesses.

3. Decentralized infrastructure

3.1 Definitions and characteristics

Instead than relying on a centralized authority or server, decentralized infrastructure is a sort of information technology (IT) architecture that distributes resources across a network of autonomous nodes. Lack of single points of failure, higher scalability and resilience, and better user control over data and resources are the characteristics of this kind of architecture. According to Buterin and Griffith (2017), A more secure and democratic replacement for conventional centralized systems, decentralized infrastructure is based on the tenets of transparency, immutability, and consensus.

In the event that one server fails, another can step in to maintain the network operational. Instead of being distributed automatically or equally, decentralized infrastructure management distributes network loads among a cluster of master servers based on network administrator parameters. The number of master servers that manage and coordinate your network's services and operations is the primary contrast between centralized and decentralized networks. A centralized network is based on a single central server or domain controller, which simplifies network administration but imposes significant limits. A decentralized network is managed by a collection of domain controllers who distribute network traffic and provide redundancy in the case of server failure.
It is critical to note that decentralized networks do not distribute data storage and computation uniformly across the network, which is why master and slave nodes exist. Nonetheless, they outlast their centralized counterparts.

3.2 Advantages of using decentralized infrastructure

- **More secure** : Because they have more possible points of failure and can survive cyberattacks better, decentralized networks are more reliable than centralized ones. IT network resilience

improves with decentralization.Each department has its own server, so if a network or system failure occurs, one server can function as a backup server for another.

- **Scalability** : Because it allows you to add more computers to the cluster as your organization expands, decentralized network management scales more successfully. A decentralized network has fewer bottlenecks since it may disperse traffic among multiple servers, which can be located in data centers and branch offices.

- **Management** : Decentralized infrastructure provides greater autonomy for individual business units or locations to manage their IT resources. This method allows for more rapid decision-making and better flexibility in responding to local business needs.When individual departments have the authority to make IT decisions, they can select and configure IT resources to meet their specific needs. Because judgments are made rapidly, there is no need for a lengthy approval chain.

- **Increased Innovation** : Responding to evolving IT trends faster. Departments in decentralized organizations can employ new technologies more easily since they can make distinct decisions. Assume your customer service department wishes to improve services by implementing online live chat. In a decentralized arrangement, it can do it autonomously. Purchasing would be complicated in a centralized arrangement, beginning with receiving approval from the IT department. Slowly responding to emerging technical breakthroughs may place you at a competitive disadvantage.

- **Lower costs** : Decentralized infrastructure can be less expensive to implement and maintain than centralized infrastructure. Organizations, especially those with constrained IT budgets, may experience cost reductions as a result of this strategy.

3.3 Disadvantage of using decentralized infrastructure

- **Increased cost of maintenance** : Decentralized

network implementation necessitates the installation and configuration of numerous servers with load balancing and failover capabilities, which increases cost and deployment time. Furthermore, they are more intricate and require more technological support, making them more labor and money costly to maintain. They are not ideal for smaller systems due to their low cost/benefit ratio.

- **Difficulty in management** : In decentralized networks, several servers must coordinate and copy data, and any errors or pauses in this process may result in security issues and service failures. Multiple master nodes run separately and may or may not communicate with one another in a decentralized system. This design decision may limit decentralized systems' adaptability by making it difficult to arrange nodes to work on a collective effort.

- **Lack of centralized cyber policies** : Despite the fact that a decentralized network is more secure than a centralized network due to multiple points of failure, replication across master servers assures that hackers can still access the majority or all of your network from a single location.

- **Fragmented decision-making** : Decentralized infrastructure can result in fragmented decision-making across different business units or locations, making it more challenging to implement consistent policies and standards across the organization (Ghosh & Chakraborty, 2018). As a result, IT management processes may become inefficient and inconsistent.

4. Distributed infrastructure

4.1 Definition and characteristics

The need to address more complicated computer issues that a single machine could not manage gave rise to distributed systems. Distributed systems have emerged as a result of the constraints of existing systems. With increased security, data storage, and privacy issues, as well as the ongoing need to improve performance, distributed systems are the natural choice for many businesses(Manfred Touron,2018).

Distributed infrastructure refers to an IT management approach in which IT resources are distributed across multiple locations or

business units, but with a greater degree of central coordination and control than in a decentralized infrastructure (Ghosh & Chakraborty, 2018). Distributed systems are composed of nodes that can operate independently of one another. In contrast to decentralized systems, every node in a distributed system is equal, which means that data ownership and processing resources are spread fairly throughout the network.

Because of the degrees of abstraction involved, users wrongly believe they are working with a single system. To work as a single coherent system, the collection of distinct nodes must be able to interact and collaborate with one another. As a result, ensuring and maintaining a constant communication channel across all network components is the primary problem in developing a distributed system.

Although implementing, managing, and debugging distributed systems can be challenging, the advantages of performance, scalability, low latency, and fault tolerance make the effort and expense worthwhile.

4.2 Advantages of using distributed infrastructure

- **Highly fault tolerant** : Distributed systems are made up of several nodes that collaborate to achieve a common purpose. The system is reliable and fault resilient as a result of this architecture. Any server can fail without affecting the rest of the network; the functions of that server are automatically redistributed among the remaining accessible servers.

- **Scalable** : Because IT resources can be added or removed from different locations as needed, distributed infrastructure can be more easily scaled to accommodate growth or changing business needs. Distributed systems can scale vertically as well as horizontally.

- **More Secure** : No single server controls all of your enterprise's sensitive data and key services over a distributed network. If a single node has been compromised, the hacker can use only the data particular to that node. Before your network orchestration solution redistributes network processes to a new server, a hacker can only cause minor damage to a server on a distributed network.

- **High up-time** : This measure denotes the overall amount of time the system is operational. In general, distributed systems have high levels of availability. Because distributed systems are made up of several machines, they can divide workload during maintenance operations to ensure business continuity.

- **Low latency** : Latency should ideally be as near to "0" as possible. The benefit of distributed systems is that nodes can be geographically scattered, allowing traffic to reach the node closest to it. Because network processing power is

dispersed evenly across multiple nodes, distributed networks have lower latency than alternative topologies.

- **Improved disaster recovery :** Data and IT resources can be replicated and stored in many places, minimizing the chance of data loss in the case of a disaster, which can increase disaster recovery capabilities.

4.3 Disadvantages of using an distributed infrastructure

- **Expensive** : Distributed network management is more expensive since it necessitates the use of network orchestration tools to offer continuous load balancing and ensuring that all nodes coordinate for configuration and routing updates, as well as changes to security policies.
- **Difficult to manage** : Distributed networks are more difficult to plan and execute, and there are fewer network engineers and sysadmins with hands-on expertise with them.
- **Overloading** : Overloading is a typical problem in distributed systems that occurs when all of the distributed system's nodes attempt to submit data at the same time. Overloading has an effect on the reaction time of a system.
- **Increased complexity** : The central coordination and management of IT resources across different locations or business units in a distributed infrastructure can be more complex than centralized or decentralized infrastructure, requiring more specialized knowledge and expertise.
- **inconsistent IT management practices** : Without proper coordination and oversight, distributed infrastructure can lead to inconsistent IT management practices across different locations or business units, which can lead to inefficiencies and increased risk.
- **Dependence on network connectivity** : Distributed infrastructure relies heavily on network connectivity, and any disruptions or outages in the network can affect the availability and performance of IT resources across different locations.

The benefits of distributed systems must exceed the drawbacks, and they take decentralization to a new level by evenly and automatically spreading processes, jobs, and functions throughout your whole company network. Despite being less frequent than centralized or decentralized networks, distributed networks benefit large commercial networks and may see growing usage in the future.

5. Factors to consider before deciding on a infrastructure

5.1 Business needs

Businesses must consider a lot of things before deciding on an IT infrastructure for their needs . Some of the considerations to examine are the infrastructure's scalability and adaptability, its security features, the quality of technical assistance provided, and the total cost of ownership.

Scalability and flexibility are key elements for enterprises since they require an IT infrastructure that can support their development and changing needs. Given the prevalence and seriousness of cyberattacks, security is another important consideration. Technical assistance is critical for quickly and efficiently fixing any infrastructure defects or problems. Finally, enterprises must carefully assess the whole cost of infrastructure ownership, which includes not only the initial investment but also ongoing maintenance and upgrading expenditures.

Overall, businesses must carefully assess their needs and goals before selecting an IT infrastructure to ensure that it aligns with their strategic objectives and provides the necessary features and capabilities to support their operations efficiently.

5.2 Budget

Budget constraints are an important element for firms to consider before settling on an IT infrastructure. Budget limits are an important consideration for firms because IT infrastructure deployment can be costly. To determine the anticipated return on investment for their IT infrastructure expenditure, businesses must conduct a cost-benefit analysis. This analysis should also consider ongoing maintenance expenses and anticipated future enhancements.

Companies must assess how much money they can reasonably spend on IT infrastructure while still meeting their business needs. "Budget constraints can lead to the selection of lower-cost solutions that may not meet the requirements for scalability, dependability, and security." Businesses can make informed judgments regarding the IT infrastructure that will best suit their goals while maintaining within their budgetary constraints by carefully analyzing budget constraints. Therefore, businesses must reach a middle ground between their Infrastructure needs and the financial limitations so that they can support their operations in the long run.

5.3 Integration

Before choosing an IT infrastructure, firms must carefully evaluate integration aspects. A business must make sure that its new IT infrastructure works effectively with the organization's processes and workflows and that it is compatible with the hardware and software already in use (Ahmad et al., 2019). Compatibility with existing systems, capacity to integrate with new systems, and simplicity of data movement are all integration-related concerns. It is crucial to take cooperation and communication issues into account when choosing an IT

infrastructure because they can affect how effective the infrastructure is. These elements comprise the capacity for real-time communication, support for distant work, and integration with collaboration tools. It is crucial to take cooperation and communication issues into account when choosing an IT infrastructure because they can affect how effective the infrastructure is. These elements comprise the capacity for real-time communication, support for distant work, and integration with collaboration tools.

The integration limitations of current systems and applications must be taken into account when choosing an IT infrastructure. To avoid any conflicts or disruptions in company operations, firms should assess how well the new infrastructure works with the current systems. Assessing the system's compatibility with legacy applications, databases, and middleware is part of this process. Companies should also think about whether the new infrastructure might need to be customized or modified in order to ensure seamless interaction with old systems. In general, being aware of integration limits can assist businesses in selecting IT infrastructure that is in line with their needs and goals.

5.4 Security

When choosing on an IT infrastructure, security is a critical element to consider. Businesses must safeguard their infrastructure against cyber risks such as data leaks, malware, and hacking attempts. Physical security, network security, and data security are all important considerations. Physical security entails protecting hardware and equipment from damage and unauthorized access. Network security entails safeguarding the network against cyber risks such unauthorized access, viruses, and hacking attempts. Data security entails protecting sensitive information from unauthorized access, loss, or corruption. To prevent security threats, businesses should undertake a thorough risk assessment and adopt suitable solutions such as firewalls, intrusion detection systems, and data encryption. Furthermore, frequent security audits and updates should be performed to assure the infrastructure's security throughout time.

5.5 Compliance

Organizations must examine compliance issues before deciding on an infrastructure. Organizations should comply with various guidelines relying upon their industry and district, including information protection regulations, industry-explicit norms, and worldwide regulations. Inability to maintain these principles might have significant repercussions, including fines, mischief to one's standing, and loss of customers. As a result, selecting an infrastructure that meets the proper compliance criteria is crucial.

According to a Frost & Sullivan (2018) survey, one of the primary drivers of IT infrastructure decisions in the healthcare industry is regulatory compliance. As indicated by the survey, medical care associations focus on an IT framework that agrees with information security regulations

like the Health care coverage Conveyability and Responsibility Act (HIPAA). This emphasizes the significance of compliance concerns in IT infrastructure decision-making.

5.6 Management and maintenance

Management and maintenance issues should be considered while deciding on an IT infrastructure. This includes the availability of qualified staff for maintenance and upgrades, as well as the infrastructure's ease of management and scalability. It is critical to ensure that the infrastructure can support the business's long-term demands and expansion goals, and that suitable management and maintenance practices are in place to maintain smooth operation and reduce downtime.

As stated by Lin et al. (2013),"Proactive and effective management and maintenance are critical for ensuring an IT infrastructure's security, reliability, and availability". Thus, organizations should cautiously evaluate the administration and support prerequisites of a proposed framework to guarantee that they have the assets and information to oversee and keep up with it effectively over the long run.

6. Cybersecurity implications on centralized and decentralized IT infrastructure

6.1 The influence of centralized and decentralized infrastructure on cybersecurity

The effects of centralized versus decentralized infrastructure on cybersecurity can differ. Centralized infrastructure can benefit from a more centralized approach to security, with fewer access points that can be more readily controlled and monitored. It does, however, introduce a single point of failure because a breach in the central system can endanger the entire network. If the central server is hacked, the entire system goes down and activities can be suspended. The importance of protecting the central server cannot be overstated.

The attack vector is substantially wider under a decentralized and distributed setup. Regardless of whether one of the hubs or systems fail, the remaining of the network can keep on working. In addition, if the problem is found, the afflicted element of the system can be isolated while the remainder of the system remains operational. Decentralized architecture can distribute security and decrease the impact of a single breach, but it can also result in a lack of consistency and standardization in network security procedures. However, if the security breach is not detected, malware might spread throughout the network and infect all nodes and devices.

Finally, when it comes to cybersecurity, both centralized and decentralized infrastructure offer advantages and downsides, and companies must carefully examine which strategy best suits their objectives and risk tolerance.

6.2 Possible cyber threats for centralized and decentralized infrastructure

Both centralized and decentralized infrastructure models are powerless to various sorts of internet based dangers, for example, malware, phishing, and social engineering attacks. Each infrastructure type gives some degree of resistance to particular attacks, which can be quite damaging in some circumstances.

The centralized system has many cybersecurity problems because only one core server controls the entire network. Its operation may be greatly affected by a DDOS attack. In a DDoS assault, the attacker overwhelms the target system with traffic, using up all of its resources and blocking access to it for authorized users. An attack against a single point of failure, such as a central server or infrastructure, is possible in a centralized system. This might cause a full breakdown of the framework, making it inaccessible to clients and causing serious monetary and reputational damage to the organization. All of the data on centralized systems is held on a single server, making them a popular target for hackers.Essentially, man-in-the-center attacks are risky in light of the fact that they give the assailant admittance to a huge organization of systems by compromising one system in the network.

Because of different weak spots, decentralized foundation is less defenseless to cyberattacks than centralized servers, despite the fact that it is as yet not thoroughly secure. Unreported intrusions or infections spread to connected networks if they are not stopped. A decentralized infrastructure is particularly vulnerable to Sybil attacks and blockchain 51% attacks.

6.3 Best security practices

Firewalls: The firewall protects the network by constantly monitoring the data that flows over it. It is a system that prevents cyberattacks by utilizing both hardware and software technology. They block and redirect traffic based on a preset set of network rules. The first line of security for any ICS system must be a firewall established by vendors with a proven track record.

Encryption: Data exfiltration is one of the most serious cybersecurity issues that enterprises confront. Encryption is required for any network communication. Data encryption secures information even if it is stolen from a network and adds an extra degree of protection to protect critical information.

Redundancy: To boost resilience, redundancy must be introduced into the system. Backups maintain business continuity even after a cyberattack by storing data on a central server that is frequently backed up in multiple places. When hackers destroy the data stored on the central server, such backups can restore it.

Passwords and Authentication: Using common passwords is one of the most prevalent entrance points for hackers. Some

facilities fail to alter the default passwords sent with manufacturers' devices and software. Strong passwords should be used, and corporate password management software can help with this. To give an additional layer of protection to the organization, two-factor verification or multi-factor authentication can be used.

Security Updates and Audits: External agencies undertake security audits to assess the firm's cybersecurity defenses. White-hat hackers utilize penetration testing and other ways to breach security defenses during a security assessment. This experiment exposes the system's weakness and has the potential to increase the ICS's cyber resistance.

Cyberattacks can affect any type of computing equipment. They are continually evolving, and the defenses against them must do the same. Cybersecurity is a continuous endeavor by the industry to remain on top of novel attack methods.

7. Blockchain: a secure solution for Infrastructure management in IT industry

"Blockchain is a distributed digital ledger technology that enables secure and transparent transactions between parties without the need for a central authority or intermediary" (Swan, 2015, p.4). Blockchain is unusual in that it has successfully challenged our perceptions of data storage and management. To the uninformed, blockchain may appear to be nothing more than a database, and they are partially true. Blockchain, in its most basic form, is a transactional history. Data entered into a blockchain network is protected by complicated cryptographic techniques and stored in structures known as blocks. Each block of transactions contains a set of data from the preceding block, which connects them and forms a chain of blocks. Data cannot be altered since it is stored in thousands of interconnected blocks. If a malicious actor attempts to tamper with data from a block of transactions, the system will deem all subsequent blocks obsolete, discarding any changes that are not allowed by network participants.

The blockchain's decentralized nature imposes transparency, trust, and responsibility. Businesses and trade partners will no longer need to rely on third parties to settle disputes, execute audits, verify, and share data since the blockchain will hold the only genuine version of the truth. Each participant keeps an encrypted record of every transaction, and confidence is ensured by complicated mathematics at every level of the transaction process. This durable recording method cannot be rejected, as such, parties that do not totally trust each other can engage in economic exchanges.

7.1 decentralized processing system

The blockchain is decentralized and no central authority or intermediary is regulating it. Instead, all network participants have equal control and can validate and verify transactions. Thus, the blockchain is more impervious to threats and

restrictions. "One of the critical elements of blockchain innovation is decentralization, which empowers a safer and straightforward framework for exchange and information of the executives"(Narayanan et al., 2016, p. 31).

One of the main parts of blockchain innovation is decentralization, which takes into consideration a safer and more straightforward framework for transaction and data management. Decentralization has no single point of failure , making the organization more impervious to assaults and bringing down the risk of censorship or fraud. A decentralized blockchain can disturb various ventures by giving a safer and more straightforward framework for exchange and data management that isn't constrained by a central authority or middleman.

7.2 distributed processing system

A distributed blockchain network is one in which numerous nodes collaborate to maintain the blockchain and there is no centralized authority governing the network. Each network node keeps a complete copy of the blockchain, which is regularly updated via a consensus mechanism. Since there is no weak link or shortcoming, the organization is decentralized and resistant to threats. In a distributed blockchain network, all hubs have an equivalent position to validate and verify transactions, and every hub is responsible for the blockchain's Integrity. Since distributed blockchain dispenses with the requirement for go-betweens and empowers secure and direct peer-to-peer transactions, it is more secure and transparent than centralized systems. Overall, distributed blockchain can possibly change different businesses by giving a protected, straightforward, and decentralized framework for transaction and data management that is not centralized.

8. Most used Infrastructure management methodology

Both centralized and decentralized have their own benefits. There is no doubt that states, affiliations, and associations need command over their assets, regardless, when they need to give up efficiency for it. Before decentralized systems emerged, centralized mechanisms aided the growth of the earliest networks. Decentralized infrastructure, which are less inclined to failure and permit more limited access times, have given a huge improvement over traditional frameworks. They are still broadly utilized today, particularly since they have become more reasonable over the long run.

Decentralized framework gives individual systems more power and independence, taking into account more noteworthy adaptability and decision making. You can also use hybrid or federated blockchain systems to implement decentralization in a sustainable close environment. Simply because monolithic architecture is incapable of handling the platform's high volume of traffic. Several servers running in parallel divide the load amongst themselves, lowering the app's latency. They also help in tackling some of the critical issues like a single point of failure, data loss prevention

measures like data replication, etc(Shivang, 2022). Servers in data centers are also geographically distributed, closer to the end user, across continents, further reducing app latency.

While centralization is popular, multiple factors indicate a tendency toward increased decentralization. Millennials, for example, are currently the largest generation in the labor force. Millennials, in particular, demand flexibility and autonomy in their jobs, attributes that are more conducive to decentralized systems. To keep that rising part of the workforce engaged, decision-making may need to be dispersed more extensively across the organization. Many companies have turned their centralized systems into decentralized systems by implementing server clusters to handle vital network processes, so understanding decentralized management is important when deciding which management model to use.

8.1 Why is it more popular than other methods?

There are several reasons why companies may prefer decentralized over centralized and distributed infrastructure. One reason is that decentralized infrastructure provides greater control and autonomy to individual business units, which allows for more flexibility and faster decision-making (Raj & Haq, 2019). Additionally, decentralized infrastructure can provide better resilience to system failures, as a failure in one business unit will not necessarily affect the operations of other units .

Another motivation behind why organizations might lean toward a decentralized framework is that it can lessen the risk of single point failure, which is a concern in centralized infrastructure. By distributing the infrastructure across multiple locations or business units, the impact of any failure or attack can be limited (Miorandi et al., 2012).

Newer, smaller companies and organizations that need to respond quickly to new IT developments are most likely to benefit from decentralized IT networks(Borovyk, 2021). Overall, companies may prefer decentralized infrastructure because it provides more control, flexibility, resilience, and security. However, the decision of infrastructure management methodology relies upon the particular necessities of the organization.

8.2 How is it compared to other methodologies?

For most firms, comparing infrastructure management models is pointless because centralized architectures are too restricted for the needs of the modern enterprise network and have fallen out of favor. In some cases, such as data center administration and isolated LANs used for testing or government classified operations, centralized network management may still be useful.

Most businesses, however, adopt a decentralized network design in which clusters of master servers coordinate and govern network activities and services. Many data centers, colocation facilities, and branch offices use decentralized network administration. As a result, they are perfect for businesses that require quick and dependable access to network resources. By scattering your master servers among your network's systems, distributed management further decentralizes your network. Distributed networks are fault resistant, extremely adaptive, and, on average, faster and safer than other infrastructure types. Distributed networks, in any event, are more difficult to coordinate and manage, which might be a barrier to deployment.

Although distributed network management can be utilized in the same settings as decentralized networks, it is often preferred by high-tech enterprises that place a premium on security and privacy. Cryptocurrencies, for example, utilize decentralized networks, making it nearly hard for a hacker to access the full database of digital wallets or bring the network down. However, businesses lack the experience and tools required to completely establish a distributed network.

9. Conclusion

9.1 Final recommendation for companies considering centralized, decentralized and distributed IT infrastructure management methodologies

Concerning IT infrastructure management models, there is no one-size-fits-all model. Each organization has unique needs and requirements that will decide the best approach for them. However, based on the understanding of the pros and cons of each methodology, we can get to know which infrastructure models suit a business model better:

When size or uniformity is a big cost factor, when specialized production capabilities are required, or when manufacturing strategy is an important component of corporate strategy, centralization makes sense. Centralized IT infrastructure management is best suited for organizations that have a relatively small IT infrastructure and a limited budget for IT staff. This methodology can help reduce IT costs and improve efficiency by centralizing the management of resources and streamlining processes. However, it may not be the best fit for larger organizations that require more complex infrastructure management solutions.

Decentralization, on the other hand, is more suited when various products for different markets are required, or when the organization must respond swiftly to changing or geographically diverse client needs. Although the pendulum may be swinging back toward decentralization, centralized structures still could offer potentially significant cost savings(Ted Billies,2016). Choosing the correct model for your organization is crucial to any restructuring effort—the decision can affect

not only your organization's costs and efficiency but also customer happiness and staff engagement. Decentralized IT infrastructure management can be a good fit for organizations that have multiple locations or business units that require autonomy over their IT resources. This approach takes into account more noteworthy adaptability and responsiveness to necessities, yet it can likewise prompt conflicting administration practices and possibly greater expenses because of duplication of exertion.

Distributed IT infrastructure management is ideal for organizations with geographically dispersed operations and a need for high availability and reliability. This approach ensures that IT resources are available at all times, and can help minimize downtime and disruptions. Companies aiming to scale more and also require the system to be more fault tolerant should go with distributed systems. It can, however, be harder to oversee and may require more resources and responsibility.

Finally, the optimal technique will be determined by your organization's specific objectives and goals. Before choosing a management technique, it is critical to properly examine your IT infrastructure and consider criteria such as size, complexity, budget, and human resources. Furthermore, ongoing monitoring and evaluation of your IT infrastructure will be required to guarantee that your chosen technique continues to fulfill the needs of your firm over time.

11. **Reference**

1. Myhill, W. N., Cogburn, D. L., & Samant, D. (2008). Developing Accessible Cyberinfrastructure-Enabled Knowledge Communities in the National Disability Community: Theory, Practice, and Policy. Assistive Technology. https://doi.org/10.1080/10400435.2008.10131943

2. Cybersecurity Infrastructure adoption Model for Malware Mitigation in Small Medium Enterprises (SME). (2022, August 6). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9915696

3. Gedia, D., & Perigo, L. (2018). A Centralized Network Management Application for Academia and Small Business Networks. Information Technology in Industry, 6(3), 1–10. https://doi.org/10.17762/itii.v6i3.59

4. An integrated approach to centralized communications network management. (1979). IBM Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/5387970

5. Bililies, T. (2016) CENTRALIZATION VERSUS DECENTRALIZATION, 8 April. Available at:https://www.alixpartners.com/insights-impact/insights/centralization-versus-decentralization/

6. Borovyk, O. (2021) Decentralization principle, prezi.com. Available at: https://prezi.com/p/svhoqlxhn3oc/decentralization-principle

7. Stewart, C. A., Simms, S. C., Plale, B., Link, M. R., Hancock, D. J., & Fox, G. C. (2010). What is cyberinfrastructure. SIGUCCS: User Services Conference. https://doi.org/10.1145/1878335.1878347

8. Touron, M. (2019) Centralized vs decentralized vs Distributed Systems · Berty Technologies, Berty Technologies. Available at: https://berty.tech/blog/decentralized-distributed-centralized

9. Pandey, A. (2021) Scale-up vs scale-out, LinkedIn. Available at: https://www.linkedin.com/pulse/scale-up-vs-scale-out-ayush-pandey-1e?trk=articles_directory

10. shivang (2022) Difference between centralized, decentralized & Distributed Systems oversimplified, Scaleyourapp. Available at: https://scaleyourapp.com/difference-between-centralized-decentralized-distributed-systems-explained

11. Lin, W., Lai, C., & Chang, C. (2013). A study on the implementation of IT infrastructure and its effects on business performance: Empirical evidence from container shipping companies in Taiwan. Information Management & Computer Security, 21(1), 33-48. Available at : https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

12. Ahmad, I., Ahmad, N., & Ahmad, R. (2019). Key factors to consider while designing an information technology infrastructure for business. International Journal of Advanced Computer Science and Applications, 10(10), 449-455.

13. KSpiceworks. (2019). State of IT: The Annual Report on IT Budgets and Tech Trends. https://www.spiceworks.com/marketing/state-of-it/report/

14. Ghosh, S., & Chakraborty, A. (2018). Centralized vs. decentralized IT infrastructure management: A comparative study. International Journal of Computer Applications, 181(16), 7-12. doi: 10.5120/ijca2018917673

15. Wright, D. J., & Wang, S. (2011). The emergence of spatial cyberinfrastructure. Proceedings of the National Academy of Sciences of the United States of America, 108(14), 5488–5491. https://doi.org/10.1073/pnas.1103051108

16. Kim, Y., & Crowston, K. (2011). Technology adoption and use theory review for studying scientists' continued use of cyber-infrastructure. Proceedings of the Association for Information Science and Technology, 48(1), 1–10. https://doi.org/10.1002/meet.2011.14504801197

17. Yu, Y., Ibarra, J., Kumar, K., & Chergarova, V. (2021). Coevolution of cyberinfrastructure development and scientific progress. Technovation, 100, 102180. https://doi.org/10.1016/j.technovation.2020.102180

18. Kee, K. F., Le, B., & Jitkajornwanich, K. (2021). If you build it, promote it, and they trust you, then they will come: Diffusion strategies for science gateways and cyberinfrastructure adoption to harness big data in the science, technology, engineering, and mathematics (STEM) community. Concurrency and Computation: Practice and Experience. https://doi.org/10.1002/cpe.6192

19. Ribes, D., & Lee, C. E. (2010). Sociotechnical Studies of Cyberinfrastructure and e-Research: Current Themes and Future Trajectories. Computer Supported Cooperative Work, 19(3–4), 231–244. https://doi.org/10.1007/s10606-010-9120-0

20. Bietz, M. J., Ferro, T., & Lee, C. E. (2012). Sustaining the development of cyberinfrastructure. Conference on Computer Supported Cooperative Work. https://doi.org/10.1145/2145204.2145339

21. Stewart, C. A., Apon, A., Hancock, D. J., Furlani, T. R., Sill, A., Wernert, J., Lifka, D., Berente, N., Cheatham, T. E., & Slavin, S. D. (2019). Assessment of non-financial returns on cyberinfrastructure. IEEE International Conference on Cloud Computing Technology and Science. https://doi.org/10.1145/3355738.3355749

22. Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. Applied Sciences, 11(10), 4580. https://doi.org/10.3390/app11104580