Smart City Insights

www.journal-sci.com

Smart City Ins. Vol. 1, No. 1 (2024) 34–42.

Paper Type: Original Article

Cloud Security and Virtualization

Priyanshu Su Panda[1,*], Om Priyadarshan[1], Lokesh Dash[1]

[1] School of Computer Engineering, KIIT Deemed to Be University, Bhubaneswar-751024, Odisha, India; 2105395@kiit.ac.in; 2105386@kiit.ac.in; 2105380@kiit.ac.in.

Citation:

Received: 8 August 2023 *Revised: 6 October 2023* *Accepted: 4 April 2024*	Panda, S. P., Priyadarshan, O., & Dash, L. (2024). Cloud security and virtualization. *Smart city insights, 1*(1), 34-42.

Abstract

As organizations increasingly adopt cloud computing and virtualization technologies to enhance flexibility, scalability, and cost-efficiency, concerns about security have become paramount. This abstract explores the intersection of cloud security and virtualization, addressing the challenges and strategies for ensuring robust data protection in this dynamic environment. The paper delves into the unique security risks posed by cloud computing and virtualization, including data breaches, unauthorized access, and compliance issues. It discusses the importance of implementing comprehensive security measures, such as encryption, access controls, and intrusion detection systems, to safeguard sensitive data across cloud and virtualized environments. Furthermore, the abstract examines emerging trends and technologies, such as containerization and software-defined networking, that offer enhanced security capabilities for mitigating risks in the cloud. By understanding and addressing these challenges, organizations can leverage the benefits of cloud computing and virtualization while maintaining the highest standards of data security and privacy.

Keywords: Security, Cybersecurity, Virtual.

1 | Introduction

The growth of cloud computing has raised the need for information security and left some other non-traditional security hazards. There is a pressing requirement for an intensified research effort into technology that can enhance security measures in various types of cloud computing applications, thereby supporting infrastructure, goods, and technologies meant to provide safety. Many products offer cloud computing [1]. The rapid growth of centralized computing has meant that information security is undoubtedly a vital issue, and some new types of insecurity have emerged. Research must be done to create more secure cloud-based services for companies to use. This will help to support the technology, infrastructure, and security goods for cloud computing applications as well as services. Some global Information Technology (IT) enterprises have unveiled many products based on cloud computing, but it still poses considerable security challenges [1]. It has experienced few cases of breaches; furthermore, the term' cloud computing' itself has become common among people who are increasingly enlightened about it. Today, when using or moving towards clouds, there are mostly security issues that attract attention more than ever before, hence becoming the greatest problem

Corresponding Author: Priyanshu Su Panda

now. Without resolving this problem, the cloud would not help industries transform or upgrade applications easily. Therefore, studies should be carried out in the field of cloud computing security with great practical significance. These problems include increased threat levels because of the proliferation of computing within organizations and accompanying sensitive data movement trends; besides, system administrators cannot know all the objects on their network ultimately since devices like tablets keep emerging every day [2]. This is due to a few security incidents, as well as the widespread adoption of the cloud computing concept and people's growing awareness of it. As a result, security is now the most significant concern when using cloud computing or migrating to the cloud. This problem is not solved; cloud computing would be complicated for industrial upgrading and applications. Therefore, cloud computing security research has important practical significance.

1.1 | Cloud Security

Cloud security is provided as a service. Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) are examples of services that have emerged because of XaaS. In today's world, cloud computing is a significant factor that contributes to the development of the industry and other sectors. This is an emerging field that has been explored from several viewpoints, including SOA, service-oriented architectures, and cloud virtualization. Cloud computing is an emerging field in which computing services are available as internet-based services. This is emerging, but it comes with some issues and challenges. Whenever it comes to data theft, this is an area of concern.

1.2 | Virtualization

Virtualization has become important again in improving system security and helping deliver the value of cloud computing. It enables businesses to reduce IT costs while increasing the efficiency, utilization, and flexibility of their existing computer hardware. Academics focus on cloud computing security and have hosted worldwide conferences on the topic. Our expertise includes cloud computing research, deployment, policy, and security. Berkeley cloud computing white paper problems list the consequences faced [2]. The paper [3] covered cloud storage, put forth concepts for a cloud storage system's architecture and touched on pertinent problems, like storage security, but it omitted the necessary remedy. The articles covered the problems with cloud computing's privacy, security, and credibility, as well as some potential solutions to boost trust and security. The adoption of cloud Infrastructure-as-a-Service (IaaS) is hampered by multi-tenancy, in which numerous tenants share the underlying physical infrastructure provided by a cloud service provider. In the context of a public cloud, a tenant could be an enterprise, whereas, in the case of a private cloud, it could be a department inside a business. Virtualization technology enables the service provider to save costs by delivering virtualized hardware resources like virtual machines, virtual storage, and virtual networks as a service to multiple tenants. For example, a tenant's virtual machine may be hosted on the same physical server as that of many other tenants. It is well known that the isolation of the execution environment provided by hypervisors, which enable virtualization technology, has various disadvantages [4].

Experts have also directed their focus to cloud computing security, hosting multiple international conferences on the subject and conducting research on cloud computing technology, deployment, policy, and security concerns. Ten obstacles and possibilities related to cloud computing have been listed in the Berkeley cloud computing paper [3]. Bijon et al. [4] discussed cloud storage, put out concepts for a cloud storage system's construction, and touched on pertinent problems, including storage safety, but it omitted the necessary remedy. The papers covered the problems with cloud computing's privacy, security, and credibility, as well as some potential solutions for improving trust and security. A quantitative approach to risk assessment and the security effects of cloud computing was provided in the article [3]. In this paper, we will survey and verify cloud security and virtualization, their impact on security, and future possibilities. We present the details of cloud security solutions as well as virtualization, highlighting their features, advantages, potential security problems, and flaws, with a focus on their deployment in the cloud. I am also looking forward to correcting the flaws and trying to come up with the solution needed for the deployment soon.

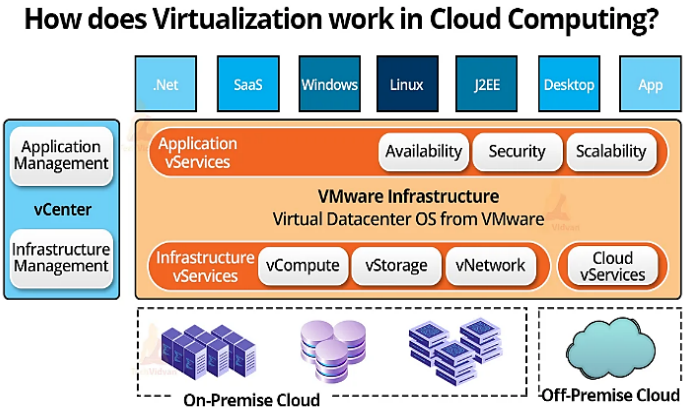

Fig. 1. Virtualization with cloud computing.

2 | Literature Review

Cloud security is a set of policies, strategies, controls, procedures, and practices designed to protect the data, resources, and applications hosted on the cloud from various threats. Cloud security entails multiple aspects, such as data center security, access control, threat prevention, detection and mitigation, redundancy, legal compliance, and cybersecurity policy. Virtualization technology has been adopted at a significant level by many data centers in the industry. It provides benefits like server consolidation, live migration, data security, and less power consumption. At the same time, storage virtualization abstracts physical storage (SAN, NAS) resources from front-end applications running in the system. Storage virtualization is helpful for maintaining large volumes of data with a continuous backup facility. Bele and Desai [5] look at the idea or concept of virtualization beyond mere server virtualization and give us other lines to explore when looking at the value of virtualization overall. Any technology that really permeates the market typically can perform multiple functions but is usually part of a larger technology. The main research questions addressed by the literature review are:

I. What are the benefits of cloud security for organizations and users?

II. What are the main challenges and risks associated with cloud security?

III. What are the current and future developments and trends in cloud security?

Identification of cloud security as:

I. Security democratization: cloud security enables organizations to access advanced security solutions and services without requiring extensive resources or expertise.

II. Continuous visibility: cloud security provides organizations with real-time monitoring and reporting of their cloud assets and activities, enhancing their situational awareness and accountability.

III. Increased resiliency: cloud security enhances the availability and reliability of cloud services and resources, reducing the impact of disruptions and disasters.

IV. Comprehensive defense: loud security offers a holistic and multi-layered approach to protect cloud assets from a wide range of existing and emerging threats, such as DDoS attacks, malware infections, data breaches, and identity theft.

V. Automated regulatory compliance: cloud security helps organizations meet the legal and ethical requirements and standards of their industry and jurisdiction, reducing the risk of violations and penalties.

The cloud computing infrastructure's virtualization methods inherently provide a vulnerable surface. The following are the main security issues we can see in a cloud situation. Privilege user access: to reduce the

possibility of high privilege role abuse, only a small group of trustworthy users should be able to access sensitive data in the cloud. Reliability and availability: the cloud provider must build up an efficient replication and recovery strategy to restore services in the event of a security breach-lack of data/computation isolation: One instance of client data must be totally isolated from data belonging to other customers [6]. The autonomy of position in the way but to some extent position independence, that is, the user does not know and can't control their resource's physical location while in case some of them have a virtual position at the higher abstract levels such as country, state, province or data center. This word has many meanings because there are different books. There was no strict definition of virtualization during its formative stage, as it was usually used undefinedly. Virtualization is generally taken to be a method where computer components operate on a hypothetical base rather than a real one and can be seen as a solution for simplification of management and optimal usage of resources [7].

2.1 | Cloud Security Framework and Benefits

To start with, a cloud security architecture is an integrated set of guidelines and techniques on application and data protection aimed at organizations' ability to securely deploy and manage their applications and data in the cloud computing environment. A cloud security architecture is also capable of managing these issues, particularly due to the use of a cloud, such as the volatile nature of a setup that includes cloud-based elements, the evolving threat landscape, and the division of responsibility between service providers and their clients. Apart from that, by implementing cloud security architectures, organizations can meet industry-specific and jurisdiction-specific security requirements and comply with regulations [6]. There are different frameworks for cloud security, such as ISO/IEC 27017, CSA STAR, CIS, and MITRE ATT&CK, among others. Based on their scope, objectives, and approach, a particular framework may be most beneficial for cloud service suppliers' customers at different levels or types.

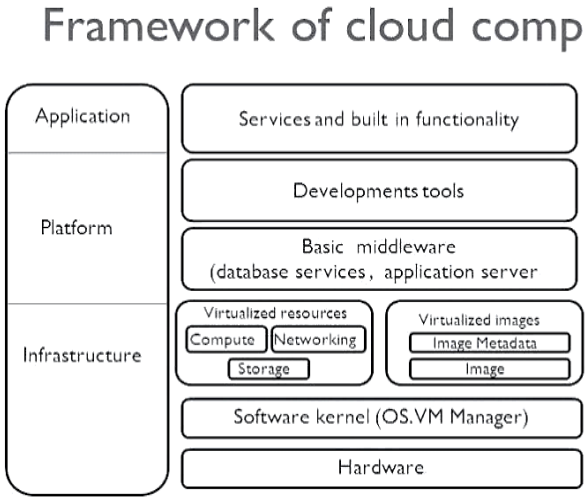

Fig. 2. Cloud computing framework.

Visibility cloud security enables organizations to monitor and report their cloud assets and activities in real time, enhancing their situational awareness and accountability. Higher availability of disasters. Effective attacks. Data mechanisms and pay cloud security allows organizations to access advanced security solutions and services without requiring extensive resources or expertise and only pay for what they use.

2.2 | Virtualization Framework and Access Control

The virtualization security framework is organized effectively into two modules: virtual system security and virtualization security management. Two modules perform their duties without disturbing each other so that the entire framework can be more efficient. The virtual system security consists of three layers [7]. the first layer is the physical resource layer. The second layer is VMM, which is the most essential layer that should be

heavily facilitated with security mechanisms to protect VMs from running. The top layer is VMs that provide virtualization services to consumers [8], [9]–[11].

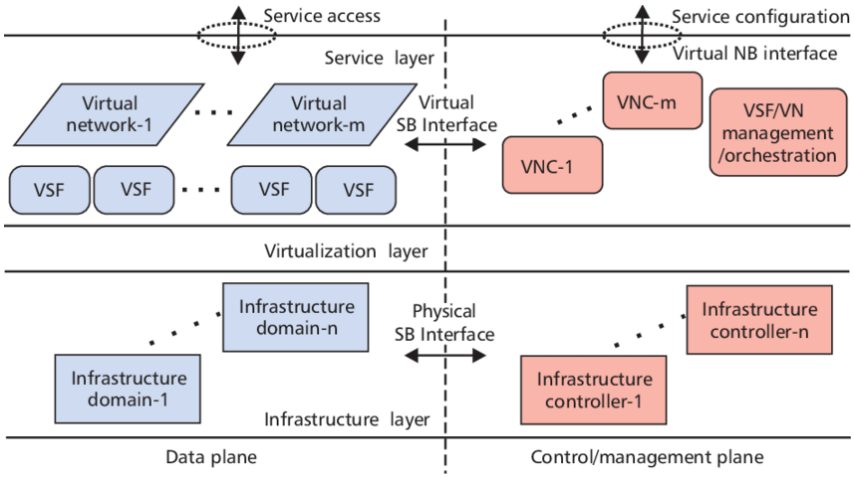

Fig. 3. Virtualization with cloud computing.

2.2.1 | Instruction set architecture level

It is an abstract model of a computer. It is also referred to as architecture or computer architecture. A realization of an Instruction Set Architecture (ISA) is called an implementation. An ISA permits multiple implementations that may vary in performance, physical size, and monetary cost (among other things) because the ISA serves as the interface between software and hardware. Software that has been written for an ISA can run on different implementations of the same ISA. This has enabled binary compatibility between different generations of computers to be easily achieved, as well as the development of computer families. Both developments have helped to lower the cost of computers and to increase their applicability. For these reasons, the ISA is one of the most essential abstractions [8], [12], [13].

2.2.2 | Hardware abstraction layer level

Virtualization at this level exploits the resemblance in guest architectures and host platforms to cut down the interpretation latency. The virtualization technique helps map the virtual resources to physical resources and use the native hardware for VM computations. When an emulated machine communicates the physical resources, the simulator takes over and multiplexes appropriately. It is performed on top of the bare hardware. This approach generates a VM in a virtual hardware environment. Computer resources such as processors, memory, and I/O devices are virtualized. The objective of this virtualization is to increase the hardware utilization by multiple users concurrently. Examples: Xen, VMware, VirtualBox, Virtual, Denali, User-Mode-Linux (UML), and Plex86 [14]–[16].

2.2.3 | Operating system level

Operating-system-level virtualization, also known as containerization, refers to an operating system feature in which the kernel allows the existence of multiple isolated user-space instances. Such instances, called containers, partitions, Virtualization Engines (VEs), or jails (FreeBSD jail or chroot jail), may look like real computers from the point of view of programs running in them. A computer program running on an ordinary operating system can see all resources (connected devices, files and folders, network shares, CPU power, quantifiable hardware capabilities) of that computer. However, programs running inside a container can only see the container's contents and devices assigned to the container [17], [18].

2.3 | Research Gap

In spite of notable progress in cloud computing and virtualization technologies, a significant gap in research persists concerning the intricate relationship between security measures and virtualized environments within cloud infrastructures. While current literature provides insights into general best practices for cloud security and virtualization methods, there's a scarcity of exploration into the specific complexities and vulnerabilities that arise when these two domains intersect. Furthermore, there's a noticeable absence of empirical studies evaluating the effectiveness of security controls tailored for virtualized cloud environments, which leaves organizations seeking guidance on securing their cloud deployments without practical direction. Moreover, the rapid evolution of cloud architectures and virtualization platforms introduces dynamic complexities that warrant further investigation. Emerging trends such as containerization, serverless computing, and edge computing add layers of complication to the security landscape, yet research efforts have yet to fully elucidate their implications on cloud security within virtualized contexts.

Additionally, there's a gap in research focusing on the socio-technical aspects of cloud security and virtualization, including factors such as human behavior, organizational culture, and governance frameworks in mitigating security risks. Closing these research gaps is critical for developing comprehensive strategies to secure cloud-based systems leveraging virtualization technologies effectively. Future research endeavors should prioritize empirical studies that assess the efficacy of security measures tailored to virtualized cloud environments alongside interdisciplinary inquiries that consider both technical and socio-organizational dimensions of cloud security. By addressing these gaps, researchers can offer actionable insights to inform the design, implementation, and management of secure cloud infrastructures in an increasingly virtualized landscape.

In modern computing environments, cloud security and virtualization play crucial roles. Evaluating existing models is essential to effectively address security challenges. This paper presents a comparative analysis methodology for assessing these models.

2.3.1 | Review of existing models

Prominent models, frameworks, and approaches for cloud security and virtualization are identified and reviewed. Notable examples include the Cloud Security Alliance (CSA), Cloud Controls Matrix (CCM) [19], NIST Special Publication 800-144 [20], and ISO/IEC 27017 [8]. Each model's essential features, strengths, and limitations are summarized. Criteria for evaluating model effectiveness and suitability are defined. Factors such as comprehensiveness, scalability, adaptability to different cloud architectures, and alignment with industry standards and best practices are considered. Stakeholder and expert feedback are incorporated. A systematic comparison of identified models is conducted based on evaluation criteria. Key features, strengths, and weaknesses are compared side-by-side, highlighting similarities and differences in approach, scope, and applicability. Case studies or real-world examples illustrating model applications in various cloud environments are included. Practical considerations, such as implementation challenges, resource requirements, and organizational readiness, are discussed. The effectiveness of each model in addressing specific security concerns and mitigating risks is analyzed. Gaps and limitations in existing models are identified based on the comparative analysis. Opportunities for improvement and enhancement to address emerging threats and technological advancements are explored. Recommendations for future research directions and model development are proposed. The findings of the comparative analysis are summarized, providing insights into existing model strengths and weaknesses. Recommendations are offered for organizations seeking to select or adapt models for their cloud security initiatives.

3 | Findings from Analysis

The comparative analysis of existing models for cloud security and virtualization revealed several key insights into the strengths, weaknesses, and applicability of different approaches:

I. Cloud security models: the review highlighted diverse frameworks such as ISO/IEC 27017, CSA STAR, CIS, and MITRE ATT&CK, each offering unique perspectives on cloud security architecture and benefits. While ISO/IEC 27017 emphasizes industry-specific security requirements and regulatory compliance, CSA STAR focuses on transparency and assurance in cloud service provider evaluations. CIS offers prescriptive security controls, whereas MITRE ATT&CK focuses on adversary tactics and techniques. Understanding the scope, objectives, and approach of these frameworks is crucial for organizations to select the most suitable model based on their specific needs and requirements.

II. Benefits of cloud security: the analysis underscored the multifaceted benefits of cloud security, including visibility, higher availability, adequate protection against DDoS attacks, data security, and pay-as-you-go flexibility. Cloud security enables organizations to access advanced security solutions without requiring extensive resources or expertise, enhancing their ability to meet legal and ethical requirements while reducing the risk of violations and penalties [21], [22].

III. Virtualization security frameworks: in exploring virtualization security, the study identified the importance of effective organization and management, mainly through virtual system security and virtualization security management modules. Understanding the layers of virtualization, from the physical resource layer to VMs, is essential for implementing robust security mechanisms to protect against vulnerabilities and threats [23], [24].

IV. Levels of virtualization: the analysis delved into different levels of virtualization, including ISA Level, Hardware Abstraction Layer (HAL) level, and operating system level. Each level offers distinct advantages and challenges, from binary compatibility and performance to hardware utilization and resource allocation. Examples such as Xen, VMware, and containerization technologies showcase the diversity of virtualization approaches available to organizations [25].

V. Implications for research and practice: these findings have a significant impact on both research and practice in cloud security and virtualization. By understanding the strengths and weaknesses of existing models and frameworks, organizations can make informed decisions when selecting, implementing, and managing cloud security measures. Future research should focus on addressing gaps in current approaches, exploring emerging trends and technologies, and advancing the state-of-the-art in cloud security and virtualization [26].

In conclusion, the comparative analysis provides valuable insights into the complexities and opportunities inherent in cloud security and virtualization. By leveraging these findings, organizations can enhance their security posture and resilience in an increasingly digital and interconnected landscape.

4 | Conclusion

In conclusion, the comprehensive review of cloud security models and virtualization frameworks illuminates the diverse landscape of approaches available to organizations seeking to fortify their digital infrastructure. The exploration of ISO/IEC 27017, CSA STAR, CIS, and MITRE ATT&CK frameworks underscores the importance of aligning security measures with industry-specific requirements, regulatory compliance, transparency, and adversary tactics. Moreover, the benefits of cloud security, including enhanced visibility, availability, protection against DDoS attacks, and flexible scalability, highlight its pivotal role in modern data protection strategies. Similarly, the examination of virtualization security frameworks emphasizes the necessity of robust organization and management, considering the layers and levels of virtualization. This synthesis not only informs decision-making processes for selecting suitable security models but also underscores the need for ongoing research and innovation in cloud security and virtualization. By addressing existing gaps, exploring emerging technologies, and advancing best practices, organizations can effectively navigate the evolving landscape of cybersecurity threats and challenges in the digital age.

References

[1] Etro, F. (2009). The economic impact of cloud computing on business creation, employment and output in Europe. *Review of business and economics*, *54*(2), 179–208.

[2] Baiardi, F., Maggiari, D., Sgandurra, D., & Tamberi, F. (2009). Transparent process monitoring in a virtual environment. *Electronic notes in theoretical computer science*, *236*, 85–100. https://doi.org/10.1016/j.entcs.2009.03.016

[3] Virtualization, A. (2005). *Secure virtual machine architecture reference manual*. AMD publication. https://0x04.net/~mwk/doc/amd/33047.pdf

[4] Bijon, K., Krishnan, R., & Sandhu, R. (2015). Mitigating multi-tenancy risks in IAAS cloud through constraints-driven virtual resource scheduling. *Proceedings of the 20th ACM symposium on access control models and technologies* (pp. 63–74). Association for Computing Machinery. https://doi.org/10.1145/2752952.2752964

[5] Bele, R., & Desai, C. (2012). Review on virtualization: In the light of storage and server virtualization technology. *Journal of information and operations management*, *3*(1), 245-260.

[6] Brasser, F., Capkun, S., Dmitrienko, A., Frassetto, T., Kostiainen, K., & Sadeghi, A. R. (2017). *DR. SGX: hardening SGX enclaves against cache attacks with data location randomization*. https://doi.org/10.48550/arXiv.1709.09917

[7] Cazalas, J., McDonald, J. T., Andel, T. R., & Stakhanova, N. (2014). Probing the limits of virtualized software protection. *Proceedings of the 4th program protection and reverse engineering workshop* (pp. 1–11). Association for Computing Machinery. https://doi.org/10.1145/2689702.2689707

[8] International organization for standardization (ISO). (2015). *ISO/IEC 27017:2015 - Information technology -- security techniques -- code of practice for information security controls based on ISO/IEC 27002 for cloud services*. https://www.iso.org/standard/43757.html

[9] Luo, S., Lin, Z., Chen, X., Yang, Z., & Chen, J. (2011). Virtualization security for cloud computing service. *2011 international conference on cloud and service computing* (pp. 174–179). IEEE. https://doi.org/10.1109/CSC.2011.6138516

[10] Mohapatra, H., & Rath, A. K. (2019). Fault tolerance in WSN through PE-LEACH protocol. *IET wireless sensor systems*, *9*(6), 358–365.

[11] Bele, S., & Desai, D. (2012). Exploring the concept of virtualization beyond server virtualization. *Journal of cloud computing: advances, systems and applications*, *1*(1), 1–17.

[12] Hu, Y., Li, T., Yang, P., & Gopalan, K. (2013). An application-level approach for privacy-preserving virtual machine checkpointing. *2013 IEEE sixth international conference on cloud computing* (pp. 59–66). IEEE. https://doi.org/10.1109/CLOUD.2013.28

[13] Mohapatra, H., & Rath, A. K. (2019). Detection and avoidance of water loss through municipality taps in India by using smart taps and ICT. *IET wireless sensor systems*, *9*(6), 447–457.

[14] Jansen, W., Grance, T., & others. (2011). Guidelines on security and privacy in public cloud computing. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-144.pdf

[15] Bhalotia, N., Kumar, M., Alameen, A., Mohapatra, H., & Kolhar, M. (2023). A helping hand to the elderly: securing their freedom through the HAIE framework. *Applied sciences*, *13*(11), 6797. https://doi.org/10.3390/app13116797

[16] Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud security and privacy: an enterprise perspective on risks and compliance*. O'Reilly Media, Inc. https://books.google.com/books?id=BHazecOuDLYC&dq

[17] Mohapatra, H. (2021). Socio-technical challenges in the implementation of smart city. *2021 international conference on innovation and intelligence for informatics, computing, and technologies (3ICT)* (pp. 57–62). IEEE https://doi.org/10.1109/3ICT53449.2021.9581905

[18] Mohapatra, H., & Mishra, S. R. (2024). Unlocking insights: exploring data analytics and AI tool performance across industries. In *Data analytics and machine learning: navigating the big data landscape* (pp. 265–288). Springer. https://link.springer.com/chapter/10.1007/978-981-97-0448-4_13

[19] Mohapatra, H., & Rath, A. K. (2019). Fault tolerance through energy balanced cluster formation (EBCF) in WSN. *Smart innovations in communication and computational sciences: proceedings of icsiccs-2018* (pp. 313–321). Springer.

[20] National Institute of Standards and Technology (NIST). (2011). *NIST special publication 800-144: guidelines on security and privacy in public cloud computing*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

[21] Mohapatra, H., & Rath, A. K. (2020). Survey on fault tolerance-based clustering evolution in WSN. *IET networks*, *9*(4), 145–155.

[22] Pearson, S. (2013). Privacy, security, and trust issues arising from cloud computing. In *Cloud computing* (pp. 357–388). Springer.

[23] Mohapatra, H., & Rath, A. K. (2022). IoE based framework for smart agriculture: networking among all agricultural attributes. *Journal of ambient intelligence and humanized computing*, *13*(1), 407–424. DOI:10.1007/s12652-021-02908-4

[24] Hoopes, J. (2009). *Virtualization for security: including sandboxing, disaster recovery, high availability, forensic analysis, and honeypotting*. Syngress.

[25] Rath, A. K., & Mohapatra, H. (2020). *Fundamentals of software engineering designed to provide an insight into the software engineering concepts.* Bpb Publications.

[26] Niyaz, Q., Sun, W., Zhang, Y., & Choo, K. K. R. (2018). A survey of virtualization-based security solutions for cloud computing. *Journal of network and computer applications*, *96*, 1–16.