Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2024, 11(9):87-94

Research Article ISSN: 2394 - 658X

A Comprehensive Review on Security and Privacy Properties in Cloud-Based Business and Scientific Workflows

Vedaprada Raghunath

IT Director, IMR soft LLC, USA.
vedapradaphd@gmail.com

ABSTRACT

The ability of cloud computing to supply an enormous amount of computer resources on demand has contributed to its rising popularity. This is because there has been a meteoric rise in the number of data-and computation-intensive applications, including scientific and business workflows, in the last several years. Security concerns are a major roadblock to the broad adoption of cloud computing, particularly for workflows that deal with sensitive information and processes. This paper provides a comprehensive overview of current practices for handling security and privacy issues in cloud-based scientific and business workflows. We also point out where the existing corpus of knowledge in this area is lacking or inadequate. First, within the framework of this extensive literature review, we will present state-of-the-art security solutions organized according to the stages of the scientific and business process workflow life cycles that they are intended to address. According to the results, most of the literature focuses on the planning and implementation stages, whereas the evaluation and adjustment stages are under-discussed in a few of articles. As a result, there is a significant knowledge gap in the area of cloud-based workflows that pertains to the detection, prevention, and response to security violations.

Keywords: Cloud, scientific workflows, privacy issues.

INTRODUCTION

Due to its unparalleled adaptability, scalability, and cost-effectiveness, cloud computing has completely transformed the way organizations operate. Businesses across many different industries have begun using cloud computing in an effort to save costs, boost collaboration, and speed up innovation. But, the inherent complexity of ensuring the security of sensitive data and resources stored and processed on the cloud comes with the widespread adoption of cloud services. Because cyber threats are always becoming more complex and more common, it is crucial to protect cloud systems from unauthorized access, data breaches, and other security risks.

Within the scope of this article, we will investigate the most effective methods for safeguarding your cloud infrastructure. Data encryption, IAM, network security, compliance issues, and proactive threat mitigation strategies are just a few of the important subjects that will be covered by these approaches. Firms may strengthen their cloud infrastructures and reduce cloud computing risks by implementing strong security measures and adhering to industry standards. Businesses are able to safeguard critical assets in this way, ensuring their availability, confidentiality, and integrity.

It is impossible to overstate the significance of cloud computing in the operations of modern businesses, as it has completely altered the way in which organizations carry out their activities and make use of technology. There are a number of important elements that contribute to the significance of cloud computing: One advantage of cloud computing is its scalability, which lets companies quickly modify their resource consumption in reaction to fluctuations in demand.

Because of this flexibility, enterprises are able to manage fluctuations in workload without having to make significant investments in infrastructure or hardware. Due to its pay-as-you-go model, cloud computing allows companies to save money by only paying for the resources they use.

Because of this, there is no longer a requirement for making substantial initial investments in hardware, and the continuous operational costs that are connected with maintenance and upgrades are reduced. Accessing cloud

services is feasible from any place with an internet connection. Because of this, workers may communicate and interact with one another remotely, no matter their physical location. The availability of this data enhances adaptability and efficiency in modern workplaces.

Machine learning, artificial intelligence, big data analytics, and the Internet of Things (IoT) are just a few examples of the state-of-the-art technologies and services made available to customers through cloud computing. With these skills, businesses are able to empower themselves through innovation, creating new goods, services, and business models. In the case of unexpected interruptions or catastrophes, cloud computing's complete backup and recovery solutions will keep business operations running smoothly and data will be resilient.

Cloud-based backups make it possible for businesses to recover data quickly and reduce the amount of time they are down. Computing on the cloud speeds up the process of developing and deploying applications and services, which in turn reduces the amount of time it takes to bring new goods and projects to market. Also, cloud computing increases agility.

The use of cloud infrastructure makes agile development approaches and DevOps processes easier to use, which in turn enables quick iteration and deployment. Safety and Regulatory Compliance: Cloud computing companies make significant investments in sophisticated security measures, compliance certifications, and data protection methods, despite the fact that security issues should be taken into consideration. Establishing a partnership with cloud service providers that have a solid reputation can help enterprises improve their security posture and guarantee that they are in compliance with regulatory standards. In general, cloud computing has evolved into a vital tool for contemporary firms that wish to maintain their competitive edge, innovate, and adjust to the ever-shifting dynamics of the market. It has become an integral part of contemporary companies' operations due to its scalability, affordability, accessibility, and ability to encourage innovation. The importance of cloud computing security is skyrocketing due to the increasing number of organizations migrating their activities to cloud environments.

Although cloud computing presents a number of advantages, such as scalability, cost-effectiveness, and accessibility, it also presents a number of obstacles that are not seen in other forms of computing.

Concerns about data privacy and integrity preservation and cyber-attack prevention arise when infrastructure management and maintenance rely on third-party cloud service providers. Protecting sensitive data, reducing risks, and maintaining stakeholder confidence in cloud settings requires the deployment of rigorous security measures, which must be guaranteed in this scenario. This study delves into the importance of cloud computing security by examining the most pressing concerns and recommending solutions for effectively protecting cloud infrastructures. Enterprises must proactively address security concerns if they want to fully utilize cloud computing's potential while minimizing risks and maintaining the availability, confidentiality, and integrity of their data and resources.

Because the cloud computing security landscape is complicated and constantly evolving, businesses that use cloud services have their own particular set of issues.

In cloud environments, the dynamic nature of risks is caused by a number of variables, including the following: The most serious dangers to cloud computing are data breaches, which are one of the most common types of data breaches. Sensitive data that is kept in the cloud is the target of attackers. Personal information (PII), financial details, and intellectual property are all part of this data set.

Storage in the cloud that has been improperly set, access restrictions that are inadequate, or vulnerabilities in cloud applications can all lead to breaches. There is a considerable risk to cloud security posed by insider threats. This is because authorized users with access to cloud resources can jeopardize data's secrecy, integrity, or availability, either on purpose or by accident.

An insider threat can emerge from an unhappy employee, an act of carelessness, or the use of stolen credentials. Cloud infrastructures are vulnerable to malware and ransomware infections, which can compromise data and halt operations. Cloud applications, email attachments, and hacked user accounts are common vectors for malware distribution, and ransomware is a kind of cloud-based encryption that demands payment to decrypt data. When malicious actors get unauthorized access to credentials or cloud accounts, they have committed account compromise. This is also known as unauthorized access or account hijacking. Compromised accounts pose a significant risk to the security of cloud services used by organizations since they can be utilized for stealing data, launching attacks, or committing fraud. The goal of a distributed denial of service (DDoS) assault is to make cloud services and infrastructure unavailable to consumers by flooding them with malicious traffic.

Websites, apps, and services hosted in the cloud are vulnerable to distributed denial of service (DDoS) assaults, which can cause outages, monetary losses, and brand harm. Cloud service providers and third-party vendors are the targets of supply chain attacks, which aim to obtain access to customers' cloud environments by exploiting security holes in their systems or software. Security issues, such as data breaches, can occur when cloud services are compromised due to assaults on the supply chain.

Organizations running in the cloud have a substantial risk of not complying with data protection legislation and industry standards. Failing to comply with regulations like GDPR, HIPAA, or PCI DSS can lead to monetary fines, legal ramifications, and harm to one's reputation. To effectively mitigate these risks, organizations should

incorporate robust cloud security measures such as encryption, multi-factor authentication, threat detection, and incident response planning into their overall security strategy.

Cloud environments must also undergo regular audits, compliance checks, and security assessments to guarantee their continued security and compliance. Successful cloud data, application, and infrastructure security requires an awareness of the dynamic threat landscape and the adoption of preventative security measures. Data encryption is crucial for the security of data in cloud computing environments since sensitive information is processed, stored, and transported across decentralized infrastructure.

Data can be rendered unreadable to unauthorized persons by converting it from plaintext to ciphertext using cryptographic methods and keys. To avoid data breaches, insider threats, and snooping eyes, data encryption is essential in cloud computing.

When thinking about cloud data encryption, there are some important factors to keep in mind: Encrypting data while it is in transit or at rest is known as data-at-rest encryption. This method is appropriate for databases, object storage, and file systems that are located in the cloud. Encryption makes sure that no one, not even those with the necessary decryption keys, can read the encrypted data, even if they manage to breach the storage infrastructure itself. Many cloud providers have encryption capabilities already built in, so businesses may encrypt data while it's in transit or at rest in a transparent way that doesn't affect performance or usability. Protecting data while it travels over networks from cloud storage to endpoints to users is the job of data-in-transit encryption. Data encryption during transmission is a standard practice, with protocols like Secure Sockets Layer (SSL) and Transport Layer Security (TLS) providing extra protection from prying eyes. To protect private information while it travels over the Internet or other public networks, secure communication methods are a must. Important Executives: To guarantee the safety and authenticity of encrypted data in cloud settings, efficient key management is essential.

LITERATURE REVIEW

Clients of all sizes can reap the benefits of cloud computing, which is rapidly becoming one of the most popular subfields in the IT industry.

This is one of the most important factors that enables a great number of businesses and organizations. Computing in the cloud is quite popular in the modern era because it provides a wide variety of services at prices that are accessible. [1-5] Cloud solutions also have the advantages of being more accessible, not requiring contracts for an extended period of time, and being easily scalable to meet the changing demands of businesses. No matter how many benefits cloud computing offers, it is not without its share of problems and downsides.

Currently, there are ongoing research projects that are being conducted in order to find solutions to the many problems that cloud computing is currently facing [6-11].

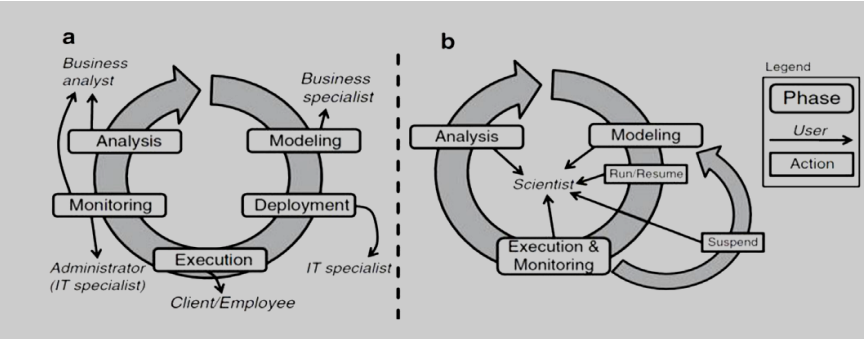

Figure 1. *(a) Business Workflow Life Cycle (b) Scientific Workflow Life Cycle.*

As seen in Figure 1, the domains' respective workflow life cycles take a somewhat different approach. In corporate settings, processes are viewed as software objects that may be accessed and used by distinct user roles. These roles often handle different aspects of the workflows' administration, such as modeling, execution, assessment, and monitoring. [12-15] On the other hand, the scientist is at the core of scientific workflows, as they are the ones who use and oversee the software artifacts.

And be aware that the business process life cycle will be the primary framework for our research because it is more comprehensive and allows for a more thorough examination of the current literature [12-16]. The TLR described in [13] has reviewed the literature by outlining the components necessary to secure scientific processes while they are being executed, naming various domains where security is crucial, and highlighting potential security risks. [17--19] The scientific workflow's scheduling step is the exclusive subject of the paper. The safety issues with scheduling resources have been examined in [20-22]. The authors classified the many types of security constraints into three categories: data, data center, and infrastructure. Each category was then assigned a model.

The scheduling phase is the sole subject of this paper. Some of the goals of these literature studies are distinct, while others do not attempt to address every stage of the workflow life cycle.[23] It follows that the whole workflow life cycle has not been adequately examined to determine how the privacy and security issues of cloud-based workflows affect the WfMS architecture.

Workflow Life Cycle and Security

Figure 2 depicts the entire workflow life cycle, including the adaptation phase. In addition, it shows how the chosen papers in the SLR address security and privacy issues at each stage of the workflow, classified by kind of workflow. It is clear from the figure that most of the studies focused exclusively on the scientific workflow execution phase. In contrast to the abundance of literature on commercial workflows, which mostly focuses on this stage, the security and privacy requirements of scientific workflows during the modeling and IT refinement stages have received surprisingly little attention.

Scientists often fail to differentiate between process models and actual executions, which is a contributing factor. The modeling and execution steps are not strictly sequenced since their workflows are developed through trial and error [24]. There is a lack of information in the literature regarding the different phases of the life cycle and how to model or specify the security needs in scientific workflows.

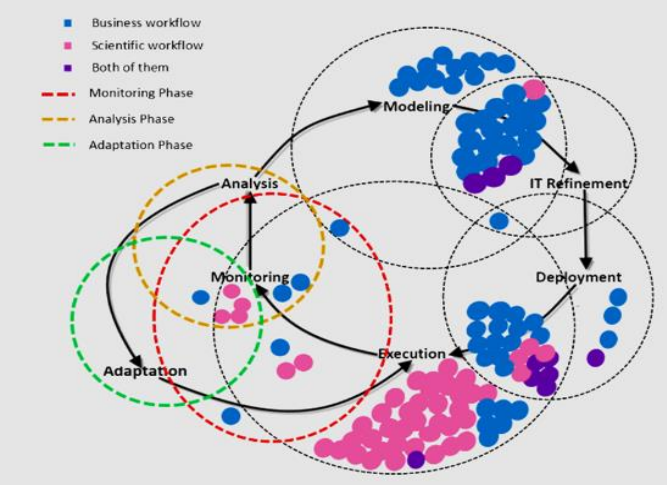

Figure 2: *Ensuring the security and privacy of workflows throughout their life cycles*

.

Also, as shown in Figure 2, most of the research on scientific and commercial workflows has concentrated on security during the modeling and execution phases, which leaves a lot of room for improvement when it comes to cloud workflow adaptation, analysis, and monitoring. In particular, we were unable to locate any published work that offered a solution to the problem of how to modify active business workflow instances in response to security breaches. Most papers that discuss the modeling phase—which usually also involves IT refinement—have focused on ways to extend modeling tools and languages so that user security requirements can be specified and captured at many levels of abstraction. Several of them build extensions to the widely used BPMN (Business Process Model and Notation) to make it easier to declare non-functional requirements, such as security.

These studies added security characteristics to BPMN diagrams using graphical user interfaces or textual notations [16,25].

Diagnostic

Security breaches that happened during the workflow monitoring phase were the exclusive focus of this group's research efforts. Here is a rundown of what was contributed to each publication.

Users are able to remotely evaluate the correctness of the executions of business processes thanks to the architecture that was offered by the authors of [17,26]. Specifically, they made advantage of a framework that allowed them to log sensitive behaviors that occurred within business processes. The client can request a signed version of the log after the procedure is finished and then verify it frequently to make sure the process was executed appropriately. Automated adaptation and real-time monitoring during execution are beyond the scope of this article. In order to guarantee safety, the authors of [18,27] used provenance information. They integrated the Security Analysis Package (SAP) into the extended Kepler provenance module to analyze provenance information within a security context. They zeroed down on the following three data-flow based security features: The first step is input validation, which involves using a whitelist of allowed inputs to detect and filter out unauthorized input. The second step is remote access validation, which involves creating an internal firewall that contains valid URLs and IP addresses. The third step is data integrity, which involves comparing on-hash and post-hash data to validate data

integrity. However, the data about provenance was used just to find a few security holes and figure out what to do next time scientific workflows are executed to avoid these kinds of assaults.

Cloud-wide auditing was utilized by the authors in [19,28,29] in order to identify potential security flaws. Vulnerability Diagnostic Trees, or VDTs, were created with the intention of clearly displaying vulnerability patterns along many audit trails. With this technology, automatic detection processes may be set up to take in different types of audit trails and then target risks according to their location and kind.

During the course of their diagnostics, however, they failed to take into account the various requirements that individuals and services have. Researching all potential attacks using this strategy for all services could add unnecessary computing cost and time to the system, making it unscalable. When this happens, the number of potential assaults and service composition violations narrows down, and the scope of the job becomes much more manageable. It appears that this paper failed to prevent or address any of the infractions it did discover, as it could only identify a handful based on the audit record.

The authors of the paper cited as [20,30] put out the idea of an intrusion-tolerant scientific workflow system. To guarantee the workflow's implementation, they used a number of tactics: 1) Increasing reliability by running the same subtask in parallel across numerous different types of virtual machines (VMs); 2) proposing a resource-circulation-based dynamic task scheduling method to disrupt the attack chain; and 3) Conceiving of a short-term method of data backup for workflows. method that can stop compromised workflows from running. Furthermore, the identification of integrity violations that happened during the execution phase of scientific processes was the exclusive focus of this study. It was not possible to This is why the intermediate data was saved; using it to re-run the workflow sub-tasks with less certainty is possible now. An evaluation of the tasks' confidence is done by a process called the "lagged decision mechanism," which is presented after them.

In an effort to remedy a limitation of their previous work, the same authors attempted to schedule subtask replicates in [31-33].

This was done in order to ensure that an attacker would not be able to disrupt the entire workflow just by compromising a single virtual machine. This approach has the potential to be regarded as a versatile tool for discovering the various other sorts of security breaches. A method of dynamic rescheduling was described in the research that was presented in [22,34]. This method was developed to deal with changes in the availability of cloud resources, such as the failure of the resources that were already available or the availability of new resources. To rephrase, once it notices a change in state, the cost model will reschedule incomplete operations to handle run-time failures by dynamically assessing the cost of deploying them onto the now-accessible cloud resources. Note that the availability of resources throughout the execution of the scientific workflow is the only security element that this study considers.

Choosing the right virtualization technology (VT) and thinking about how it relates to security are critical steps in the deployment and execution phases. This is because the majority of the security difficulties that cloud infrastructure faces are caused by Virtualization Technology (VT). It is possible for this to give quality of service (QoS) to end-users at cheaper pricing, as well as a solution that is both cost-effective and efficient in terms of resource use for cloud service providers (CSP). In light of this, we need to suggest a security-aware scheduling approach that considers workflow features and user needs when choosing the right virtual machines (VT) for tasks and workflows. A few examples of VT are Unikernel, Containers within VM, Lightweight VM, and Virtual Machines (VM) [35-41]. Also the Various WfMSs addressing cloud security issues are given in table 1.

Table 1: Various WfMSs addressing cloud security issues

WfMS	Type of supported workflow	Supported representation model	Extension	Execution environment	Covered security objectives
[24], 2018	Scientific	DAG		Cloud-based	• Data Integrity
SecDATAVIEW [25], 2019	Scientific	DAG	DATAVIEW	Within SGX enclaves, run the WfMS kernel (the parts responsible for processing sensitive data); on trusted premises, like private cloud platforms or the user's endpoint, run the rest of the WfMS	• Data Confidentiality • Data/Task Integrity • Data/Logic Confidentiality

				components.	
[26], 2021	Scientific workflow	DAG	DATAVIEW	The execution phase of scientific workflows was the sole focus of this article, which failed to uncover any other forms of security issues.	Detecting the sub-tasks with low confidence based on the lagged decision mechanism.
[27], 2021	Scientific workflows	DAG	DATAVIEW	Re-executing the failure tasks	Engine-side Monitoring

CONCLUSION

In conclusion, businesses in every sector must implement stringent cloud security procedures to protect customer information and privacy in today's interconnected world. Data breaches, illegal access, and regulatory non-compliance are growing concerns as cloud computing is integrated increasingly into everyday operations and undergoes further evolution. Organizations can greatly improve their cloud security by implementing encryption, strong authentication methods, and strict access limits. Consistent monitoring, proactive risk mitigation strategies, and adherence to regulatory frameworks such as GDPR and CCPA are necessary to maintain compliance and reduce potential risks. Prioritizing cloud security and executing a comprehensive strategy that incorporates procedural, instructional, and technological components may help enterprises efficiently secure their data and privacy in an interconnected environment. This will promote confidence with their stakeholders and customers.

We utilized the SLR procedure on the articles found by the SMR and the gaps in current knowledge concerning security issues in workflow monitoring, analysis, and adaption. Adaptation kind considered workflow type, adaptation cause, and monitoring and detection module/mechanism were the criteria used to compare the works. This leads us to the conclusion that there is a lack of current research on scalable and dependable methods for detecting, preventing, and reacting to security breaches, as well as ways to mitigate or even completely eliminate the impact on cloud-based scientific and corporate activities. We also looked at the current WfMS implementations in terms of the supported representation model, workflow life cycle phases covered, types of supported workflows, and security objectives covered.

REFERENCES

[1]. H. A. AL-Jumaili, R. C. Muniyandi, M. K. Hasan, M. J. Singh, J. K. S. Paw, and M. Amir, "Advancements in intelligent cloud computing for power optimization and battery management in hybrid renewable energy systems: A comprehensive review," Energy Reports, vol. 10, pp. 2206-2227, 2023.

[2]. S. Thiyagarajan, "Automate Provisioning and Orchestration of Cloud Infrastructure using AWX," Dublin, National College of Ireland, 2022.

[3]. O. Ali, A. Shrestha, A. Chatfield, and P. Murray, "Assessing information security risks in the cloud: A case study of Australian local government authorities," Government Information Quarterly, vol. 37, no. 1, p. 101419, 2020.

[4]. I. Naseer, "AWS Cloud Computing Solutions: Optimizing Implementation for Businesses," STATISTICS, COMPUTING AND INTERDISCIPLINARY RESEARCH, vol. 5, no. 2, pp. 121-132, 2023.

[5]. H. A. Khattak, H. Farman, B. Jan, and I. U. Din, "Toward integrating vehicular clouds with IoT for smart city services," IEEE Network, vol. 33, no. 2, pp. 65-71, 2019.

[6]. A. R. Kunduru, "THE PERILS AND DEFENSES OF ENTERPRISE CLOUD COMPUTING: A COMPREHENSIVE REVIEW," Central Asian Journal of Mathematical Theory and Computer Sciences, vol. 4, no. 9, pp. 29-41, 2023.

[7]. F. Thabit, S. Alhomdy, and S. Jagtap, "A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions," International Journal of Intelligent Networks, vol. 2, pp. 18-33, 2021.

[8]. N. Mazher, Z. Asharaf, and M. A. Ganne, "Artificial Intelligence Based Architecture to Enhance Cloud Computing Security," Authorea Preprints, 2023.

[9]. J. Weinman, Cloudonomics+ Website: The Business Value of Cloud Computing. Wiley Online Library, 2023.

[10]. Supongmen Walling, "A Comprehensive Review on Cloud Computing and Cloud Security Issues ", International Journal of Scientific Research in Computer Science, Engineering and Information

Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 4, pp. 483-490, July-August 2020. Available at doi : https://doi.org/10.32628/CSEIT206489 Journal URL : http://ijsrcseit.com/CSEIT206489

[11]. J. Liu et al., "A Survey of Data-Intensive Scientific Workflow Management To cite this version : HAL Id : lirmm-01144760," J. Grid Comput., vol. 13(4), p. pp.457-493., 2019

[12]. A. O. Francis, B. Emmanuel, D. D. Zhang, W. Zheng, Y. Qin, and D. D. Zhang, "Exploration of Secured Workflow Scheduling Models in Cloud Environment: A Survey," Proc. - 2018 6th Int. Conf. Adv. Cloud Big Data, CBD 2018, pp. 71–76, 2018, doi: 10.1109/CBD.2018.00022

[13]. Sheikh, M. Munro, and D. Budgen, "Systematic Literature Review (SLR) of resource scheduling and security in cloud computing," Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 4, pp. 35–44, 2019, doi: 10.14569/ijacsa.2019.0100404.

[14]. J. Angela Jennifa Sujana, T. Revathi, and S. Joshua Rajanayagam, "Fuzzy-based Security-Driven Optimistic Scheduling of Scientific Workflows in Cloud Computing," IETE J. Res., vol. 66, no. 2, pp. 224–241, 2020, doi: 10.1080/03772063.2018.1486740.

[15]. H. Djigal, J. Feng, and J. Lu, "Performance Evaluation of Security-Aware List Scheduling Algorithms in IaaS Cloud," Proc. - 20th IEEE/ACM Int. Symp. Clust. Cloud Internet Comput. CCGRID 2020, pp. 330–339, 2020, doi: 10.1109/CCGrid49817.2020.00-60.

[16]. Y. Wang, Y. Guo, Z. Guo, W. Liu, and C. Yang, "Protecting scientific workflows in clouds with an intrusion tolerant system," IET Inf. Secur., vol. 14, no. 2, pp. 157–165, 2020, doi: 10.1049/iet-ifs.2018.5279.

[17]. Y. Wang, Y. Guo, W. Wang, H. Liang, and S. Huo, "INHIBITOR: An intrusion tolerant scheduling algorithm in cloud-based scientific workflow system," Futur. Gener. Comput. Syst., vol. 114, pp. 272–284, 2021, doi: 10.1016/j.future.2020.08.004.

[18]. Z. Wen, R. Qasha, Z. Li, R. Ranjan, P. Watson, and A. Romanovsky, "Dynamically Partitioning Workflow over Federated Clouds for Optimising the Monetary Cost and Handling Run-Time Failures," IEEE Trans. Cloud Comput., vol. 8, no. 4, pp. 1093–1107, 2020, doi: 10.1109/TCC.2016.2603477.

[19]. A. S. Gowri and others, "Impact of virtualization technologies in the development and management of cloud applications," Int. J. Intell. Syst. Appl. Eng., vol. 7, no. 2, pp. 104–110, 2019.

[20]. Y. wen Wang, J. xing Wu, Y. fei Guo, H. chao Hu, W. yan Liu, G. zhen Cheng, Scientific workflow execution system based on mimic defense in the cloud environment, Front. Inf. Technol. Electron. Eng. 19 (12) (2018) 1522–1536, http://dx.doi.org/10.1631/FITEE.1800621.

[21]. S. Mofrad, I. Ahmed, S. Lu, P. Yang, H. Cui, F. Zhang, SecDataView: A secure big data workflow management system for heterogeneous computing environments, in: ACM Int. Conf. Proceeding Ser, 2019, pp. 390–403, http://dx.doi.org/10.1145/3359789.3359845.

[22]. Y. Wang, Y. Guo, W. Wang, H. Liang, S. Huo, INHIBITOR: An intrusion tolerant scheduling algorithm in cloud-based scientific workflow system, Futur. Gener. Comput. Syst. 114 (2021) 272–284, http://dx.doi.org/10. 1016/j.future.2020.08.004.

[23]. Z. Ahmad, B. Nazir, A. Umer, A fault-tolerant workflow management system with quality-of-service-aware scheduling for scientific workflows in cloud computing, Int. J. Commun. Syst. 34 (1) (2021) http://dx.doi.org/ 10.1002/dac.4649.

[24]. Ramya Manikyam, J. Todd McDonald, William R. Mahoney, Todd R. Andel, and Samuel H. Russ. 2016.Comparing the effectiveness of commercial obfuscators against MATE attacks. In Proceedings of the 6th Workshop on Software Security, Protection, and Reverse Engineering (SSPREW'16)

[25]. R. Manikyam. 2019.Program protection using software based hardware abstraction.Ph.D. Dissertation.University of South Alabama.

[26]. GPB GRADXS, N RAO, Behaviour Based Credit Card Fraud Detection Design And Analysis By Using Deep Stacked Autoencoder Based Harris Grey Wolf (Hgw) Method, Scandinavian Journal of Information Systems 35 (1), 1-8.

[27]. R Pulimamidi, GP Buddha, Applications of Artificial Intelligence Based Technologies in The Healthcare Industry, Tuijin Jishu/Journal of Propulsion Technology 44 (3), 4513-4519.

[28]. R Pulimamidi, GP Buddha, AI-Enabled Health Systems: Transforming Personalized Medicine And Wellness, Tuijin Jishu/Journal of Propulsion Technology 44 (3), 4520-4526.

[29]. GP Buddha, SP Kumar, CMR Reddy, Electronic system for authorization and use of cross-linked resource instruments, US Patent App. 17/203,879.

[30]. Nadella, G. S. (2023). Validating the Overall Impact of IS on Educators in U.S. High Schools Using IS-Impact Model – A Quantitative PLS-SEM Approach, DAI-A 85/7(E), Dissertation Abstracts International, Ann Arbor, ISBN 9798381388480, 189, 2023.

[31]. Gonaygunta, Hari, Factors Influencing the Adoption of Machine Learning Algorithms to Detect Cyber Threats in the Banking Industry, DAI-A 85/7(E), Dissertation Abstracts International, Ann Arbor, United States, ISBN 9798381387865, 142, 2023.

[32]. Hari Gonaygunta (2023) Machine Learning Algorithms for Detection of Cyber Threats using Logistic Regression, 10.47893/ijssan.2023.1229.
[33]. Hari Gonaygunta, Pawankumar Sharma, (2021) Role of AI in product management automation and effectiveness, https://doi.org/10.2139/ssrn.4637857.
[34]. Sri Charan Yarlagadda, Role of Artificial Intelligence, Automation, and Machine Learning in Sustainable Plastics Packaging markets: Progress, Trends, and Directions, International Journal on Recent and Innovation Trends in Computing and Communication, Vol:11, Issue 9s, Pages: 818–828, 2023.
[35]. Sri Charan Yarlagadda, The Use of Artificial Intelligence and Machine Learning in Creating a Roadmap Towards a Circular Economy for Plastics, International Journal on Recent and Innovation Trends in Computing and Communication, Vol:11, Issue 9s, Pages: 829-836, 2023.
[36]. Nagaraj, A. Kalaivani, S. B. R, S. Akila, H. K. Sachdev, and S. K. N, "The Emerging Role of Artificial intelligence in STEM Higher Education: A Critical review," International Research Journal of Multidisciplinary Technovation, pp. 1–19, Aug. 2023, doi: 10.54392/irjmt2351.
[37]. Sivabalaselvamani, K. Nanthini, Bharath Kumar Nagaraj, K. H. Gokul Kannan, K. Hariharan, M. Mallingeshwaran, Healthcare Monitoring and Analysis Using ThingSpeak IoT Platform: Capturing and Analyzing Sensor Data for Enhanced Patient Care, IGI Global eEditorial Discovery, Pages: 25, 2024. DOI: 10.4018/979-8-3693-1694-8.ch008.
[38]. Amol Kulkarni, Amazon Athena Serverless Architecture and Troubleshooting, International Journal of Computer Trends and Technology, Vol, 71, issue, 5, pages 57-61, 2023.
[39]. Amazon Redshift Performance Tuning and Optimization,International Journal of Computer Trends and Technology, vol, 71, issue, 2, pages, 40-44, 2023.