

Managing Risk in Medical Software: A Quality Assurance Framework for Healthcare Technology

Noone Srinivas^{1*}, Nagaraj Mandalaju², Siddhartha Varma Nadimpalli³

1Senior Quality Engineer, American Express

2Senior Salesforce Developer

3Sr Cybersecurity Engineer, Moody's Corporation

Abstract

The integration of technology in healthcare has revolutionized patient care and operational efficiency, but it also introduces significant risks associated with medical software. Effective risk management is essential in the quality assurance (QA) process for these systems, given the potential implications for patient safety and data security. This paper explores the critical importance of risk management in medical software, presenting a structured framework for identifying, assessing, and mitigating risks throughout the software development lifecycle (SDLC). The framework incorporates advanced testing techniques, adherence to regulatory standards, and continuous monitoring to enhance the safety, security, and reliability of medical software systems. It underscores the necessity of robust risk management strategies that protect patient data, ensure system functionality, and facilitate high-quality care delivery. By establishing clear protocols for risk assessment and management, healthcare organizations can foster stakeholder confidence and improve overall healthcare outcomes. Ultimately, this manuscript aims to equip healthcare technology developers and quality assurance professionals with the knowledge needed to navigate the complexities of medical software while prioritizing patient safety and regulatory compliance.

Keywords: Medical Software, Assurance, Framework, Healthcare Technology.

Introduction

As healthcare increasingly relies on software solutions, the complexities involved in developing and maintaining medical software systems have grown significantly. These systems, which range from electronic health records (EHR) to clinical decision support systems, are vital for ensuring patient safety and effective care delivery. However, with increased reliance on technology comes the risk of software failures, security breaches, and compliance issues that can jeopardize patient safety and data integrity. To address these challenges, integrating risk management into the quality assurance process is paramount. Risk management in medical software involves a systematic approach to identifying potential hazards, evaluating their impact, and implementing strategies to mitigate risks throughout the software development lifecycle (SDLC). This proactive stance not only helps safeguard patient welfare but also ensures adherence to regulatory standards established by authorities such as the Food and Drug Administration (FDA) and the European Medicines Agency (EMA). The proposed framework for managing risk encompasses several essential components. It emphasizes the use of advanced testing techniques, such as automated testing, stress testing, and usability testing, to evaluate software performance in various scenarios. By rigorously assessing software under realistic conditions, developers can identify vulnerabilities early in the development process. Additionally, the framework advocates for continuous monitoring of medical

software systems post-deployment. This ongoing oversight enables organizations to detect emerging risks, assess software performance, and implement necessary updates or interventions swiftly. By fostering a culture of continuous improvement and responsiveness, healthcare organizations can ensure their systems remain safe and effective throughout their lifecycle. Moreover, effective risk management strategies are vital for protecting patient data, ensuring system functionality, and maintaining the quality of care. The collaboration of stakeholders, including developers, healthcare providers, and regulatory bodies, is essential to create a cohesive approach to risk management. By prioritizing risk throughout the development and deployment phases, organizations can enhance stakeholder confidence and ultimately improve patient outcomes. In this paper, we will delve deeper into the components of a quality assurance framework for medical software, outlining best practices for risk management and discussing the implications of these practices on healthcare technology. By equipping stakeholders with the tools and knowledge necessary for effective risk management, we aim to contribute to the safe, reliable, and efficient delivery of healthcare technology.

Tables

Table 1: Key Components of Risk Management in Medical Software

Component	Description	Importance
Risk Identification	Process of identifying potential risks	Early detection of hazards
Risk Assessment	Evaluating the likelihood and impact of risks	Informed decision-making
Risk Mitigation	Implementing strategies to reduce risks	Enhances safety and reliability
Continuous Monitoring	Ongoing assessment of software performance	Timely response to issues
Regulatory Compliance	Adherence to standards set by regulatory bodies	Ensures legal and safety standards

Table 2: Advanced Testing Techniques in Medical Software

Technique	Description	Benefits
Automated Testing	Using scripts to execute tests without human intervention	Increases efficiency and coverage
Stress Testing	Evaluating software performance under extreme conditions	Identifies breaking points
Usability Testing	Assessing user experience and interaction	Enhances user satisfaction
Security Testing	Identifying vulnerabilities and threats	Protects patient data
Performance Testing	Measuring system responsiveness and stability	Ensures reliability in use

Table 3: Regulatory Standards for Medical Software

Standard	Description	Applicability
----------	-------------	---------------

FDA 21 CFR Part 820	Quality System Regulation for medical devices	U.S. medical software
ISO 13485	International standard for quality management systems	Global medical devices
IEC 62304	Standards for software lifecycle processes	Software used in medical devices
HIPAA	Regulation for protecting patient health information	Healthcare software
CE Marking	Certification for products sold in the European market	European medical software

Table 4: Risk Assessment Matrix

Risk Level	Likelihood	Impact	Risk Category	Action Required
Low	Rare	Minor	Acceptable	Monitor
Moderate	Possible	Moderate	Manage	Implement controls
High	Likely	Major	Mitigate	Immediate corrective actions
Critical	Almost certain	Catastrophic	Avoid	Cease operations or redesign

Table 5: Risk Mitigation Strategies

Strategy	Description	Examples
Design Controls	Implementing safety features during development	Fail-safes, redundancies
Training Programs	Educating staff on risk management practices	Workshops, e-learning courses
Regular Audits	Conducting periodic evaluations of software	Compliance checks, performance reviews
Incident Response Plans	Preparing for potential failures	Established protocols, drills
Continuous Improvement	Ongoing refinement of processes and tools	Feedback loops, iterative testing

Table 6: Key Stakeholders in Medical Software Development

Stakeholder	Role	Responsibilities
Software Developers	Build and maintain software	Design, coding, testing
Quality Assurance Professionals	Ensure software meets quality standards	Testing, documentation, compliance
Regulatory Bodies	Oversee compliance with laws and regulations	Approval, monitoring, guidance
Healthcare Providers	Use the software in clinical settings	Patient care, feedback
Patients	End-users of healthcare technology	Safety, satisfaction

Table 7: Benefits of Continuous Monitoring

Benefit	Description	Impact
Early Detection	Identifying issues before they escalate	Reduces risk of failure
Improved Compliance	Ensuring ongoing adherence to regulations	Maintains legal standing
Enhanced Performance	Monitoring software effectiveness over time	Sustains high-quality care
User Feedback	Collecting insights from end-users	Informs updates and improvements
Data Security	Protecting sensitive information continuously	Safeguards patient data

Table 8: Challenges in Risk Management for Medical Software

Challenge	Description	Solutions
Complexity	Intricacies of software systems	Simplify processes, use tools
Regulatory Changes	Adapting to evolving standards	Stay updated, conduct training
Resource Constraints	Limited time and budget for risk management	Prioritize high-impact areas
Cultural Resistance	Reluctance to adopt new practices	Foster a culture of safety
Integration Issues	Difficulties in aligning tools and processes	Comprehensive planning and testing

Table 9: Software Development Lifecycle Stages

Stage	Activities	Key Deliverables
Requirements	Gathering and analyzing user needs	Requirement specifications
Design	Architectural and detailed design	Design documents
Development	Coding and unit testing	Functional software modules
Testing	Integration, system, and acceptance testing	Test reports
Deployment	Implementing the software in a live environment	Deployed software
Maintenance	Ongoing support and updates	Maintenance logs

Table 10: Common Risks in Medical Software Development

Risk	Description	Mitigation Strategies
Software Bugs	Errors in the code that affect functionality	Rigorous testing and debugging
Data Breaches	Unauthorized access to patient data	Strong encryption and access controls
Non-compliance	Failure to meet regulatory requirements	Regular audits and compliance checks
User Errors	Mistakes made by users during operation	Comprehensive training and user support

System Failures	Breakdowns in software functionality	Robust design and testing protocols
-----------------	--------------------------------------	-------------------------------------

Table 11: Risk Communication Strategies

Strategy	Description	Purpose
Regular Updates	Providing stakeholders with consistent information	Ensures awareness of risks
Risk Reporting	Formal documentation of identified risks	Promotes transparency
Stakeholder Meetings	Gathering key individuals to discuss risks	Collaborative problem-solving
Training Sessions	Educating staff on risk management processes	Builds capacity and knowledge
Feedback Mechanisms	Channels for receiving input on risks	Encourages proactive engagement

Table 12: Best Practices for Quality Assurance in Medical Software

Practice	Description	Benefits
Comprehensive Testing	Ensuring all aspects of the software are tested	Higher quality and reliability
Documentation	Keeping detailed records of processes and changes	Clarity and accountability
Stakeholder Involvement	Engaging all relevant parties in the QA process	Better outcomes and collaboration
Use of Standards	Adhering to established QA frameworks	Consistency and reliability
Training and Development	Ongoing education for QA teams	Enhanced skills and performance

Table 13: Key Metrics for Measuring Software Quality

Metric	Description	Importance
Defect Density	Number of defects per unit of software	Indicates quality level
Test Coverage	Percentage of requirements covered by tests	Assesses thoroughness
Mean Time to Failure	Average time until failure occurs	Reflects reliability
User Satisfaction	Feedback from users regarding software usability	Measures effectiveness
Compliance Rate	Percentage of adherence to regulatory standards	Ensures safety and legality

Table 14: Technologies Supporting Medical Software Risk Management

Technology	Application	Benefits
Automated Testing	Streamlining the testing process	Increases efficiency and accuracy

Machine Learning	Predicting potential risks based on data	Enhances proactive risk management
Cloud Computing	Facilitating data storage and access	Supports scalability and security
Blockchain	Securing patient data and ensuring integrity	Enhances data protection
Analytics Tools	Monitoring software performance and usage	Informs risk assessment

Table 15: Elements of a Risk Management Plan

Element	Description	Purpose
Risk Assessment	Evaluating potential risks	Informs mitigation strategies
Risk Register	Documenting identified risks and their status	Maintains oversight
Communication Plan	Strategies for informing stakeholders	Ensures awareness
Mitigation Measures	Actions taken to reduce risks	Enhances safety
Review Process	Periodic evaluation of the risk management plan	Promotes continuous improvement

Table 16: Common Compliance Challenges in Medical Software

Challenge	Description	Strategies for Mitigation
Evolving Regulations	Keeping up with changes in laws and standards	Regular training and updates
Documentation Gaps	Incomplete records of processes and decisions	Implementing comprehensive documentation practices
Audit Preparedness	Being ready for regulatory audits	Conducting mock audits
Data Security	Protecting sensitive information	Strong cybersecurity measures
User Compliance	Ensuring users follow protocols and standards	Regular training and reminders

Table 17: Risk Management Lifecycle

Phase	Activities	Deliverables
Planning	Establishing risk management objectives	Risk management plan
Identification	Identifying potential risks	Risk register
Analysis	Assessing risks in terms of likelihood and impact	Risk assessment report
Response	Developing strategies to manage risks	Mitigation plans
Monitoring	Ongoing assessment of risks and responses	Monitoring reports

Table 18: Factors Influencing Risk in Medical Software

Factor	Description	Impact
Complexity	The intricacy of the software being developed	Increases potential for failure
User Interaction	The way users interact with the software	Affects usability and satisfaction
Regulatory Environment	The landscape of applicable laws and regulations	Determines compliance requirements
Technological Advances	The introduction of new technologies	May create new risks or opportunities
Development Methodology	The approach taken to develop software	Impacts testing and quality assurance processes

Table 19: Tools for Risk Management in Medical Software

Tool	Purpose	Features
Risk Management Software	Streamlining risk assessment processes	Automated risk identification
Testing Tools	Conducting various types of tests	Comprehensive reporting
Compliance Checklists	Ensuring adherence to regulatory standards	Easy tracking and documentation
Monitoring Systems	Real-time observation of software performance	Alerts for anomalies
Data Encryption Tools	Protecting patient data	Enhanced security measures

Table 20: Future Trends in Risk Management for Medical Software

Trend	Description	Implications
AI in Risk Assessment	Utilizing artificial intelligence to predict risks	Improved accuracy in risk identification
Enhanced Security Protocols	Developing more robust data protection measures	Greater patient data security
Agile Methodologies	Adopting agile practices in software development	Increased flexibility in managing risks
Integration of IoT	Managing risks associated with Internet of Things devices	New challenges in data security and interoperability
User-Centric Design	Focusing on user needs and feedback in software design	Improved usability and reduced errors

Table 21: Examples of Medical Software Risks

Risk Type	Description	Examples
Software Bugs	Flaws in the code that lead to malfunction	Crashes, incorrect calculations
Security Vulnerabilities	Weaknesses that can be exploited by attackers	Data breaches, unauthorized access

Compliance Issues	Failure to meet regulatory requirements	Incomplete documentation, audits
Usability Problems	Challenges faced by end-users	Confusing interfaces, error-prone processes
Integration Challenges	Difficulties in connecting with other systems	Incompatibility, data silos

Table 22: Risk Management Roles and Responsibilities

Role	Responsibilities	Required Skills
Project Manager	Oversee risk management strategies	Leadership, communication
QA Specialist	Conduct testing and validate software quality	Analytical skills, attention to detail
Regulatory Affairs Manager	Ensure compliance with law and regulations	Knowledge of regulations, advocacy
Security Analyst	Identify and mitigate security risks	Cybersecurity expertise
Software Developer	Implement risk management practices in coding	Programming skills, problem-solving

Table 23: Risk Management Best Practices

Best Practice	Description	Benefits
Regular Training	Continuous education on risk management techniques	Enhances team competence
Cross-Functional Teams	Involving diverse expertise in risk management	Comprehensive risk assessment
Root Cause Analysis	Investigating the underlying causes of risks	Prevents recurrence
Scenario Planning	Developing strategies for potential risk scenarios	Improves preparedness
Continuous Improvement	Ongoing refinement of processes based on feedback	Enhances overall quality

Table 24: Common Tools Used in Risk Management

Tool	Purpose	Features
JIRA	Issue and project tracking	Workflow management, reporting
RiskWatch	Risk assessment and management	Risk scoring, compliance tracking
Microsoft Excel	Data organization and analysis	Customizable risk matrices
Trello	Task management and project organization	Visual task tracking
TestRail	Test case management	Test execution tracking, reporting

Table 25: Risk Assessment Techniques

Technique	Description	Use Cases
Qualitative Analysis	Subjective evaluation of risks	Early-stage risk identification
Quantitative Analysis	Statistical evaluation of risks	Detailed risk analysis
SWOT Analysis	Assessing strengths, weaknesses, opportunities, threats	Strategic planning
FMEA (Failure Mode and Effects Analysis)	Identifying potential failure points and their impacts	Product design and testing
Bowtie Analysis	Visual representation of risk pathways and controls	Comprehensive risk visualization

Table 26: Impact of Technology on Risk Management

Technology	Impact on Risk Management	Challenges
Artificial Intelligence	Enhances predictive analytics for risk identification	Data quality and interpretability
Cloud Computing	Facilitates real-time monitoring and data storage	Compliance and security concerns
Big Data Analytics	Enables analysis of large datasets for trends	Complexity in data management
Blockchain	Provides secure data handling and audit trails	Integration with existing systems
Internet of Things (IoT)	Increases data sources but adds vulnerabilities	Security and interoperability

Table 27: Financial Implications of Risk Management

Area	Potential Costs	Benefits
Compliance Fines	Costs associated with regulatory non-compliance	Avoidance of legal penalties
Incident Response	Expenses related to handling data breaches	Protects reputation and trust
Software Failures	Costs from software malfunction or downtime	Increased operational reliability
Training Programs	Investment in staff education on risk management	Enhanced team capabilities
Quality Assurance	Budget for testing and validation processes	Improved product quality

Table 28: Metrics for Monitoring Risk Management Effectiveness

Metric	Description	Target Values
Number of Incidents	Count of security or compliance incidents	Decrease over time
Compliance Rate	Percentage of compliance with regulations	100% compliance
User Satisfaction	Survey results regarding software usability	Above 85% satisfaction
Risk Mitigation Success	Rate of successfully mitigated risks	Increase year-over-year

Training Completion	Percentage of staff completing risk management training	100% completion rate
---------------------	---	----------------------

Table 29: User Feedback Mechanisms

Mechanism	Description	Purpose
Surveys	Gathering user opinions on software usability	Identifying usability issues
Focus Groups	Group discussions to gather detailed feedback	In-depth insights on user experience
Bug Reporting Systems	Formalized processes for reporting software issues	Streamlines issue identification
Usability Testing Sessions	Observing real users interact with the software	Direct feedback on design flaws
User Forums	Community platforms for sharing experiences	Enhances peer support and feedback

Table 30: Future Challenges in Medical Software Risk Management

Challenge	Description	Potential Solutions
Rapid Technological Change	Keeping up with emerging technologies	Continuous learning and adaptation
Increasing Regulations	Adapting to new laws and standards	Proactive compliance strategies
Cybersecurity Threats	Growing sophistication of cyber-attacks	Enhanced security measures
Integration of New Technologies	Incorporating AI and IoT into existing systems	Comprehensive integration plans
Patient Privacy Concerns	Ensuring data protection amid increased digitalization	Strong data governance policies

Conclusion

Managing risk in medical software is an essential component of ensuring patient safety and maintaining high-quality healthcare delivery. As the healthcare landscape becomes increasingly complex, with the integration of advanced technologies and growing regulatory requirements, the need for a structured risk management framework is more critical than ever. This framework must encompass all stages of the software development lifecycle, from initial planning through post-deployment monitoring. The structured approach outlined in this paper emphasizes several key elements: the identification, assessment, and mitigation of risks through advanced testing techniques, compliance with regulatory standards, and continuous monitoring. These components work synergistically to detect vulnerabilities early in the development process, thereby enhancing the reliability and effectiveness of medical software solutions. By implementing robust risk management practices, healthcare organizations can ensure that they are not only compliant with regulations but also prioritizing patient safety and operational efficiency. Furthermore, fostering a culture of risk awareness across all levels of an organization is vital. It involves engaging stakeholders—including software developers, quality assurance professionals, healthcare

providers, and patients—in discussions about risk management. This collaborative environment enhances communication and facilitates a shared understanding of risks, ultimately leading to better decision-making and outcomes. As technological advancements continue to reshape the healthcare landscape, organizations must remain vigilant and adaptable. The incorporation of emerging technologies such as artificial intelligence and machine learning can significantly enhance risk assessment capabilities, allowing for more proactive and predictive management of potential threats. Additionally, as the complexity of medical software increases, the integration of user-centric design principles will be essential for addressing usability issues and ensuring that software meets the needs of its users. A robust quality assurance framework that emphasizes risk management is critical for the successful deployment of medical software. By embracing effective risk management strategies, organizations can protect patient data, ensure system functionality, and maintain high standards of care delivery. This not only enhances patient outcomes but also builds trust among stakeholders and strengthens the overall integrity of healthcare systems. As we move forward, prioritizing risk management in medical software will be essential for navigating the challenges and opportunities presented by an ever-evolving digital health landscape.

References

- [1] Syed, Fayazoddin Mulla. "Ensuring HIPAA and GDPR Compliance Through Advanced IAM Analytics." *International Journal of Advanced Engineering Technologies and Innovations* 1, no. 2 (2018): 71-94.
- [2] Nersu, S. R. K., Kathram, S. R., & Mandalaju, N. (2020). Cybersecurity Challenges in Data Integration: A Case Study of ETL Pipelines. *Revista de Inteligencia Artificial en Medicina*, 11(1), 422-439.
- [3] Nersu, S. R. K., Kathram, S. R., & Mandalaju, N. (2021). Automation of ETL Processes Using AI: A Comparative Study. *Revista de Inteligencia Artificial en Medicina*, 12(1), 536-559.
- [4] Mandalaju, N. kumar Karne, V., Srinivas, N., & Nadimpalli, SV (2021). A Unified Approach to QA Automation in Salesforce Using AI, ML, and Cloud Computing. *ESP Journal of Engineering & Technology Advancements (ESP-JETA)*, 1(2), 244-256.
- [5] Suvvari, S. K. (2020). Agile Risk Management: Strategies And Techniques For Mitigating Project Risks. *Webology* (ISSN: 1735-188X), 17(4).
- [6] Munagandla¹, V. B., Nersu, S. R. K., Kathram, S. R., & Pochu, S. (2019). Leveraging Data Integration to Assess and Improve Teaching Effectiveness in Higher Education. *Unique Endeavor in Business & Social Sciences*, 2(1), 1-13.
- [7] Munagandla¹, V. B., Pochu, S., Nersu, S. R. K., & Kathram, S. R. (2019). A Microservices Approach to Cloud Data Integration for Healthcare Applications. *Unique Endeavor in Business & Social Sciences*, 2(1), 14-29.
- [8] Nersu, S. R. K., Kathram, S. R., & Mandalaju, N. (2020). Cybersecurity Challenges in Data Integration: A Case Study of ETL Pipelines. *Revista de Inteligencia Artificial en Medicina*, 11(1), 422-439.
- [9] Kathram, S. R., & Nersu, S. R. K. (2020). Adopting CICD Pipelines in Project Management Bridging the Gap Between Development and Operations. *Revista de Inteligencia Artificial en Medicina*, 11(1), 440-461.
- [10] Munagandla¹, V. B., Nersu, S. R. K., Kathram, S. R., & Pochu, S. (2020). Student 360: Integrating and Analyzing Data for Enhanced Student Insights. *Unique Endeavor in Business & Social Sciences*, 3(1), 17-29.

- [11] Munagandla¹, V. B., Nersu, S. R. K., Pochu, S., & Kathram, S. R. (2020). Distributed Data Lake Architectures for Cloud-Based Big Data Integration. *Unique Endeavor in Business & Social Sciences*, 3(1), 1-16.
- [12] Nersu, S. R. K., Kathram, S. R., & Mandalaju, N. (2021). Automation of ETL Processes Using AI: A Comparative Study. *Revista de Inteligencia Artificial en Medicina*, 12(1), 536-559.
- [13] Pochu, S., Munagandla, V. B., Nersu, S. R. K., & Kathram, S. R. (2021). Multi-Source Data Integration Using AI for Pandemic Contact Tracing. *Unique Endeavor in Business & Social Sciences*, 4(1), 1-15.
- [14] Kathram, S. R., & Nersu, S. R. K. (2022). Effective Resource Allocation in Distributed Teams: Addressing the Challenges of Remote Project Management. *Revista de Inteligencia Artificial en Medicina*, 13(1), 615-634.
- [15] Kathram, S. R., & Nersu, S. R. K. (2022). Enhancing Software Security through Agile Methodologies and Continuous Integration. *Journal of Multidisciplinary Research*, 8(01), 26-37.
- [16] Pochu, S., & Nersu, S. R. K. (2022). Cybersecurity in the Era of Quantum Computing: Challenges and Solutions. *Journal of Multidisciplinary Research*, 8(01), 01-13.
- [17] Nersu, S. R. K., & Kathram, S. R. (2022). Harnessing Federated Learning for Secure Distributed ETL Pipelines. *Revista de Inteligencia Artificial en Medicina*, 13(1), 592-615
- [18] Ghali, A.A., S. Jamel, K.M. Mohamad, N.A. Yakub, and M.M. Deris. (2017) A review of iris recognition algorithms. *JOIV: International Journal on Informatics Visualization*. 1(4-2): 175-178.
- [19] Ghali, A.A., S. Jamel, Z.A. Pindar, A.H. Disina, and M.M. Daris. Reducing error rates for iris image using higher contrast in normalization process. in *IOP Conference Series: Materials Science and Engineering*. 2017. IOP Publishing.
- [20] Pindar, Z.A., S. Jamel, A. Disina, A.R. Ghali, and M.M. Deris. Check Digit System Based on Quasigroup String Transformation. in *IOP Conference Series: Materials Science and Engineering*. 2017. IOP Publishing.
- [21] Belanda, S.E., A.A. Ghali, S. Jamel, and M.M. Deris. A Two-Way Image Quality Enhancement for Iris Recognition System Using Modified Enhanced Histogram Equalization for Normalization. in *2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*. 2018. IEEE.
- [22] Ghali, A.A., S. Jamel, K.M. Mohamad, S.K.A. Khalid, Z.A. Pindar, and M.M. Deris. An improved low contrast image in normalization process for iris recognition system. in *Recent Advances on Soft Computing and Data Mining: Proceedings of the Third International Conference on Soft Computing and Data Mining (SCDM 2018)*, Johor, Malaysia, February 06-07, 2018. 2018. Springer.
- [23] Aminu Ghali, A., R. Ahmad, and H.S.A. Alhussian. Comparative analysis of DoS and DDoS attacks in Internet of Things environment. in *Artificial Intelligence and Bioinspired Computational Methods: Proceedings of the 9th Computer Science On-line Conference 2020*, Vol. 2 9. 2020. Springer.
- [24] Ghali, A.A., R. Ahmad, and H. Alhussian. (2021) A framework for mitigating ddos and dos attacks in iot environment using hybrid approach. *Electronics*. 10(11): 1282.
- [25] Ghali, A.A., R. Ahmad, and H. Alhussian. A framework for enhancing network lifetime in Internet of things environment using clustering formation. in *International Conference on Artificial Intelligence for Smart Community: AISC 2020*, 17–18 December, Universiti Teknologi Petronas, Malaysia. 2022. Springer.