CyberCloud Framework: Integrating Cybersecurity Resilience into Cloud Infrastructure Optimization for Enhanced Operational Efficiency

ANUOLUWAPO COLLINS[1], CHISOM ELIZABETH ALOZIE[2], OLUMESE ANTHONY ABIEBA[3], JOSHUA IDOWU AKERELE[4], OLANREWAJU OLUWASEUN AJAYI[5]

[1]*Cognizant Technology Solutions, Canada*

[2]*University of the Cumberlands*

[3]*Abeam Consulting USA*

[4]*Independent Researcher, Nigeria*

[5]*University of the Cumberlands*

Abstract- The increasing adoption of cloud computing has revolutionized the way organizations manage their data and operations, offering unparalleled scalability and flexibility. However, this digital transformation brings along significant cybersecurity challenges, with cloud environments becoming prime targets for cyber threats. In response, the CyberCloud Framework emerges as a pioneering approach that seamlessly integrates cybersecurity resilience into cloud infrastructure optimization to enhance operational efficiency. This abstract presents an overview of the CyberCloud Framework, outlining its key components and the benefits it offers to organizations navigating the complexities of cloud security and performance optimization. The framework operates at the intersection of cybersecurity and cloud computing, offering a holistic approach to mitigate risks while maximizing the benefits of cloud technology. Key elements of the CyberCloud Framework include proactive threat detection mechanisms, robust encryption protocols, dynamic access controls, and continuous monitoring capabilities. By embedding these security measures into the fabric of cloud infrastructure optimization processes, the framework ensures that cybersecurity resilience becomes an inherent aspect of cloud operations. Furthermore, the CyberCloud Framework emphasizes the importance of adaptability and scalability, catering to the evolving threat landscape and the dynamic nature of cloud environments. Through automated responses and intelligent analytics, the framework enables organizations to swiftly detect and respond to security incidents, minimizing potential disruptions and ensuring uninterrupted business operations. Overall, the CyberCloud Framework represents a paradigm shift in cybersecurity strategy, offering organizations a comprehensive solution to fortify their cloud infrastructure against cyber threats while enhancing operational efficiency. As organizations continue to embrace cloud technologies, the CyberCloud Framework stands as a crucial tool to safeguard their digital assets and maintain a competitive edge in today's rapidly evolving cyber landscape.

Indexed Terms- Cybercloud; Cybersecurity; Resilience; Cloud Infrastructure; Operational Efficiency; Review

I. INTRODUCTION

Cloud computing adoption has indeed experienced significant growth in recent years, providing scalability, flexibility, and cost-efficiency to organizations. However, this rapid adoption has also introduced various cybersecurity challenges (Golightly et al., 2022). The dynamic nature of cloud environments, shared responsibility models, and the complexity of cloud infrastructures have rendered them vulnerable to cyber threats (Salek et al., 2022). Ensuring the security and resilience of cloud infrastructure has become crucial to protect sensitive data and uphold operational efficiency (Baikloy et al., 2020).

The integration of cybersecurity resilience into cloud infrastructure optimization is essential to enhance the overall security posture of cloud environments. By incorporating cybersecurity measures into the design and management of cloud infrastructure, organizations can proactively mitigate risks and respond effectively to cyber incidents (Baikloy et al., 2020). This integration ensures that security is a foundational element of cloud operations, leading to improved threat detection, incident response, and overall operational resilience (Baikloy et al., 2020).

The CyberCloud Framework aims to meet the critical need for integrating cybersecurity resilience into cloud infrastructure optimization. This framework offers a structured approach to enhancing the security of cloud environments while optimizing operational efficiency (Baikloy et al., 2020). Through the utilization of the CyberCloud Framework, organizations can align their cybersecurity strategies with cloud infrastructure best practices, strengthening their defenses against evolving cyber threats and ensuring operational continuity (Baikloy et al., 2020).

In conclusion, the CyberCloud Framework acts as a strategic roadmap for organizations seeking to enhance their cybersecurity resilience within cloud environments. By highlighting the significance of integrating security measures into cloud infrastructure optimization, this framework enables organizations to securely and efficiently navigate the complexities of cloud computing, safeguarding their digital assets and ensuring uninterrupted business operations.

2.1. Literature Review

The CyberCloud Framework aims to integrate cybersecurity resilience into cloud infrastructure optimization to enhance operational efficiency. This framework combines the concepts of cloud computing, cybersecurity, and resilience to ensure that cloud services providers can evaluate and enhance their cybersecurity levels effectively (Baikloy et al., 2020). By incorporating a cyber resilient capability maturity model, organizations can assess their cybersecurity readiness and improve their defenses against cyber threats in cloud computing environments.

In the context of critical infrastructure, cybersecurity plays a vital role in ensuring the resilience of organizations. Studies have highlighted the importance of intellectual capital in cybersecurity performance and crisis response within critical infrastructure organizations (Garcia-Perez et al., 2021). Additionally, it has been emphasized that a comprehensive cybersecurity strategy should include cyber resilience alongside defense policies to effectively protect critical infrastructure (Malatji & Solms, 2020). This integrated approach to cybersecurity resilience, which includes aspects like cryptography, IoT security, and cloud computing security, is crucial for safeguarding critical infrastructure against cyber threats (Malatji & Solms, 2021).

Efficiency in operational processes, such as operating room management, is essential for optimizing resources and improving overall performance. While some studies focus on operational efficiency in various sectors like healthcare (Dexter et al., 2004; Cima et al., 2011), shipping (Venkadasalam et al., 2020), and railway transportation (Niu et al., 2022), the CyberCloud Framework specifically addresses the integration of cybersecurity resilience into cloud infrastructure optimization. By leveraging methodologies like Lean and Six Sigma, organizations can enhance operational efficiency in high-volume settings like academic medical centers (Cima et al., 2011; Saheed et al., 2022). Moreover, the CyberCloud Framework aligns with the evolving cybersecurity paradigm that emphasizes cyber resilience and business continuity (Javorník & Husák, 2022). By integrating cybersecurity with operational efficiency, organizations can better protect their cloud infrastructure while ensuring optimal performance. This approach not only enhances cybersecurity posture but also contributes to overall operational efficiency and organizational resilience in the face of cyber threats.

In conclusion, the CyberCloud Framework represents a holistic approach to enhancing operational efficiency by integrating cybersecurity resilience into cloud infrastructure optimization. By leveraging established models like Lean and Six Sigma and emphasizing the importance of cyber resilience in critical infrastructure, organizations can fortify their defenses, improve operational efficiency, and ensure business continuity in the digital age.

2.2. Key Components of the CyberCloud Framework

The CyberCloud framework integrates key components to ensure robust cybersecurity measures. Proactive threat detection mechanisms are implemented through intrusion detection systems (IDS) and intrusion prevention systems (IPS) (Sultana et al., 2020). These systems aid in identifying and mitigating potential threats in real-time. Furthermore, machine learning algorithms are employed for anomaly detection, enhancing the framework's capability to detect unknown and evolving threats (Gou et al., 2016; Adisa et al., 2024).

To secure data, robust encryption protocols are utilized, employing strong encryption algorithms for data both in transit and at rest (Touil et al., 2021). Integration of encryption key management systems further bolsters data security by ensuring proper key handling and protection (Farshim et al., 2013). These measures assist in safeguarding sensitive information from unauthorized access and data breaches. Dynamic access controls are a critical aspect of the framework, involving the implementation of role-based access control (RBAC) mechanisms (Janicke et al., 2012). By assigning permissions based on roles, access to resources is managed and restricted, thereby reducing the risk of unauthorized access. Moreover, the utilization of multi-factor authentication (MFA) enhances access security by necessitating multiple forms of verification for user authentication (Ding et al., 2019; Saheed et al., 2022).

Continuous monitoring capabilities are integrated into the framework through the deployment of real-time monitoring tools for network traffic and system activities (Gou et al., 2016). By continuously monitoring activities, potential security incidents can be promptly detected and addressed. Integration with security information and event management (SIEM) systems offers comprehensive visibility into the network, enabling effective threat detection and response (Rotaru et al., 2021; Saheed and Raji, 2022). In conclusion, the CyberCloud framework incorporates proactive threat detection mechanisms, robust encryption protocols, dynamic access controls, and continuous monitoring capabilities to establish a comprehensive cybersecurity posture. By integrating these key components, organizations can enhance their resilience against cyber threats and effectively safeguard their critical assets.

2.3. Integration with Cloud Infrastructure Optimization Processes

Integration with cloud infrastructure optimization processes involves key aspects such as automation of security measures, scalability, adaptability, and alignment with operational efficiencies. To enhance security, integrating security automation tools into cloud orchestration platforms and streamlining security policies through automation are crucial (Oulaaffart et al., 2022; Oulaaffart et al., 2022). This ensures that security measures can be efficiently managed and adapted to changing threat landscapes and regulatory requirements (Peters et al., 2018; Bringhenti et al., 2019). Scalability and adaptability are essential for cloud infrastructure optimization. Having the flexibility to scale security measures alongside cloud resource scaling and the agility to adapt to evolving threats and regulations are vital components (Peters et al., 2018; Bringhenti et al., 2019; Raji et al., 2020). This allows for a dynamic and responsive security framework within cloud environments. Aligning with operational efficiencies involves minimizing security overhead through optimized resource utilization and reducing operational disruptions through proactive threat mitigation (Paladi et al., 2018; Bringhenti et al., 2019). By optimizing resource allocation and proactively addressing security threats, operational efficiency can be significantly improved in cloud environments (Olodo et al., 2020).

In conclusion, integrating security automation tools, ensuring scalability and adaptability of security measures, and aligning with operational efficiencies are critical for optimizing cloud infrastructure processes. By implementing these strategies, organizations can enhance the security, efficiency, and flexibility of their cloud environments.

2.4. Benefits of the CyberCloud Framework

To understand the benefits of the CyberCloud framework, we can draw insights from various reputable sources. The CyberCloud framework offers several advantages that align with the key aspects of enhanced security posture, improved operational efficiency, cost savings through optimization, and competitive advantage in the digital landscape.

The CyberCloud framework can significantly enhance security postures by providing features such as device authentication, key agreement, policy authorization, and improved trust-based security mechanisms (Chien et al., 2020; Renjith et al., 2022). These security enhancements help protect vital information from external attacks and malicious intrusions, ensuring a robust security infrastructure within the cloud environment. Implementing the CyberCloud framework can lead to improved operational efficiency by optimizing security-as-a-service allocation, managing risks effectively, and enhancing the overall security alert system (Chaisiri et al., 2015; Khanum & Shivakumar, 2019; Adeoti et al., 2018). By streamlining security services allocation and risk management, organizations can operate more efficiently and respond promptly to security threats, thereby increasing operational effectiveness. The CyberCloud framework offers cost-saving opportunities through optimization strategies such as secure collaborative data mining, dynamic authentication frameworks, and improved security models for web services (Lu et al., 2012; Kumaresan & Gopalan, 2017; Jiang et al., 2016). By leveraging these optimization techniques, organizations can reduce costs associated with security breaches, software vulnerabilities, and inefficient security protocols, leading to significant cost savings in the long run. Adopting the CyberCloud framework can provide organizations with a competitive advantage in the digital landscape by enhancing their security posture, operational efficiency, and cost-effectiveness (Ma, 2004). By leveraging advanced security frameworks and optimization strategies, organizations can differentiate themselves in the market, build customer trust, and stay ahead of competitors in the rapidly evolving digital ecosystem.

In conclusion, the CyberCloud framework offers a comprehensive approach to cybersecurity, operational efficiency, cost savings, and competitive advantage in the digital landscape. By integrating the key features of enhanced security posture, improved operational efficiency, cost savings through optimization, and competitive advantage, organizations can strengthen their cybersecurity defenses, optimize their operations, reduce costs, and gain a competitive edge in today's digital environment.

2.5. Future Outlook

The future outlook of the CyberCloud Framework involves integrating cybersecurity resilience into cloud infrastructure optimization to enhance operational efficiency. This entails leveraging existing research on cybersecurity capabilities for critical infrastructure resilience Malatji & Solms (2021) and developing cyber resilient capability maturity models for cloud computing services (Baikloy et al., 2020). By incorporating these frameworks, organizations can measure resilience levels and evaluate their cybersecurity capabilities to improve operational efficiency and enhance cybersecurity levels in cloud services.

Additionally, it is essential to consider the intellectual capital perspective in cybersecurity performance and crisis response for critical infrastructure organizations (Garcia-Perez et al., 2021). This perspective informs future research and practice by highlighting the role of intellectual capital management in supporting cybersecurity and digital resilience. Moreover, aligning cybersecurity with business continuity to achieve cyber resilience is crucial for the future cybersecurity paradigm (Javorník & Husák, 2022). Furthermore, the development of a cloud security capability maturity model (CSCMM) can provide a structured approach to enhancing cybersecurity in cloud environments (Le & Hoang, 2017). This model extends existing cybersecurity frameworks and standards to optimize security metrics and resilience across all levels of cloud infrastructure. By adopting such models, organizations can proactively address cybersecurity challenges and improve their overall cyber resilience.

In conclusion, the future outlook of the CyberCloud Framework lies in the strategic integration of cybersecurity resilience measures into cloud infrastructure optimization. By drawing on established cybersecurity frameworks, maturity models, and intellectual capital perspectives, organizations can fortify their cloud environments against cyber threats, enhance operational efficiency, and ensure robust cybersecurity practices for the future.

2.6. Recommendation and Conclusion

The CyberCloud Framework represents a groundbreaking approach to address the evolving cybersecurity challenges faced by organizations in the era of cloud computing. By seamlessly integrating cybersecurity resilience into cloud infrastructure optimization processes, the framework offers a holistic solution to enhance operational efficiency while safeguarding digital assets from cyber threats. Its key components, including proactive threat detection mechanisms, robust encryption protocols, dynamic access controls, and continuous monitoring capabilities, empower organizations to fortify their cloud environments against cyber attacks. Furthermore, the CyberCloud Framework emphasizes adaptability, scalability, and alignment with operational efficiencies, ensuring that cybersecurity measures do not impede but rather enhance organizational agility and competitiveness in the digital landscape.

In light of the increasing reliance on cloud technologies and the growing sophistication of cyber threats, it is imperative for organizations to prioritize cybersecurity resilience as an integral part of their cloud infrastructure optimization strategies. The CyberCloud Framework provides a blueprint for achieving this goal, offering practical guidelines and best practices to fortify cloud environments while maximizing operational efficiency. Therefore, organizations must proactively adopt and implement the CyberCloud Framework, leveraging its comprehensive approach to mitigate risks, minimize disruptions, and maintain a competitive edge in today's dynamic business environment. By integrating cybersecurity resilience into cloud infrastructure optimization, organizations can ensure the sustainability of their operations, safeguard critical data assets, and uphold the trust of their stakeholders in an increasingly interconnected and digital world.

REFERENCES

[1] Adeoti, J. O., Olawale, A. Y., & Raji, A. M. (2018). The Impact Of Celebrity Endorsement On The Brand Image Of MTN Telecommunications Limited: The Perspective Of Subscribers IN ILORIN METROPOLIS.

[2] Adisa, O., Ilugbusi, B.S., Adewunmi, O., Franca, O. and Ndubuisi, L. (2024a). A comprehensive review of redefining agricultural economics for sustainable development: Overcoming challenges and seizing opportunities in a changing world. World Journal Of Advanced Research and Reviews, 21(1), pp.2329–2341.

[3] Baikloy, E., Praneetpolgrang, P., & Jirawichitchai, N. (2020). Development of cyber resilient capability maturity model for cloud computing services. Tem Journal, 915-923. https://doi.org/10.18421/tem93-11

[4] Bringhenti, D., Marchetto, G., Sisto, R., Valenza, F., & Yusupov, J. (2019). Towards a fully automated and optimized network security functions orchestration.. https://doi.org/10.1109/cccs.2019.8888130

[5] Chaisiri, S., Ko, R., & Niyato, D. (2015). A joint optimization approach to security-as-a-service allocation and cyber insurance management.. https://doi.org/10.1109/trustcom.2015.403

[6] Chien, H., Chen, Y., Qiu, G., Liao, J., Hung, R., Lin, P., … & Su, C. (2020). A mqtt-api-compatible iot security-enhanced platform. International Journal of Sensor Networks, 32(1), 54. https://doi.org/10.1504/ijsnet.2020.104463

[7] Cima, R., Brown, M., Hebl, J., Moore, R., Rogers, J., Kollengode, A., … & Deschamps, C. (2011). Use of lean and six sigma methodology to improve operating room efficiency in a high-volume tertiary-care academic medical center. Journal of the American College of Surgeons, 213(1), 83-92. https://doi.org/10.1016/j.jamcollsurg.2011.02.009

[8] Dexter, F., Epstein, R., Traub, R., Xiao, Y., & Warltier, D. (2004). Making management decisions on the day of surgery based on operating room efficiency and patient waiting times. Anesthesiology, 101(6), 1444-1453. https://doi.org/10.1097/00000542-200412000-00027

[9] Ding, S., Cao, J., Li, C., Fan, K., & Li, H. (2019). A novel attribute-based access control scheme using blockchain for iot. Ieee Access, 7, 38431-38441. https://doi.org/10.1109/access.2019.2905846

[10] Farshim, P., Libert, B., Paterson, K., & Quaglia, E. (2013). Robust encryption, revisited., 352-368. https://doi.org/10.1007/978-3-642-36362-7_22

[11] Garcia-Perez, A., Sallos, M., & Tiwasing, P. (2021). Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: an intellectual capital perspective. Journal of Intellectual Capital, 24(2), 465-486. https://doi.org/10.1108/jic-06-2021-0166

[12] Garcia-Perez, A., Sallos, M., & Tiwasing, P. (2021). Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: an intellectual capital perspective. Journal of Intellectual Capital, 24(2), 465-486. https://doi.org/10.1108/jic-06-2021-0166

[13] Golightly, L., Chang, V., Xu, Q., & Gao, X. (2022). Adoption of cloud computing as innovation in the organization. International Journal of Engineering Business Management, 14, 184797902210939. https://doi.org/10.1177/18479790221093992

[14] Gou, G., Bai, Q., Xiong, G., & Li, Z. (2016). Discovering abnormal behaviors via http header fields measurement. Concurrency and Computation Practice and Experience, 29(20). https://doi.org/10.1002/cpe.3926

[15] Janicke, H., Cau, A., Siewe, F., & Zedan, H. (2012). Dynamic access control policies: specification and verification. The Computer Journal, 56(4), 440-463. https://doi.org/10.1093/comjnl/bxs102

[16] Javorník, M. and Husák, M. (2022). Mission-centric decision support in cybersecurity via bayesian privilege attack graph. Engineering Reports, 4(12). https://doi.org/10.1002/eng2.12538

[17] Javorník, M. and Husák, M. (2022). Mission-centric decision support in cybersecurity via bayesian privilege attack graph. Engineering Reports, 4(12). https://doi.org/10.1002/eng2.12538

[18] Jiang, W., Xu, H., Dong, H., Jin, H., & Liao, X. (2016). An improved security framework for web service-based resources. Turkish Journal of Electrical Engineering & Computer Sciences, 24, 774-792. https://doi.org/10.3906/elk-1303-12

[19] Khanum, A. and Shivakumar, R. (2019). An enhanced security alert system for smart home using iot. Indonesian Journal of Electrical Engineering and Computer Science, 13(1), 27. https://doi.org/10.11591/ijeecs.v13.i1.pp27-34

[20] Kumaresan, G. and Gopalan, N. (2017). Educloud: a dynamic three stage authentication framework to enhance security in public cloud. International Journal of Engineering and Manufacturing, 7(6), 12-26. https://doi.org/10.5815/ijem.2017.06.02

[21] Le, N. and Hoang, D. (2017). Capability maturity model and metrics framework for cyber cloud security. Scalable Computing Practice and Experience, 18(4). https://doi.org/10.12694/scpe.v18i4.1329

[22] Lu, Q., Xiong, Y., Gong, X., & Huang, W. (2012). Secure collaborative outsourced data mining with multi-owner in cloud computing.. https://doi.org/10.1109/trustcom.2012.251

[23] Ma, H. (2004). Toward global competitive advantage. Management Decision, 42(7), 907-924. https://doi.org/10.1108/00251740410550961

[24] Malatji, M. and Solms, S. (2020). Cybersecurity policy and the legislative context of the water and wastewater sector in south africa. Sustainability, 13(1), 291. https://doi.org/10.3390/su13010291

[25] Malatji, M. and Solms, S. (2021). Cybersecurity capabilities for critical infrastructure resilience. Information and Computer Security, 30(2), 255-279. https://doi.org/10.1108/ics-06-2021-0091

[26] Niu, Y., Xiao, F., Zhang, N., & Sadeghi, M. (2022). Transportation efficiency of railway operation enterprises.. https://doi.org/10.21203/rs.3.rs-2316597/v1

[27] Olodo, H. B., Aremu, M. A., Raji, M. A., & Aminu, H. A. (2020) Teamwork And Organisational Performance: A Study Of AL-HIKMAH UNIVERSITY. 5 (1), pp75-86

[28] Oulaaffart, M., Badonnel, R., & Bianco, C. (2022). An automated smt-based security framework for supporting migrations in cloud composite services..

https://doi.org/10.1109/noms54207.2022.9789768

[29] Oulaaffart, M., Badonnel, R., & Festor, O. (2022). Cmsec: a vulnerability prevention tool for supporting migrations in cloud composite services.. https://doi.org/10.1109/cloudnet55617.2022.9978826

[30] Paladi, N., Michalas, A., & Dang, H. (2018). Towards secure cloud orchestration for multi-cloud deployments.. https://doi.org/10.1145/3195870.3195874

[31] Peters, K., Bradbury, J., Bergmann, S., Capuccini, M., Cascante, M., Atauri, P., … & Steinbeck, C. (2018). Phenomenal: processing and analysis of metabolomics data in the cloud. Gigascience, 8(2). https://doi.org/10.1093/gigascience/giy149

[32] Raji, M. A., Brimah, A. N., & Mustapha, Y. I. (2020). Effect of sensory marketing on customer patronage in south west Nigeria (case study of KFC). Fountain University Osogbo Journal of Management (FUOJM), 5(2), 97-110.

[33] Renjith, P., Ramesh, K., & Balasubramani, S. (2022). An improved trust-based security framework for iot health care monitoring system.. https://doi.org/10.21203/rs.3.rs-1970278/v1

[34] Rotaru, D., Smart, N., Tanguy, T., Vercauteren, F., & Wood, T. (2021). Actively secure setup for spdz. Journal of Cryptology, 35(1). https://doi.org/10.1007/s00145-021-09416-w

[35] Saheed, Y. K., & Raji, M. A. (2022, March). Effectiveness of Deep Learning Long Short-Term Memory Network for Stock Price Prediction on Graphics Processing Unit. In 2022 International Conference on Decision Aid Sciences and Applications (DASA) (pp. 1665-1671). IEEE.

[36] Saheed, Y. K., Ayobami, R. M., & Orje-Ishegh, T. (2022). A Comparative Study of Regression Analysis for Modelling and Prediction of Bitcoin Price. In Blockchain Applications in the Smart Era (pp. 187-209). Cham: Springer International Publishing.

[37] Saheed, Y. K., Baba, U. A., & Raji, M. A. (2022). Big Data Analytics for Credit Card Fraud Detection Using Supervised Machine Learning Models. In Big Data Analytics in the Insurance Market (pp. 31-56). Emerald Publishing Limited.

[38] Saheed, Y. K., Kehinde, T. O., Ayobami Raji, M., & Baba, U. A. (2023). Feature selection in intrusion detection systems: a new hybrid fusion of Bat algorithm and Residue Number System. Journal of Information and Telecommunication, 1-19.

[39] Salek, M., Khan, S., Rahman, M., Deng, H., Islam, M., Khan, Z., … & Shue, M. (2022). A review on cybersecurity of cloud computing for supporting connected vehicle applications. IEEE Internet of Things Journal, 9(11), 8250-8268. https://doi.org/10.1109/jiot.2022.3152477

[40] Sultana, T., Almogren, A., Akbar, M., Ullah, I., & Javaid, N. (2020). Data sharing system integrating access control mechanism using blockchain-based smart contracts for iot devices. Applied Sciences, 10(2), 488. https://doi.org/10.3390/app10020488

[41] Touil, H., Akkad, N., & Satori, K. (2021). Secure and guarantee qos in a video sequence: a new approach based on tls protocol to secure data and rtp to ensure real-time exchanges. International Journal of Safety and Security Engineering, 11(1), 59-68. https://doi.org/10.18280/ijsse.110107

[42] Venkadasalam, S., Mohamad, A., & Sifat, I. (2020). Operational efficiency of shipping companies. International Journal of Emerging Markets, 15(5), 875-897. https://doi.org/10.1108/ijoem-07-2019-0493