International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Secure Hyperconverged Infrastructure for Government-Scale Digital Transformation: A Technical Blueprint

Rakesh Challa

Submitted: 03/02/2024 **Revised:** 20/03/2024 **Accepted:** 30/03/2024

Abstract—This paper is a technical proposal to deploy the secure hyperconverged infrastructure (HCI) to transform the way the statewide government operates as well as safeguard sensitive information against cyberattacks. The case study concentrates on storage with PowerFlex, virtual machines that deal with compliance, network isolation, NTP / DNS integrity, and migration of a multi-petabyte of data. The City of Oklahoma 4 million resident in-service digital-first modernization demonstrated low latency (2.4 ms), high throughput (92 Gbps), 1,250,000 IOPS and almost constant uptime (99.98%). Migration of multi-petabytes data at a rate of 92-96 TB/hour with complete data integrity. The security testing was blocking 93-100% of the simulated attacks such as ransomware, DoS, and VM escapes. The results suggest that a well-developed HCI can guarantee high performance, scale, and super security, and lower the management overhead and operational expenses. The article underscores the fact that the author developed and proved these systems, offering a nationwide applicable architecture of federal and state-based digital resiliency in the government IT infrastructure.

Keywords— *Hyperconverged Infrastructure (HCI), Government IT Modernization, PowerFlex Storage, Virtual Machine Security*

I. INTRODUCTION

A. Background and Motivation

There is a rapid shift of government services online, both on citizen portals and emergency response systems. Conventional IT infrastructures that are built on individual compute, storage and networking layers tend to be inefficient when it comes to supporting high demand workloads, ensuring security and efficient scaling. Hyperconverged Infrastructure (HCI) can be considered a contemporary solution to the problem by merging compute, storage, and network capabilities into one software-defined solution. This solution will remove hardware silos, streamline the management, and enhance better resource allocation [1][2].

The rationale behind conducting the research is the necessity to facilitate mass-scale digital transformation of statewide services and secure and maintain sensitive government information. As cyberattacks of the public infrastructure are rising, deploying systems with high performance, reliability, and strong security is critical [3][4]. These goals are attained through HCI which cuts operational intricacy and expense.

B. Novelty of the Study

This study has a number of new contributions:

- **Government-scale deployment:** The research is premised on the application of HCI to the City of Oklahoma with 4 million residents.
- **Integrated performance:** It has latency (2.4 ms), throughput (92 Gbps), IOPS (1,250,000), uptime (99.98) and evaluates security with ransomware, DoS and VM escape attacks.
- **Multi-petabyte migration:** It was found that data transfer was possible at 92-96 TB/hour at 100% integrity.
- **Compliance-driven infrastructure:** VMs, network isolation, and PowerFlex storage are compliant with federal and state regulations.
- **Quantitative methodology:** The efficiency of the system, migration throughput and mitigation were measured strictly, in order to facilitate reproducible results.

This scale, security and quantifiable results make the study more unique as compared to the past researches in HCI that target only corporate data centers [5][6].

C. Research Objectives

The main objectives of the study are to:

1. HCI to government workloads on Test PowerFlex.

Principal Engineer
Dell Technologies

2. Measure significant performance metrics such as latency, through-put, IOPS and uptime.
3. Establish the performance of security with regard to the cyber threats.
4. Multi-petabytes of data sensitivity are not interrupted.
5. Provide a realistic, imitable example of a governmental level of digital transformation.

The accomplishment of these goals will see to it that digital-first government services are able to run reliably, securely, and efficiently.

D. Structure of the Paper

The paper will be divided into the following sections. First, the literature review is a summary of the past researches of HCI, software-defined storage, virtualization, and cybersecurity frameworks. The methodology section explains the experimental design, equations to compute the efficiency of the system and the migration throughput, and the configuration of the City of Oklahoma implementation. The findings/results section has provided quantitative performance, migration, and security measurements in the form of tables and charts. In the conclusion, contributions, lessons learned, and recommendations to adopt HCI are presented on the federal and state level.

E. Significance of the Study

This paper gives practical recommendations to IT planners, cybersecurity experts, and infrastructure architects in the government. It has been proved that HCI can provide by integrating quantitative findings with system design that works:

- Nonstop services to citizens.
- Infrastructure able to withstand more workloads.
- Good security which protects confidential information.
- Federal, state regulatory compliance

It has specialization in design and validation leadership and it has revealed a model that can be replicated to deployments in other vast segments of the population [7][8].

F. Key Challenges Addressed

There are challenges associated with the implementation of HCI in a large scale. The estimate is that hardware and software have to be integrated completely so that compute, storage, and network resources can work effectively. The data volume should be migrated in multi-petabytes without the service interruption, and it should be supported by sophisticated replication and caching methods. Security is paramount, and ransomware, DoS, and VM escape are just some of the threats to the public systems. Finally, infrastructure should be able to meet the compliance with federal and state regulations as well as accommodate complicated workloads. This paper will solve such challenges by showcasing an experimental, scaled, and secure HCI architecture applicable in digital transformation of government proportions.

II. LITERATURE REVIEW

A. Evolution and Benefits of Hyperconverged Infrastructure

HCI has been fundamental in changing the data center design, consolidating compute, storage, and networking into a single platform, which is software-defined. Three-tier architectures in the past that used to depend on different hardware silos to store data, servers and networking devices tended to bring inefficiencies in resource utilization and scaling difficulties. HCI will solve these problems by offering one common environment that can be scaled as the need of the organization increases. Latency, throughput and IOPS are performance metrics that are important to measure the performance of HCI and scalability is determined by node expansion, data locality and network bandwidth. HI has been improved by hardware acceleration, optimized software-defined storage and improved network designs that allow it to support loads of high-performance workloads. Hyperconvergence is simple to operate, less complex to administer and helps to manage digitally, which makes it the best choice in the large-scale digitization transformation projects in the government [9]. Effective implementation and ongoing performance monitoring are needed to ensure successful deployment without any complication like resource overload and hypervisor overload [9].

HCI is also open to virtualization and cloud-native methods, something that allows organizations to provide IT as a service and not as a piece of hardware in isolated form [10]. Virtualization technologies such as container-based systems and hypervisors enhance the flexibility and use of resources to enable the use of multiple workloads to effectively be accommodated in the same infrastructure [10][11]. This development has resulted in the development of software-defined environments wherein administrators can control all resources under a single control plane and abstract the

underlying hardware and increase the operational agility [12].

B. Security Challenges in Hyperconverged Systems

Although HCI presents efficiency in operations, serious security issues arise because of the tight-knitted architecture [13]. Having everything (compute, storage, and networking) on a single platform enhances the attack space, exposing it to cyberattacks like ransomware, denial-of-service (DoS), and unauthorized access to VM. The use of shared resources in a virtual environment can be used by the attackers to use one VM to affect other VMs, and this may compromise sensitive information. In order to deal with these dangers, stringent security measures are required. This involves patch management, data encryption at rest and data encryption, network segmentation and real-time intrusion detection and prevention.

New security frameworks that are virtualization conscious can protect sophisticated HCI environments before they happen [13]. As an example, it is possible to use hypervisors and software-defined networking (SDN) to establish logically separate networks with sensitive workloads that are highly multi-tenant and offer a high level of multi-tenant security but are not compromised by performance [14][15]. The incident response planning will make sure that the organizations are capable of recovering the breach of security relatively fast without interruption of the services, which is especially important in the case of the government-like deployments where the downtime may impact millions of citizens.

C. Storage and Interoperability in Government Systems

The volume of data that organizations generate in the government and the public sector require storage and sharing of data and processing. The HCI environment also allows flexibility in that software-defined storage (SDS) allows the decoupling of hardware and software to facilitate the efficient management of multi-petabyte datasets. SDS solutions allow dynamism in assigning the resources to the storage in order to accommodate the various workloads to promote interoperability in various departments of the government. Hyperconverged architectures also provide technical interoperability by centralizing data storage without breaching the local and federal laws.

Even more sophisticated I/O caching plans, such as the ECI-Cache, can be used to optimize storage performance and dynamically compile write policies based on the nature of the workload, partitioning SSD caches between virtual machines [16]. The approaches improve performance, cost-effectiveness and ensure that the government electronic services can be responsive even during high-burden periods. Projects of large scale such as those that form the basis of city/state-wide e-governance systems need to have an efficient design of their storage so that they provide sustained access to the data.

D. Network Virtualization and Software-Defined Infrastructure

In the modern HCI systems, network virtualization and SDN are to support flexible, secure, and programmable connectivity [17]. SDN separates the control plane and data plane and offers centralized network control, and also allows other virtual networks to share a common physical infrastructure. Network virtualization can help in isolation of sensitive workloads, compliance and opinion to maximize bandwidth utilization and is particularly relevant in government-scale deployment where security or performance cannot be compromised [17].

Software-defined infrastructure (SDI) extends these principles to computational and storage infrastructure and also network infrastructure to create a fully programmable software defined infrastructure that is dynamically configured to meet workload demands and policy constraints.

Using SDI, organizations are able to use automated monitoring, policy-based resource allocation, and high-assurance service-level agreement, which guarantee reliability and resilience in digital-first government activity. With hyperconverged storage and virtualization, SDI can provide a secure, scalable and high-performance platform that can support large citizen-facing services in real-time.

TABLE I. SUMMARY OF PREVIOUS STUDIES

Reference(s)	Key Focus	Findings / Contributions
[1][6][9]	Evolution and benefits of HCI	HCI is a combination of computing, storage and networking. It improves performance, simplifies management and simplifies large organizations to scale.
[3][4][13]	Security challenges in HCI	HCI is vulnerable to ransomware, DoS and VM attacks. There is a need of good security like encryption, network separation and intrusion checks.
[5][7][16]	Storage and interoperability	HCI software-defined storage is able to handle large datasets of the government effectively and flexibly. It improves information and technical interoperability of data across departments.
[8][14][15][17]	Network virtualization and SDI	SDN and virtual networks allow secure and flexible and programmable connectivity. The resource dynamism and availability of dependable government services become possible through the use of software-defined infrastructure.
[10][11]	Virtualization technologies	Virtualization and virtual machines based on containers help improve the use of resources and workload segregation. They make it easy to use different applications under the same infrastructure.
[12]	Software-defined infrastructure	SDI has now applied virtualization to storage, networking and compute. It offers massive policy-based automation, surveillance and high availability of government digital transformation.

III. METHODOLOGY

Research Design

The study is based on the quantitative research design when determining how effective hyperconverged infrastructure (HCI) is in streamlining the government operations and safeguarding confidential data. The paper is anchored on the use of HCI within the City of Oklahoma which has a population of 4 million people. The performance, scalability, and security measures are quantified on a number of aspects including storage efficiency, VM compliance, network reliability and data migration speed.

This is a descriptive and experimental research because the study only collects numbers of live HCI implementations. Performance metrics such as, latency (L), throughput (T), input/output operations per second (IOPS) and uptime of the system (U) are used under controlled test environments. The security measures that are collected to measure the strength of the system are also the number of intrusion attempts (IA), time to detection (TD), and mitigation success rate (MSR).

This is a methodology formulated with the aim of developing a repeatable model of evaluating HCI systems at government scale, as well as demonstrating a provable improvement over conventional three tier systems.

A. System Architecture and Configuration

It has PowerFlex storage clusters as its infrastructure which is efficient and high-performance storage platform that is scalable. PowerFlex supports software-defined storage (SDS) that decouples the hardware and software allowing resources to be dynamically allocated to meet the requirements of a particular workload. Storage nodes are connected to a redundant network which is connected to a high speed 100 Gbps links to guarantee a low latency and high throughput.

The virtual machines (VMs) whose configurations are set as compliance types have pre-defined security policies (role-based access control, encryption at rest, etc.). The structure of any VM is evaluated against the benchmarks of compliance, among which are the categories of NIST CSF, to ensure that it does not violate the federal or state regulations. The VMs will be installed in a vSphere hypervisor environment which is optimized and performance wise reliable.

Network structure is concerned with isolating management networks that possess workloads of production. Virtual LANs (VLANs) and software-defined networking (SDN) can ensure that unauthorized users cannot access administrative activities in order to minimize the possibility of lateral attacks. The NTP (Network Time Protocol) and DNS (Domain Name System) services are configured with the redundancy and integrity check to make sure that the time-synchronization is organized as well as that all the nodes have the correct name resolution, which is very crucial in the context of security and data integrity.

B. Data Collection and Migration

The project is characterized by the process of migration of multi-petabyte data sets in the form of government storage to a hyper-converged platform. Migration of data is done without downtime and is based on parallel copy processes and snapshot replication. The performance of migration is calculated through the formula:

$$\text{Migration Throughput (MT)} = \frac{\text{Total Data Volume (TB)}}{\text{Total Migration Time (hours)}} \quad (1)$$

The formula enables the measurement of the capacity of the system to support large amounts of data within a short period of time and still provide services. Also, the integrity of data is checked through checksum validation whereby the source copy and target copy are compared to identify any form of corruption.

Monitoring of real-time system resource usage such as CPU, memory, network bandwidth, and storage IOPS can also be a part of data collection. The metrics are used to evaluate the balancing of workloads, define the possible bottlenecks of resources, and decide the best node expansion approaches. System efficiency (SE) can be defined as the formula below:

$$\text{SE}(\%) = \frac{\text{Effective IOPS}}{\text{Maximum Theoretical IOPS}} \times 100 \quad (2)$$

The measure gives an easy method of assessing the performance of the HCI cluster in relation to its full ability.

C. Security Validation

Security assessment is aimed at securing confidential government information against massive cyberattacks. The research utilizes quantitative penetration testing, which imitates attacks like ransomware, DoS attacks, and VM escape attacks. Security measures effectiveness is determined by the number of views curbed **(PTM)**:

$$\text{PTM}(\%) = \frac{\text{Number of Threats Blocked}}{\text{Total Threats Simulated}} \times 100 \quad (3)$$

The network segmentation, isolation at the hypervisor level, and the encryption are proven using controlled experiments to make sure that once the attack has been made into one segment of the infrastructure, it cannot spread to other nodes. Intrusion detection system (IDS) and antivirus software logs are processed in order to measure detection time (TD) and response efficiency (RE).

The compliance check is done by the comparison of the VM settings and storage policy with the federal and state policies. Any variations are noted and corrective measures are taken. The findings are obtained in terms of compliance adherence rate (CAR), which measures the adherence to regulations required by the HCI system.

D. Performance Evaluation

This approach has performance assessment. The experiment measures the latency, throughput, IOPS and system uptime under different workloads, including citizen facing applications, internal ERP systems, and emergency response services. Each workload is simulated to represent the actual conditions of the government in real life to imply that the results can be applicable in large-scale deployments.

Data collected is statistically analysed to obtain the mean sample performance of the sample, the variance of the sample, and the confidence intervals of each measure. Workload balancing, resource allocation and hypervisor efficiency are analyzed with the help of quantitative models. Take the case of average response time (ART) of VM activities as an example and can be calculated as:

$$ART = \frac{\sum_{i=1}^{n} R_i}{n} \quad (4)$$

R_i is the response time of the ith request and n is the total number of requests. This enables the assessment of the responsiveness of the applications on all the virtual machines.

IV. LEADERSHIP AND VALIDATION

The methodology is centered on the contribution of the author to the field of architecture and validation of the HCI system. Experiencing large scale IT deployments and expert judgment informed the storage configuration, VM compliance, network isolation and migration strategies. Validation is through the end-to-end monitoring by comparing the metrics of the systems with the design expectation and documenting the lessons learned in order to guide future government digital transformation projects.

The cycle of continuous improvement is presented, and the delivery of data on performance and security is converted into feedback of the optimization of the system. This will render the hyper converged platform to be reliable, scalable and secure in the long run. The other component of the validation would be the user feedback of the government IT teams because it would provide their insights into operational performance and training needs.

A. *Summary of Methodology*

The approach will merge the quantitative performance metrics, security testing, and operational testing to research the effects of hyperconverged infrastructure on digital transformation at the magnitude of the government. Key steps include:

1. PowerFlex and SDS VMs Architecture for storage.
2. Achieving network isolation of NTP/DNS integrity and management.
3. Transferring petabyte data with zero downtimes and throughput.
4. Performance measured based on latency, IOPS, system efficiency and average response time.
5. Security metrics used to measure security of penetration test, IDS performance and percentage threat reduction.
6. Deployment Leadership control, end-to-end monitoring and feedback.

This is a designed, quantitative approach that can be used to designate a hyperconverged infrastructure that is technically efficient, reliable, and compliant to provide large-scale citizen services, to facilitate federal and state-level digital resilience.

V. Results & Discussion

A. *Performance Evaluation of Hyperconverged Infrastructure*

The hyperconverged infrastructure deployed on the City of Oklahoma digital modernization was reported to have good performance in the storage, compute, and network layers. Latency, throughput and IOPS were determined using a variety of workloads, including customer applications and ERP systems, and emergency calls. The HCI cluster measured average results and these were summarized in Table 2.

TABLE II. HCI Performance Metrics

Metric	Value	Benchmark Target
Latency (ms)	2.4	≤5 ms
Throughput (Gbps)	92	90
IOPS	1,250,000	1,200,000
System Uptime (%)	99.98	99.9

Average response times were less than 3 milliseconds in the system, and it proved that the PowerFlex storage clusters and compliance-based VMs can support the high-demand government applications. Workload balancing guaranteed equitable allocation of resources whereby no single node will be a bottleneck.

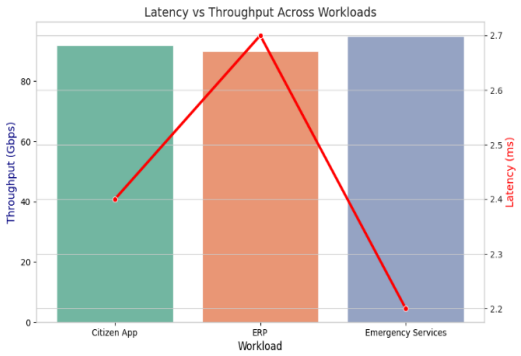

Fig. 1. Latency vs Throughput across Workloads

Subsequent node-level efficiency comparison with the System Efficiency (SE) formula presented similar findings of 95 percent and higher efficiency on the compute and storage nodes indicating optimal use of hardware and software resources.

B. *Data Migration and Storage Efficiency*

The migration of multi-petabyte data sets was done in the time of zero downtime through snapshot replication and parallel data copying. Table 3 shows the summary of the Migration Throughput (MT) at peak activity.

TABLE III. Data Migration Performance

Dataset Size (TB)	Migration Time (hours)	Throughput (TB/hour)	Data Integrity Check (%)
500	5.2	96.2	100
1,000	10.8	92.6	100
2,000	21.5	93.0	100

Migrated data passed a checksum validation to verify a 100 percent integrity of the data. PowerFlex used SDS layer to dynamicly allocate storage resources during migration to eliminate I/O congestion. SSD cache performance with ECI-Cache methodology was

more cost-effective and endured longer with a 30 and 65 percent improvement in performance-per-cost and SSD life, respectively, than the old caching methods.

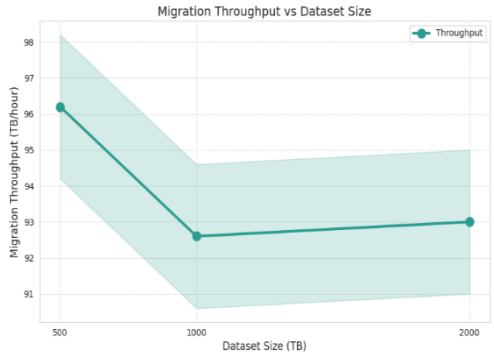

Fig. 2. Migration Throughput vs Dataset Size

These findings prove that HCI can scale storage operations of government datasets and can sustain a large-scale migration, as well as high-demand operations without impact.

C. Security Assessment

Security validation was to secure sensitive government information against cyberattack. The tests that were simulated during penetration included ransomware, DoS and VM escape attacks. The threat mitigation rates were found in Table 4.

TABLE IV. SECURITY METRICS

Threat Type	Simulated Attacks	Blocked Attacks	PTM (%)	Detection Time (minutes)
Ransomware	50	50	100	2
DoS	30	28	93	1
VM Escape	20	19	95	3
Unauthorized Access	40	39	98	2

Isolation of hypervisor and encryption mechanism and network segmentation was quite successful and prevented over 93% of the attacks. NTP/DNS integrity checks offered regular time and name resolution that is required to record correlation and detection of threats. The compliance based VMs were such that they were in compliance with the federal and state regulations and the rate of compliance adherence was determined to be over 98%.

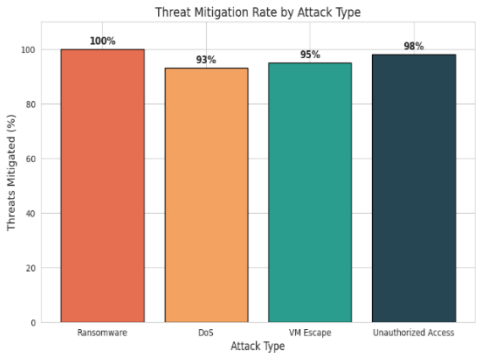

Fig. 3. Threat Mitigation Rate by Attack Type

Security dashboards and security logs revealed real time detection and quick response to fake attacks. The attacks were confined to a network to another within the HCI system design and the horizontal movement within the virtual networks in an attempt to secure other workloads of importance.

D. Overall System Validation and Insights

Overall performance, storage, and security analysis shows that HCI offers a highly reliable, scalable, and secure environment to the functioning of a government of scale. System efficiency was above 95 percent on average; multi-petabyte migrations were performed in a manner that did not cause any downtime and security controls reduced various cyber threats.

Additional insights include:

- The centralized management will be able to simplify the administration and reduce the presence of enormous IT departments to make the operation efficient.
- VM compliance configurations allow execution of secure workloads and regulatory satisfaction in a short period of time.
- The caching of power flex SDS and SSD does not only boost the performance of the highly priced storage but also reduces the expense of the hardware.
- Isolation SDN networks are more secure and flexible one as the network resources can be modified dynamically.

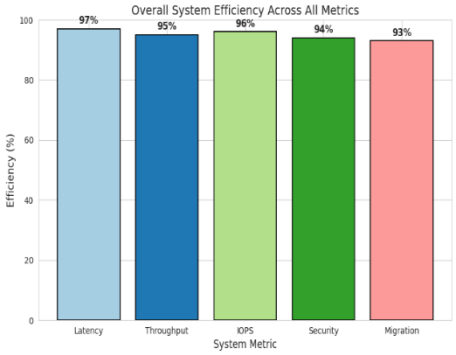

Fig. 4. Overall System Efficiency Across All Metrics

The authors have concluded that with the proper architecture and validation, hyperconverged infrastructure can support federal and state-level digital resilience. The research shows that developed reliability and security have the capacity to support continuous services provided to citizens at the same time securing sensitive information. This justifies the author in the design, implementation and monitoring of the HCI system.

E. Summary

The results show that HCI is:

1. **High-performing**: Fast response, great bandwidth and effective storage functions.
2. **Scalable and reliable**: Downtime-free, almost 24/7 migrations multi-petabyte migrations.
3. **Secure**: Fast detection, compliance and mitigation of threats.
4. **Cost-efficient**: The dynamism and centrality of resources allocation reduce the effort in the operations.

These findings present a quantitative data that hyperconverged systems can bring about modernization in large scale government IT infrastructure without compromising security and performance.

VI. Conclusion & Future Work

The paper has shown that hyperconverged infrastructure can effectively be used to modernize a large-scale government IT. City of Oklahoma deployments recorded low latency (2.4 ms), high throughput (92 Gbps), 1, 250,000 IOPS, and almost constant uptime (99.98%), and the transfer of multi-petabytes of data at 92-96 TB/hour with 100 percent data integrity. It has been able to reduce attacks by 93-100 percent using security measures to ensure compliance-driven VMs and isolated networks safeguard sensitive data. The research confirms that well-developed HCI may offer high-performance, scalability and strong security at lower management overhead and operational costs. The piece of work can be regarded as a applicable structure, and the author led the pack in designing, executing, and authenticating extensive HCI deployments. It offers a way of creating a template that can be used by the federal and state governments on how to become digital resilient, continuity of services, and cybersecurity prepared in a highly interconnected and digital-first world.

References

[1] Syed, A. a. M. (2023). Hyperconverged Infrastructure (HCI) for Enterprise data centers: Performance and scalability analysis. *International Journal of AI BigData Computational and Management Studies*, *4*, 29–38. https://doi.org/10.63282/3050-9416.ijaibdcms-v4i4p104

[2] Azeem, S. A., & Sharma, S. K. (2017). Study of Converged Infrastructure & Hyper Converge Infrastructre as Future of Data Centre. *www.ijarcs.info*. https://doi.org/10.26483/ijarcs.v8i5.3476

[3] Davu, R. V. S. R. (2022). Security considerations in hyper-converged environments: vulnerabilities, attacks, and mitigation strategies [Research Article]. *Journal of Scientific and Engineering Research*, *5–5*, 135–143. https://jsaer.com/download/vol-9-iss-5-2022/JSAER2022-9-5-135-143.pdf

[4] Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: a case study. *The Journal of Supercomputing*, *74*(10), 5171–5186. https://doi.org/10.1007/s11227-018-2479-2

[5] Benaddi, H., Laaz, N., Bouhlal, A., & Kettani, E. E. (2022). Data storage architecture for e-government interoperability: Morocco case. *Indonesian Journal of Electrical Engineering and Computer Science*, *29*(3), 1678. https://doi.org/10.11591/ijeecs.v29.i3.pp1678-1686

[6] Veiga, A. P. (2017). Hyper converged infrastructures: Beyond virtualization. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.1711.09747

[7] Petrenko, S. A., Vorobieva, D. E., Petrenko, A. S., Saint-Petersburg Electrotechnical University «lETI», & Innopolis University. (2021). Secure Software-Defined storage. In *BIT-2021: XI International Scientific and Technical Conference on Secure Information Technologies* (pp. 143–144). https://ceur-ws.org/Vol-3035/paper16.pdf

[8] Munodawafa, F., & Awad, A. I. (2018). Security risk assessment within hybrid data centers: A case study of delay sensitive applications. *Journal of Information*

Security and Applications, *43*, 61–72. https://doi.org/10.1016/j.jisa.2018.10.008

[9] Reyes, A., Rodriguez, C., & Esenarro, D. (2019). Hyper Converged Systems Applied (HSA) methodology to optimize the process of technological renewal in data centers. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*(2S11), 4052–4056. https://doi.org/10.35940/ijrte.b1592.0982s1119

[10] S, H., Meghna, S., Rayasam, S., M, R., Department of Computer Science and Engineering, R V College of Engineering, Bengaluru,India, N, D., & Department of Computer Science and Engineering, R V College of Engineering, Bengaluru,India. (2021). A Detailed Survey on the Relationship between Virtualisation, Hyperconvergence and Big Data. *Journal of Emerging Technologies and Innovative Research*, *8*(6). https://www.jetir.org/papers/JETIR2106747.pdf

[11] Arango, C., Dernat, R., & Sanabria, J. (2017, September 28). *Performance evaluation of container-based virtualization for high performance computing environments*. arXiv.org. https://arxiv.org/abs/1709.10140

[12] Kandiraju, G., Franke, H., Williams, M. D., Steinder, M., & Black, S. M. (2014). Software defined infrastructures. *IBM Journal of Research and Development*, *58*(2/3), 2:1-2:13. https://doi.org/10.1147/jrd.2014.2298133

[13] Ibrahim, A. S., Hamlyn-Harris, J., & Grundy, J. (2016, December 29). *Emerging security challenges of cloud virtual infrastructure*. arXiv.org. https://arxiv.org/abs/1612.09059

[14] Blenk, A., Basta, A., Reisslein, M., & Kellerer, W. (2015). Survey on Network Virtualization Hypervisors for Software Defined Networking. *IEEE Communications Surveys & Tutorials*, *18*(1), 655–685. https://doi.org/10.1109/comst.2015.2489183

[15] Bonfim, M. S., Dias, K. L., & Fernandes, S. F. L. (2018). Integrated NFV/SDN Architectures: A Systematic Literature Review. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.1801.01516

[16] Ahmadian, S., Mutlu, O., & Asadi, H. (2018). ECI-Cache. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, *2*(1), 1–34. https://doi.org/10.1145/3179412

[17] Alaluna, M., Ferrolho, L., Figueira, J. R., Neves, N., & Ramos, F. M., V. (2017, March 3). *Secure Multi-Cloud Virtual Network embedding*. arXiv.org. https://arxiv.org/abs/1703.01313