# Resilient by Design: Integrating Risk Management into Enterprise Healthcare Systems for the Digital Age

**Praveen Kumar Pemmasani[1], Ketty Anderson[2]**
[1]IT Solutions Architect, BJC Health Care, 2630 State Hwy K, O'Fallon, MO 63368
[2]Department of Math and Computing, University of Southern Queensland, 487/521-535 West St, Darling Heights, QLD 4350, Australia

## ABSTRACT

*Although resilient performance (RP) in health services can be both enhanced and hindered by the use of digital technologies (DTs), little is known on how this influence occurs through design. This study introduces a framework for designing resilient health services supported by DTs, involving four steps: (i) define the motivation for the framework application, select the target system, and form a project team; (ii) modeling of the target system; (iii) identify problems and countermeasures, emphasizing the role of DTs supportive of RP; and (iv) implement countermeasures. The framework was tested in the blood transfusion process of a large tertiary hospital. Data collection for this test included participant and non-participant observations, interviews, and documentary analysis. Results shed light on the framework's utility and ease of use, also giving rise to propositions that guide the framework application. These propositions are related to using business process management notation to bridge the perspectives of DTs designers and human factors experts; supporting dynamic prioritization of orders; standardizing interactions between management information systems; using DTs to amplify rather than replace human skills; using DTs to buy time for deploying responses to variabilities; accounting for the perspectives of diverse stakeholders; and learning from applying the framework. Requirements of DTs supportive of RP were also derived from the propositions, offering guidance to designers.*

**Keywords:** Healthcare IT Resilience, Risk Management in Healthcare, Cyber Risk Assessment, Business Continuity Planning (BCP), Digital Transformation, Regulatory Compliance

## Introduction

The use of digital technologies (DTs) in healthcare encompasses a wide range of applications such as management information systems, artificial intelligence algorithms, big data analytics, and smart wearables. The best outcomes from these technologies occur if their use accounts for social and organizational factors. To this end, designers of DTs should acquire a deep understanding of work-*as*-done in reality by users, acknowledging variabilities that are neglected in models of work-*as*-imagined in standardized operating procedures. If the requirements of users are not accounted for, there might be workarounds to the intended use of DTs [1]. The rapid digital transformation of healthcare has revolutionized patient care, operational efficiency, and medical research. Advanced technologies such as electronic health records, artificial intelligence (AI)-driven diagnostics, and telemedicine have significantly improved healthcare accessibility and decision-making. However, this digital shift also introduces new risks, including cybersecurity threats, data privacy concerns, system downtimes, and regulatory challenges. As healthcare organizations become increasingly reliant on digital infrastructure, the need for a robust risk management framework is more critical than ever to ensure resilience, continuity, and patient safety.

Risk management in enterprise healthcare systems extends beyond traditional clinical risks to encompass cybersecurity, financial stability, compliance, and operational efficiency. A resilient healthcare system must proactively identify potential threats, assess vulnerabilities, and implement mitigation strategies before disruptions occur. Integrating risk management into digital healthcare operations involves leveraging real-time data analytics, artificial intelligence, and automated risk assessment tools to predict and prevent system failures. This approach not only safeguards patient information but also strengthens trust in digital healthcare services. Moreover, regulatory bodies worldwide impose stringent guidelines to protect patient data and ensure healthcare system integrity. Frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in Europe set strict compliance requirements for digital healthcare operations. Failure to adhere to these standards can lead to legal penalties, reputational damage, and compromised patient safety. Therefore, enterprise healthcare organizations must embed risk management principles into their digital strategies, ensuring compliance while fostering innovation and operational resilience. The design and implementation of execution of data strategy within a health cluster is a sophisticated process. Diverse actors, stakeholders, and business functions are involved. The need for designing roadmaps for the implementation of the strategy also incorporates the identification of use cases for novel initiatives, services, and systems. In this chapter, we communicate our experience in designing use cases as carriers of enhanced efficiency and performance that is data driven. This is a high-value intellectual effort aiming to strategize the allocation of resources and the design of new robust and resilient systems to promote efficiency and performance. We exploit the outcomes of maturity assessment for data governance and data strategy, and we provide a systematic methodology for the implementation of a resilient strategy in the health cluster [2].

The framework was tested in a large tertiary hospital in the context of the blood transfusion process (BTP). This process was chosen for two main reasons: (i) it has complexity characteristics that limit the applicability of standardized operating procedures, creating the need for RP - e.g., risks to patient safety; customization to meet the needs of each patient; diversity of activities (e.g., blood donation, blood transportation); diversity of people in dynamic interactions (e.g., donors, lab staff, clinicians and patients from different hospital units), and time pressure; and (ii) prior studies suggest that DTs can play a role for coping with such complexity and supporting RP – e.g., blood bank management information systems can support inventory control and use of blood components, big data can predict transfusion reactions and the behavior of blood donors, barcodes integrated with the internet of things allow for monitoring patient reactions in real-time, while artificial intelligence algorithms predict transfusion needs and support on-time deliveries of blood components as shown in Figure 1 [3].

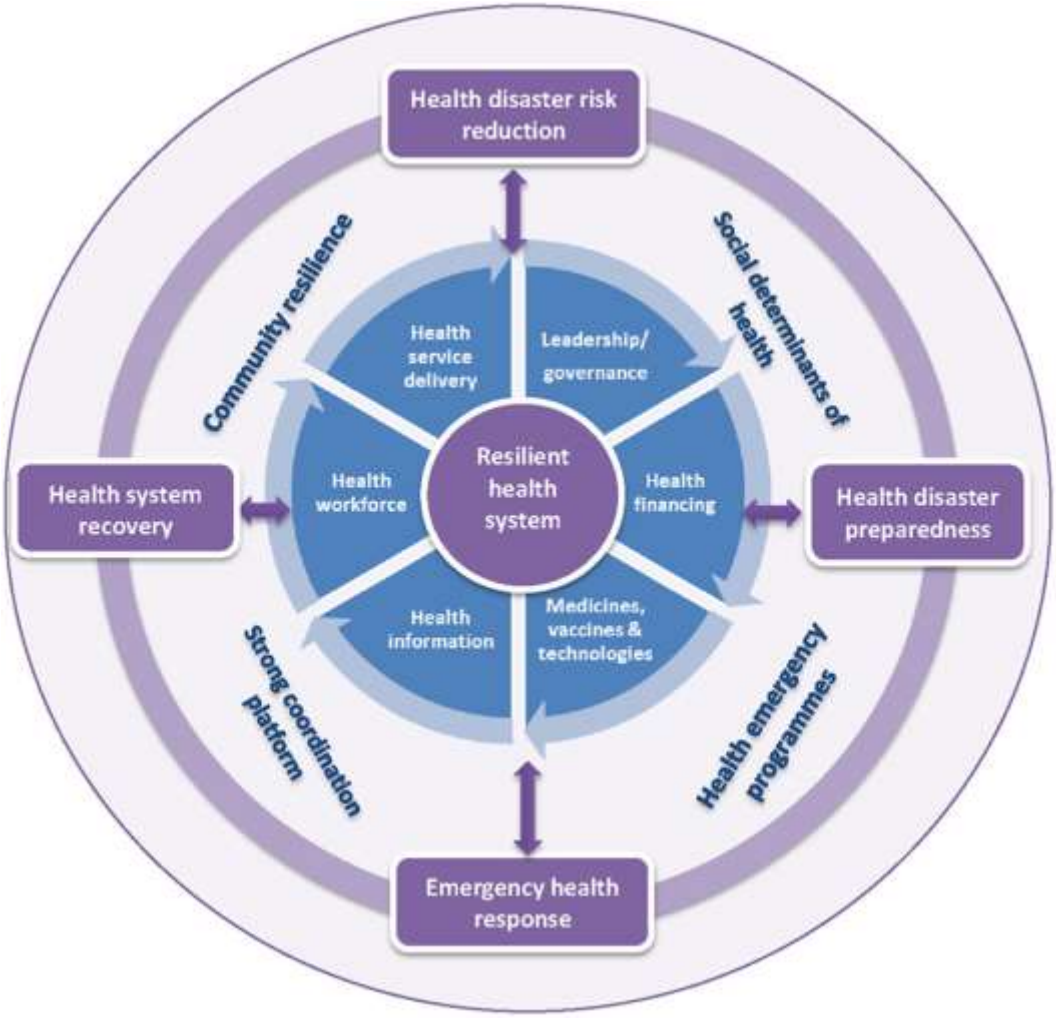


**Figure 1:** The health system building blocks as a conceptual framework for public health disaster risk management.

To thrive in the digital age, healthcare enterprises must adopt a holistic approach to risk management, integrating technological advancements with strategic governance and human expertise. A well-designed, resilient system not only mitigates risks but also enhances the agility and adaptability of healthcare organizations. By prioritizing security, compliance, and operational efficiency, enterprise healthcare systems can achieve sustainable growth while maintaining the highest standards of patient care. This review explores the essential components of risk management in modern healthcare enterprises, outlining strategies for building resilient digital infrastructures in an era of rapid technological change.

1. **Frameworks for mitigating cyber risks**

As healthcare systems become increasingly digitized, cyber risks such as data breaches, ransomware attacks, and system vulnerabilities pose significant threats to patient safety and operational continuity. Effective mitigation of these risks requires structured frameworks that

integrate proactive threat detection, incident response strategies, and regulatory compliance. Cybersecurity frameworks provide a systematic approach for healthcare enterprises to assess, manage, and reduce their exposure to cyber threats while ensuring compliance with industry standards and best practices. One widely adopted framework is the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), which offers a risk-based approach to managing cybersecurity threats. The NIST CSF consists of five core functions: Identify, Protect, Detect, Respond, and Recover. These functions help healthcare organizations build a comprehensive security posture by identifying vulnerabilities, implementing protective measures, monitoring systems for threats, responding to incidents in real-time, and ensuring swift recovery after cyberattacks. The adaptability of this framework makes it particularly effective for healthcare enterprises of all sizes (Figure 2) [4-7].

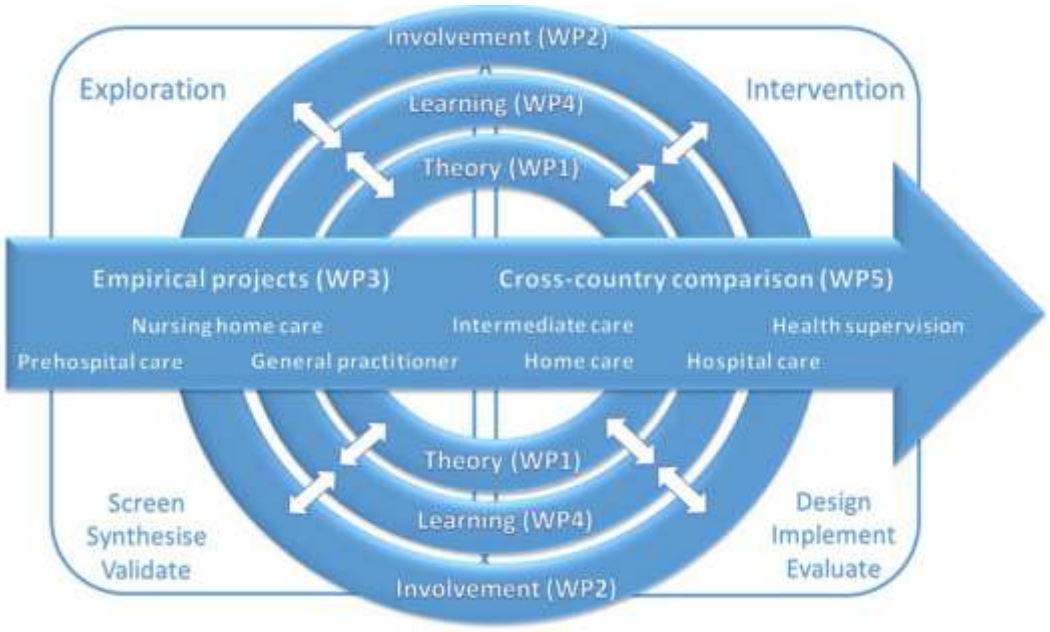


**Figure 2:** The health system building blocks as a conceptual framework for public health disaster risk management.

Another essential framework is the Health Information Trust Alliance (HITRUST) Common Security Framework (CSF), which is specifically designed for the healthcare industry. HITRUST CSF integrates various standards, including HIPAA, NIST, and ISO/IEC 27001, to provide a unified approach to cybersecurity and regulatory compliance. By implementing HITRUST CSF, healthcare organizations can streamline risk management efforts, ensuring that security protocols align with both industry requirements and emerging cyber threats. This framework also facilitates third-party risk management by ensuring that vendors and partners maintain strong cybersecurity practices. The ISO/IEC 27001 framework is another internationally recognized standard that focuses on information security management systems (ISMS). This framework emphasizes a continuous risk management process,

requiring organizations to systematically identify, assess, and mitigate cyber risks while fostering a culture of security awareness. ISO/IEC 27001 provides a structured approach for data protection, reducing the likelihood of breaches and ensuring business continuity. For healthcare enterprises handling vast amounts of sensitive patient data, adopting this framework strengthens resilience against evolving cyber threats. In addition to these frameworks, healthcare organizations must integrate zero-trust security models, robust encryption protocols, and continuous employee training programs to enhance their cybersecurity defenses [8-13]. A multi-layered approach that combines technical safeguards, regulatory adherence, and a proactive security culture is essential for mitigating cyber risks in enterprise healthcare systems. By leveraging well-established cybersecurity frameworks and continuously evolving their security strategies, healthcare organizations can safeguard patient data, maintain regulatory compliance, and ensure the resilience of their digital infrastructure in an increasingly complex threat landscape (Fig 3).


**Figure 3:** Resilience in health records system.

## 2. Impact of cyber threats on patient care

Disasters whether natural or man-made, pose major challenge to human health and development in Africa; their impact on the health of individuals and communities are often

severe and could hinder attainment of global, regional, and national development goals (1–3). Recent disasters in Africa aptly illustrate the complex interaction between health systems and disasters; a vicious cycle in which weak health systems provide fertile grounds for deterioration of public health and natural hazards into disasters while on the other hand, disasters further decimate already weak health systems [4]. The sustained transmission of the 2014/15 Ebola virus disease outbreak in Guinea, Liberia, and Sierra Leone was consistently linked to the weak health systems in these countries [5, 6]. The outbreak resulted in the death of several health workers [7], depletion of scarce financial resources, diversion of medical equipment. This in addition to overburdening of already weak health information and supply chain management systems resulted in disruption of health services delivery in these countries [8–10]. Other disasters such as the Yellow Fever outbreaks in Angola, Democratic Republic of Congo and Uganda, and ongoing armed conflicts in South Sudan, Central Africa Republic, northeast Nigeria, and other African countries also had similar consequences [11–14]. This pattern is not limited to Africa; the fragile pre-disaster health systems in the city of New Orleans in America and the Eastern Visayas Region of the Philippines contributed to the public health consequences of Hurricane Katrina and Haiyan (Yolanda) and constrained timely and effective post-disaster health system recovery efforts [13]. The pre-Katrina health system in the city of New Orleans was characterized by low coverage of health insurance and reduced access to health services by the largely poor population of the city [12]. Similar challenges such as inadequate health-care infrastructure, staffing, and low coverage of health insurance, which reduced access to health services were also prevalent in the affected areas of the Philippines pre-Hurricane Haiyan

## 3. Real-world case studies on resilient healthcare IT

The integration of information technology (IT) into healthcare systems has transformed the delivery of medical services, improving efficiency, accuracy, and patient outcomes. However, with these advancements come significant challenges, including cybersecurity threats, system failures, and data breaches. To ensure continuity and resilience, healthcare organizations have implemented robust IT strategies to mitigate risks and enhance adaptability. This section explores real-world case studies of healthcare institutions that have successfully implemented resilient IT frameworks, focusing on cybersecurity, disaster recovery, interoperability, and digital transformation. Mayo Clinic, one of the most renowned healthcare institutions globally, has prioritized cybersecurity as a fundamental aspect of its IT resilience strategy. Recognizing the increasing threats of ransomware attacks and data breaches, Mayo Clinic implemented a multi-layered cybersecurity framework. This framework includes advanced threat detection systems powered by artificial intelligence (AI), continuous network monitoring, and strict access control measures. Additionally, Mayo Clinic established a Security Operations Center (SOC) to respond to cyber threats in real time. The institution also adopted the National Institute of Standards and Technology (NIST) Cybersecurity Framework to ensure compliance with best practices and regulatory standards. In 2021, when healthcare systems were targeted by a wave of ransomware attacks, Mayo Clinic's resilience strategy proved effective. Its network segmentation and real-time threat

detection mechanisms prevented malware from spreading across critical healthcare systems. The incident response team swiftly contained the threat, ensuring that patient care was not disrupted. This case highlights the importance of proactive cybersecurity measures in safeguarding sensitive healthcare data and maintaining operational continuity.

Natural disasters and unexpected system failures can severely impact healthcare delivery. Cleveland Clinic, a leading medical institution, has implemented a comprehensive disaster recovery (DR) and business continuity plan to ensure resilience against IT failures and external disruptions. Cleveland Clinic's IT resilience strategy revolves around geographically distributed data centers and cloud-based backup systems. In 2018, when a severe snowstorm caused power outages across Ohio, Cleveland Clinic activated its DR plan. The institution seamlessly transitioned to its secondary data center, ensuring that electronic health records (EHRs) remained accessible and critical systems continued functioning. The success of this response was attributed to regular DR drills, real-time data replication, and automated failover mechanisms. By prioritizing redundancy and preparedness, Cleveland Clinic demonstrated how a well-structured disaster recovery plan can minimize downtime and maintain essential healthcare services during emergencies. Interoperability is a crucial aspect of resilient healthcare IT, enabling seamless data exchange between different healthcare providers and institutions. Singapore's Ministry of Health launched the National Electronic Health Record (NEHR) system to improve healthcare coordination and patient outcomes. The NEHR system consolidates patient records from various healthcare providers, ensuring that critical medical information is accessible across different hospitals, clinics, and primary care facilities. The system employs strict cybersecurity protocols, including encryption, multi-factor authentication, and real-time audit trails to prevent unauthorized access. During the COVID-19 pandemic, the resilience of the NEHR system was tested as healthcare facilities experienced an unprecedented surge in patient admissions. The system efficiently handled increased data traffic, enabling healthcare providers to make informed decisions quickly. By ensuring real-time access to patient records, Singapore's NEHR system exemplifies how interoperability and IT resilience can enhance healthcare efficiency, particularly in crisis situations.

The United Kingdom's National Health Service (NHS) has undergone significant digital transformation to enhance IT resilience and improve patient care. One of its major initiatives, NHS Digital, focuses on implementing robust IT solutions, including artificial intelligence (AI)-driven diagnostics, cloud computing, and cybersecurity enhancements. A notable example of NHS Digital's resilience was the response to the 2017 WannaCry ransomware attack, which affected healthcare organizations worldwide. The attack disrupted thousands of NHS computers, causing delays in patient care. Following the incident, NHS Digital implemented a comprehensive cybersecurity overhaul, including mandatory system updates, enhanced endpoint protection, and staff cybersecurity training programs. Additionally, NHS Digital has been instrumental in rolling out telemedicine services, particularly during the COVID-19 pandemic. The rapid deployment of virtual consultation platforms ensured that patients continued receiving medical care despite lockdowns and hospital capacity

constraints. This case study underscores the importance of continuous digital transformation in building resilient healthcare IT infrastructures. Predictive analytics powered by artificial intelligence (AI) is playing a pivotal role in building resilient healthcare IT systems. Kaiser Permanente, one of the largest healthcare providers in the United States, has integrated AI-driven analytics to enhance patient care and operational efficiency. Kaiser Permanente uses AI models to predict patient deterioration, optimize hospital resource allocation, and detect potential cybersecurity threats. For instance, its predictive analytics platform monitors patient data in real-time, identifying early signs of sepsis and alerting medical teams for timely intervention. This proactive approach has significantly reduced mortality rates and improved patient outcomes. Furthermore, Kaiser Permanente's AI-driven cybersecurity systems continuously analyze network activity to detect and respond to potential threats before they escalate. By integrating AI into its IT resilience strategy, Kaiser Permanente exemplifies how data-driven insights can enhance both patient care and cybersecurity preparedness [14-20]

Resilient healthcare IT systems are essential for ensuring uninterrupted patient care, safeguarding sensitive data, and adapting to evolving challenges. The real-world case studies discussed in this section demonstrate various approaches to IT resilience, including cybersecurity frameworks, disaster recovery plans, interoperability initiatives, digital transformation, and AI-driven predictive analytics. Mayo Clinic's proactive cybersecurity strategy highlights the importance of real-time threat detection and response mechanisms. Cleveland Clinic's disaster recovery plan showcases how redundancy and preparedness can minimize disruptions during crises. Singapore's NEHR system exemplifies the benefits of interoperability in enhancing healthcare coordination. NHS Digital's response to the WannaCry attack and its telemedicine advancements illustrate the necessity of continuous digital transformation. Lastly, Kaiser Permanente's AI-driven predictive analytics demonstrate how data insights can improve patient care and cybersecurity resilience. As healthcare organizations continue to adopt digital technologies, it is imperative to implement comprehensive IT resilience strategies. By learning from these real-world case studies, healthcare providers can develop robust frameworks that ensure the security, efficiency, and adaptability of their IT infrastructures, ultimately enhancing patient outcomes and operational stability.

## Conclusion

This study investigated the question of how problems and countermeasures can be identified to inform the design of digital technologies supportive of resilient performance in health services.

The question was addressed by the proposal and testing of a five-step framework. The study of the blood transfusion process shed light on the framework's utility and ease of use, giving rise to seven propositions that support the framework application, grounded on principles of DfRP. Moreover, these propositions were also associated with six generic requirements of DTs supportive of RP. Altogether, the framework, the propositions, and the requirements, pointed to areas and ways in which DTs influence RP, namely (1) using process mapping

(e.g., BPMN): to bridge the perspectives of DTs designers and human factors experts; (2) supporting dynamic prioritization of orders; (3) standardizing interactions between management information systems; (4) buying time for the deployment of responses to variabilities; (5) complementing rather than fully replacing human skills; (6) facilitating the uptake of perspectives from diverse stakeholders and considering the perspective of DTs themselves; (7) using the framework to learn how to develop resilient health services supported by DTs. These contributions address gaps in prior investigations by mapping attributes or functionalities of DTs onto resilience management frameworks (i.e., the principles of DfRP) as well as by providing guidance to the design of DTs assistive of RP. Regarding managerial contributions, members of project teams responsible for process improvement in hospitals can use the framework as a source of ideas to design resilient services supported by DTs. This study reinforces existing recommendations for a socio-technical approach to the design of DTs' while highlighting principles of DfRP that deserve attention when RP is a core desired performance dimension. Some limitations of this study must be acknowledged. Firstly, the case study context (large tertiary hospital pursuing EMRAM certification level 5) can have influenced the nature of the propositions and the requirements. Nevertheless, low digital maturity levels are still predominant in healthcare, adding to the external validity of this study. Future studies should be conducted in other hospital processes and levels of EMRAM adoption. For example, investigating DTs related to artificial intelligence as well as other health services will likely unveil additional requirements. Secondly, this study did not explore the role of blood donation, the only supply source. The inclusion of blood donation could shed light on how DTs support RP at the societal level, considering the whole network of health services. Such investigation would require the analysis of the donor perspective, which was not critical in the present study. Thirdly, this work was limited to suggesting the design of new DTs without designing any of them. Future studies could explore the use of our findings to design specific DTs supportive of RP.

**References**


[1] Aase, K., Guise, V., Billett, S., Sollid, S. J. M., Njå, O., Røise, O., Manser, T., Anderson, J. E., & Wiig, S. (2020). Resilience in Healthcare (RiH): A longitudinal research programme protocol. BMJ Open, 10(10), 1–10.

[2] Patterson, E. S. (2018). Workarounds to intended use of health information technology: a narrative review of the human factors engineering literature. Human factors, 60(3), 281-292.

[3] Barret, J. P., Chong, S. J., Depetris, N., Fisher, M. D., Luo, G., Moiemen, N., ... & Matsumura, H. (2020). Burn center function during the COVID-19 pandemic: An international multi-center report of strategy and experience. Burns, 46(5), 1021-1035.

[4] Salehi, V., Salehi, R., Mirzayi, M., & Akhavizadegan, F. (2020). Performance optimization of pharmaceutical supply chain by a unique resilience engineering and fuzzy mathematical framework. Human Factors and Ergonomics in Manufacturing & Service Industries, 30(5), 336-348.

[5] Ellis, R., Hay-David, A. G. C., & Brennan, P. A. (2020). Operating during the COVID-19 pandemic: how to reduce medical error. British Journal of Oral and Maxillofacial Surgery, 58(5), 577-580.

[6] Ravichandran, N., Inaganti, A. C., Muppalaneni, R., & Nersu, S. R. K. (2020). AI-Driven Self-Healing IT Systems: Automating Incident Detection and Resolution in Cloud Environments. Artificial Intelligence and Machine Learning Review, 1(4), 1-11.

[7] Manduva, V.C. (2020) AI-Powered Edge Computing for Environmental Monitoring: A Cloud-Integrated Approach. The Computertech. 50-73.

[8] Pasham, S.D. (2018) Dynamic Resource Provisioning in Cloud Environments Using Predictive Analytics. The Computertech. 1-28.

[9] Ravichandran, N., Inaganti, A. C., Muppalaneni, R., & Nersu, S. R. K. (2020). AI-Powered Workflow Optimization in IT Service Management: Enhancing Efficiency and Security. Artificial Intelligence and Machine Learning Review, 1(3), 10-26.

[10] Manduva, V.C. (2020) How Artificial Intelligence Is Transformation Cloud Computing: Unlocking Possibilities for Businesses. International Journal of Modern Computing. 3(1): 1-22.

[11] Pasham, S.D. (2017) AI-Driven Cloud Cost Optimization for Small and Medium Enterprises (SMEs). The Computertech. 1-24.

[12] Pasham, S.D. (2019) Energy-Efficient Task Scheduling in Distributed Edge Networks Using Reinforcement Learning. The Computertech. 1-23.

[13] Inaganti, A. C., Sundaramurthy, S. K., Ravichandran, N., & Muppalaneni, R. (2020). Zero Trust to Intelligent Workflows: Redefining Enterprise Security and Operations with AI. Artificial Intelligence and Machine Learning Review, 1(4), 12-24.

[14] Inaganti, A. C., Sundaramurthy, S. K., Ravichandran, N., & Muppalaneni, R. (2020). Cross-Functional Intelligence: Leveraging AI for Unified Identity, Service, and Talent Management. Artificial Intelligence and Machine Learning Review, 1(4), 25-36.

[15] Nersu, S. R. K., Kathram, S. R., & Mandaloju, N. (2020). Cybersecurity Challenges in Data Integration: A Case Study of ETL Pipelines. Revista de Inteligencia Artificial en Medicina, 11(1), 422-439.

[16] Srinivas, N., Mandaloju, N., & Nadimpalli, S. V. (2020). Cross-Platform Application Testing: AI-Driven Automation Strategies. Artificial Intelligence and Machine Learning Review, 1(1), 8-17.

[17] Mandaloju, N., Srinivas, N., & Nadimpalli, S. V. (2020). Machine Learning for Ensuring Data Integrity in Salesforce Applications. Artificial Intelligence and Machine Learning Review, 1(2), 9-21.

[18] Sai, K.M.V., M. Ramineni, M.V. Chowdary, and L. Deepthi. Data Hiding Scheme in Quad Channel Images using Square Block Algorithm. in 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI). 2018. IEEE.

[19] Manduva, V.C. (2020) The Convergence of Artificial Intelligence, Cloud Computing, and Edge Computing: Transforming the Tech Landscape. The Computertech. 1-24.

[20] Pasham, S.D. (2020) Fault-Tolerant Distributed Computing for Real-Time Applications in Critical Systems. The Comptertech. 1-29.