International Journal of Engineering &Technology, 8 (4) (2019) 552-558

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



A state of the art fuzzy based healthcare risk management for health information exchange

Amarendar Rao Thangeda [1] *, Alfred Coleman [2]

[1] Research Scholar, University of South Africa, South Africa and Senior Lecturer in Faculty of Computing, Botho University, Botswana
[2] Professor and Director, Department of Computer Science, University of South Africa, South Africa
**Corresponding author E-mail: amarendar.thangeda@bothouniversity.ac.bw*

Abstract

The Today health-care organizations and physicians use several processes and instruments to exchange data about the private health of patients electronically. The main aims of the different methods of information (HIE) exchange on health are to reduce healthcare costs, to minimize medical errors and to better coordinate health services. Risks of information assets have a complex nature and different approaches address risk management of information security in medial field. The objective of this paper is to create the state-of - the-art information security risk management. In order to accomplish this, a Fuzzy based Healthcare Risk Management is suggested. This research aimed at exploring the core importance of the Fuzzy based Healthcare Risk Management (FHRM) from the views of health care consumers in the health sector. The result shows that the views of patients on multiple mechanisms for exchanging data about patient privacy, trust in competence and integrity and readiness to share data are significantly different.

Keywords: *Health Information Exchange; Fuzzy Based Healthcare Risk Management (FHRM); Patients Monitoring.*

1. Introduction

This the security of information is a discipline that carries out a growing amount of empirical research and publishes them. Although this increase was observed, limited research focused on the risks to health information security [1]. Many researches is focused on IT solutions and is limited to data where it is kept on a perimetric basis and protected from external threats [2]. Almost 60 years of management of information security have, however, changed risk perception, and risk analysis should now generally be agreed from a broader perspective. This is likely to be more so in today's health, a complicated environment that does not always separate technologies, risks to humans and the services level and the geographic range [3].
Risk management includes clinical and administrative systems, processes and reports for risk detection, monitoring, evaluation, mitigation and prevention [4]. Health organizations proactively and systemically protect the safety of patients, property, market share of the organization, accreditation levels, payment, brand value and community status through risk management [5]. It is difficult to establish the limits of what is the healthcare organizations as entities within the scale, epidemiology, diagnosis, treatment, assurance, internet services, transportation or science services range [6].

1.1. Risk management value and purpose in healthcare organizations

Deployments in health risk management have traditionally focused on the important role played by patient safety and the reduce in medical errors, which influence the ability of the company to execute and protect against financial liability [7,8]. However, with the growth of medical technology, cyber-security problems are growing, the pace of health science and the evolving regulatory, legal, political and compensatory climate have become more complex over the years. Management of health risk is becoming more and more difficult [9].
Moreover, given the current value-based care movement and risk bearing models, such as bundled payments and CMS payments for the performance programs, financial risks are changing to provide providers with a broader perspective of risk management. In May 2017, Moody's Investor Services published its survey on risk-management relations and the working margins of a hospital: Maintaining a high quality of medicine will increasingly have an effect on economic results and decrease the risk of brand deficiency by moving from a pay-for-service model to higher value and results [10].

Copyright © Amarendar Rao Thangeda, Alfred Coleman. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.



Fig. 1: General Structure of Risk Management.

Therefore, the risk management programs of hospitals and other healthcare systems extend to include primarily reactive programs which promote patient's safety, prevent legal exposure and are increasingly proactive and risk the larger ecological lens [11]. In this research aimed at exploring the core importance of the Fuzzy based Healthcare Risk Management (FHRM) from the views of health care consumers in the health sector. The results show that patients ' opinions on several processes for the exchange of information concerning patient privacy, confidence in competence and integrity, the purpose of opt-in and the willingness to share information differ significantly.

1.2. Increased patient trust and integrity of information through privacy and security

Intelligent expenditures and people who are healthy, suppliers and individuals must use private and secure personal health information to achieve a promise of digital health data in order to improve health outcomes. In the absence of confidence in electronic health records and the exchange of health information for your clients [12], you may not want to provide your clients with healthcare data as you think that their data on electronic health is confidential and accurate. This is one reason why it is so important to ensure the privacy and security of health information. If you and your patients trust you and health data technology (HITs) to communicate their health data and together they take informed decision-making, they will have a more extensive image of their patients ' general health [13].
To enhance patient trust, you need to:

- Keep accurate data in patient records
- Make sure patients have an electronic access to their health records and know how to do that.

2. Literature survey

Security means a reduction in risk to an acceptable level for the organization, business or system operations. Therefore, risk evaluation or analysis methods are fundamental to the security management systems and generally identify the path of threat between assets and potentially attacking individuals in order to characterize remaining risks. The probability and effect of such risks are quantified [14].
There are currently more than 200 practice-oriented risk assessment (PORA) methods and other academic security patterns, although different risk approaches are available, but usually consist of three phases: context-setting, risk identification, and risk analysis. Then the process involves identifying and valuing assets and identifying vulnerabilities, evaluating risk and developing mitigation strategies [15].
Assets are defined as something that has both tangible and intangible value for the organization. Any threat to its availability, integrity and confidentiality [16] will result in serious damage and dysfunctionality for the organization. In any method of risk assessment, asset identification plays a crucial role, because there would be nothing to protect without assets so there would be no security [16].
The identification of assets is linked to many techniques of risk assessment. Some techniques are regarded as being discrete in the' Context Identification Stage (CIS), as in OCTAVE, the Microsoft Security Risk Management Guide (MSRMG) and other techniques like ISO-IEC 27005:2008 [17]. Asset inventory is yet another source of asset identification, but some organizations do not have or are incomplete asset inventory that gives them a wrong impression of their business risk assessment and mitigation vulnerabilities and threats [18].
Under the HIPAA Data Protection and Security Rules, employers are held responsible for their employees ' actions. UCLA health care system employees had, without proper permission, access to records of celebrities in 2011. UCLA has failed to' implement adequate security actions to reduce the risk of unauthenticated access by unauthorized users to an adequate and reasonable level to electronic health information.' The health system has agreed to resolve violations of US Health Department and Civil Rights Office (OCR) for $865,000 for privacy and security. The control of access to health information is crucial but not adequate to protect privacy; the security and protection of patient information requires additional measures, such as extensive training and reliable privacy policies and procedures [19], [20].
The above-mentioned risk management techniques have some drawbacks in information security. This paper is proposed to create the state-of - the-art information security risk management. In order to accomplish this, a Fuzzy based Healthcare Risk Management is suggested. This research aimed at exploring the core importance of the Fuzzy based Healthcare Risk Management (FHRM) from the views of health care consumers in the health sector. The result shows that the views of patients on multiple mechanisms for exchanging data about patient privacy trust in competence and integrity and readiness to share data are significantly different.

3. Fuzzy based healthcare risk management evolution (FHRM)

Hospitals and other installations adopt a more holistic strategy, named Enterprise Risk Management, for expanding the role of risk management across the organizations. Traditional risk management components including patient safety and health liability are incorporated into FHRM and extends the risk management strategy across the organisation to include a "large image."



Fig. 2: Fuzzy Based Healthcare Risk Management Domains.

The figure 2 shows the fuzzy based healthcare risk management domains. The American Society of Healthcare Risk management (ASHRM): "Enterprise risk management in healthcare promotes extensive risk-management process to maximize risk conservation and growth through risk and uncertainty management and their relationship to general value."
FHRM emphasizes further using technology to synchronize risk mitigation efforts across the business and avoid risk in siloed departments or business units. Data analysis is also incorporated in support of decisions, departmental cohesion, priority risk prioritization and allocation of resources. Analytics are essential as a manner of indicating value (what expenses have been prevented) in FHRM initiatives for the monitoring of benchmarks. These FHRM elements are constructed on a governance framework, which aligns business with the risk management scheme.
The role of the health risk management team has evolved to handle and facilitated the FHRM framework in relation to this new governance structure. Risk managers proactively recognize hazards and assess future impacts and upsides. They also formulate plans to respond to hazards. On the other hand, they react and implement containment plans to mitigate organizational exposure when unfavourable and unpredictable situations arise.

3.1. Mathematical model of fuzzy based healthcare risk management (FHRM) evolution

In this paper, we have been proposed the fuzzy based risk management evaluation.

i) Fuzzy numbers and Fuzzy Sets

The fuzzy numbers and fuzzy sets are mathematical theory which is designed to model the uncertainty of risk management process. The degree of membership in a fuzzy set is the key point of fuzzy element. The membership function is denoted by fuzzy set and the elements are mapped to degree of membership in order of time interval [0, 1]. The membership function value is allotted as 0 that means does not have a place with the element set. The membership function value is allotted as 1 that means completely with the element set. The fuzzy set is a special fuzzy number $X = \{(A, \mu(\tilde{X}(A)), A \in R$, where A is the real timehaveeed R and the interval is [0, 1]. We has been used fuzzy triangular number i.e) $\tilde{X} = (t, n, v)$ the following equation (1) as,

$$\mu_{\tilde{x}}(A) = \begin{cases} 0, & A < 1 \text{ or } A > v \\ \frac{A-t}{n-t}, & t \le A \le n \\ \frac{v-A}{v-n}, & n \le A \le v \end{cases} \quad (1)$$

$$\forall \beta \in [0,1]\ \tilde{X}_\beta = [t^\beta, v^\beta] = [(n-t)\beta + 1, -(v-n)\beta + v] \quad (2)$$

As shown in the equation (2) β denotes the confidence level of given interval.
The fuzzy set matrices are compared by using triangular fuzzy number, the following equation (3) and (4) is,

$$\tilde{X} = \begin{bmatrix} \tilde{x}_{11} & \tilde{x}_{12} & \cdots & \tilde{x}_{1m} \\ \tilde{x}_{21} & \tilde{x}_{22} & \cdots & \tilde{x}_{2m} \\ \vdots & & & \vdots \\ \tilde{x}_{m1} & \tilde{x}_{m2} & \cdots & \tilde{x}_{mm} \end{bmatrix} \quad (3)$$

$$\tilde{X} = \begin{bmatrix} \tilde{x}_{11}^{\beta} & \tilde{x}_{12}^{\beta} & \cdots & \tilde{x}_{1m}^{\beta} \\ \tilde{x}_{21}^{\beta} & \tilde{x}_{21}^{\beta} & \cdots & \tilde{x}_{2m}^{\beta} \\ \vdots & & & \vdots \\ \tilde{x}_{m1}^{\beta} & \tilde{x}_{m2}^{\beta} & \cdots & \tilde{x}_{mm}^{\beta} \end{bmatrix} \quad (4)$$

As shown in the equation (4) where β is fixed using this value we can acquired the degree of membership function.

ii) Fuzzy TOPSIS Method

The process of risk management depends on the imprecision, uncertainty and internality of fuzzy extent of fuzzy TOPSIS approach is required. The evaluation of fuzzy TOPSIS method needed the preface of the linguistic variables and other parameter. The fuzzy evaluation of risk management process attributes and weight of every examined criterion.
The pre-face information the following stages are as,
Stage 1: the evaluation of fuzzy decision matrix for the process of risk management, the fuzzy MCDM issue possibly demonstrated as, the following equation (5) is,

$$\tilde{G} = \begin{matrix} \\ L_1 \\ L_2 \\ L_3 \\ \vdots \\ L_4 \end{matrix} \begin{bmatrix} H_1 & H_2 & \cdots & H_m \\ \tilde{a}_{11} & \tilde{a}_{12} & \cdots & \tilde{a}_{1m} \\ \vdots & \ddots & & \\ \vdots & & \ddots & \\ \tilde{a}_{n1} & \tilde{a}_{n2} & \cdots & \tilde{a}_{nm} \end{bmatrix} \tag{5}$$

As shown in the equation (5) where $\tilde{G}$ denotes the fuzzy decision maker along H and L alternatives.
Stage 2: The normalized fuzzy decision matrix $\tilde{T}$ can be expressed as,

$$\tilde{T} = [\tilde{u}_{ji}]_{n*m},\ j = 1,2,\dots m; i = 1,2,\dots n \tag{6}$$

$$\tilde{u}_{ji} = \left(\frac{x_{ji}}{H_i^+}, \frac{y_{ji}}{H_i^+}, \frac{z_{ji}}{H_i^+}\right)\ where\ H_i^+ = \max_j H_{ji} \tag{7}$$

Stage 3: Calculate the decision matrix weight the normalized fuzzy decision matrix is evaluated by using equation (8)

$$\tilde{p}_{ji} = \tilde{u}_{ji} \otimes \tilde{\varphi}_i \tag{8}$$

As shown in the equation (8) Where $\tilde{p} = [\tilde{p}_{ji}]_{n*m}$, j=1, 2,…m; i=1,2,….n.
Stage 4: Compute the positive and negative point ideal distance. The interval range is [0, 1] in triangular fuzzy number in addition of the positive and negative ideal point of reference the following equation (9) as,

$$X^+ = \{\tilde{p}_1^+, \tilde{p}_2^+, \dots \tilde{p}_m^+\},\quad X^- = \{\tilde{p}_1^-, \tilde{p}_2^-, \dots \tilde{p}_m^-\} \tag{9}$$

Where

$$\tilde{p}_i^+ = (1,1,1), \tilde{p}_i^- = (0,0,0)$$

The distance of alternatives from fuzzy TOPSIS method can be expressed by following equation (10), (11) and (12) as,

$$E_j^+ = \sum_{i=1}^m e(\tilde{p}_{ji}, \tilde{p}_i^+),\qquad j = 1,2,\dots m; i = 1,2,\dots n \tag{10}$$

$$E_j^- = \sum_{i=1}^m e(\tilde{p}_{ji}, \tilde{p}_i^-),\qquad j = 1,2,\dots m; i = 1,2,\dots n \tag{11}$$

$$E(\tilde{X}, \tilde{Y}) = \sqrt{\frac{1}{3}[(x_1 - y_1)^2 + (x_2 - y_2)^2 + (x_3 - y_3)^2]} \tag{12}$$

The above mathematical equations are used to calculate the Fuzzy based Healthcare Risk Management Evolution.

3.2. Key components of fuzzy based healthcare risk management evolution (FHRM)

1) Risk identification

As risk management includes the management of uncertainty and the emergence of a new risk, it is difficult to comprehend all the threats threatening a health entity. However, threats and possible compensatory occurrences, which would otherwise be difficult to anticipate, may be revealed by using information, institutional, industrial knowledge and involving all patients, facilities, administrations and health risk managers.

2) Risk quantification and priority

Once recognized, it is important that the hazards are recognized, prioritized based on their probability and influence, that resources are allocated and then allocated to their tasks. For this purpose, Risk Matrices and heat maps can be used for risk visualizations and to encourage communication and decision-making cooperation.

3) Sentinel events investigate & report

The Sentinel Events, coined by a Joint Commission, "is an event that does not have a natural medical history leading to death or serious physical or psychological injury to a patient." If sentinel events take place, rapid response and thorough investigation are designed for the immediate safety of a patient and to reduce the risk of future events. Implementing a plan promotes calm, measurement and transparency of employees and ensures the implementation of corrective actions.

4) Reporting on compliance

The Federal, the State and other supervising bodies, like the Joint Commission, require reports on certain kinds of occurrences, including sentinels, medical errors and dysfunctions in the medical device. Incidents such as miscarriages or surgery, accidents at work, medication errors, etc. should be recorded, coded, and reported.

5) Think of latent failures beyond obviousness

Active errors are clear and easily recognized— for instance, when a nurse provides a patient the incorrect dose of medication. On the other hand, latent failures are often hidden and only revealed by means of analysis and critical examination. Consider fundamental and less readily apparent reasons in investigating the causes of an unfavourable episode.

6) Models for deploy proven incident analysis

Models for accident analysis are used for understanding latent failures, causes and risk relationships. Unemployment and fatigue, for instance, often lead to health errors. The use of well-established models increases the efficiency and efficiency of risk management. FMEA and the Failure Mode and Effect Analysis and Root Cause Analysis also are used to identify the causes and impacts of medical errors with comprehensive frameworks.

7) Robust risk information system investment (RMIS)

On the industry there are multiple reports and risk management platforms. These systems provide information on incidents, risk monitoring, reporting trends, data point benchmarking and industrial sector comparisons. Reports of losses, incidents, open claims and lost time can be generated for injured employees to name a few. RMIS can greatly improve risk management with the help of available and trusted systems, while offering total cost reduction via routine tasks.

8) Financing / transfer / retention of risk right balance

Risk funding includes techniques of financing losses that result from risk effectively and efficiently by an organization. In general, risk transfer is included in policies for insurance and retention such as self-containment and insurance.

9) Developing fuzzy based plan to manage health risk

A strong and continuous Risk Management Plan is necessary to healthcare organisations. The Risk Management Plan is the document to guide an organization's strategic identification, management and risk mitigation. Hospital management and every head of department must be aware of the development and continuing evaluation of the plan and participate in them. In health risk management plans the aim, scope and goals of the risk management protocol of the organization are communicated. They also describe risk manager roles and duties and other risk mitigation personnel. An instance of the Fuzzy based Risk Management Plan for Healthcare is here.

4. Results and discussions

1) Risk Identification

Risk identification is usually a qualitative method that is based mainly on findings, experiences, reports and professional evaluation. This process must be systematic, based on biological, chemical, and physical security principles; Infectious agent transmission techniques; crop design understanding, equipment and practice understanding; personal protective tools; and knowledge of applicable local, state and federal legislation. The proposed FHRM method which have high risk identification ratio compared PORA, MSRMG, CIS, HIPAA. The figure 3 shows the risk identification ratio of FHRM method.

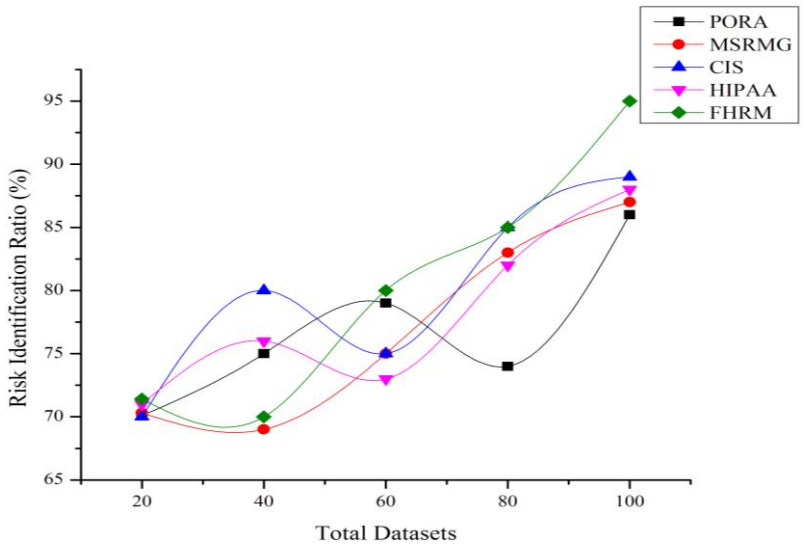


Fig. 3: Risk Identification Ratio of FHRM Method.

2) Dose-response assessment

The dose-response relationship is the next level of risk assessment. This action identifies the relation between the quantitative level of danger and the probability of an adverse reaction. Cumulative-dose effects are relevant to chemical toxicants over years of exposure, however in the case of pathogenic agents single-event exposures are the most frequent concerns. Each episode of potential exposure is considered to increase the cumulative risk for all, but the risk of disease is the same for everyone in the risk group following any single exposure episode. The proposed FHRM method which have high dose-response ratio compared PORA, MSRMG, CIS, HIPAA. The figure 4 shows the dose-response ratio of FHRM method.

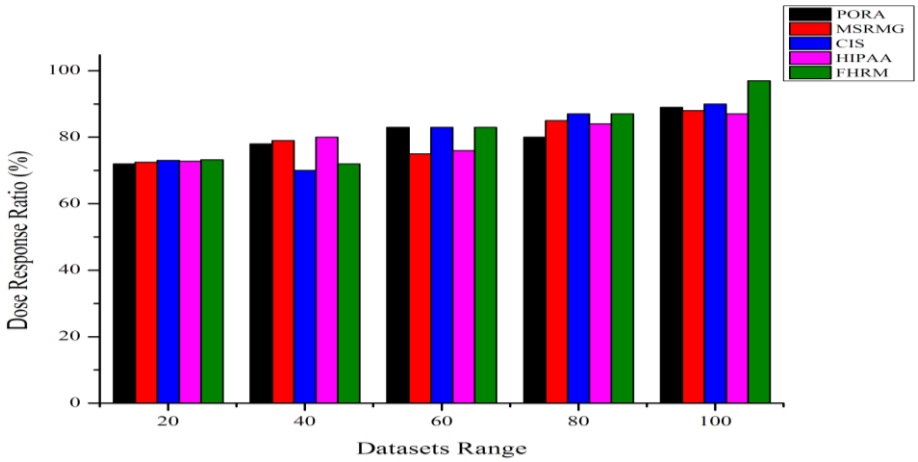


Fig. 4: Dose-Response Ratio of FHRM Method.

3) Exposure assessment

The next stage in the risk assessment has been to identify a hazard and to establish the amount of hazard that produces adverse effects. Several possible contacts such as splashes, bites, aerosols and needle sticks shall be considered in the exposure assessment. In conjunction with their work tasks and the use of personal protective equipment, the amount of contact with potential hazards should be determined. Exposure assessment should include an assessment of people's exposure experiences and ability levels. The proposed FHRM method which have high exposure assessment ratio compared PORA, MSRMG, CIS, HIPAA. The figure 5 shows the exposure assessment ratio of FHRM method.

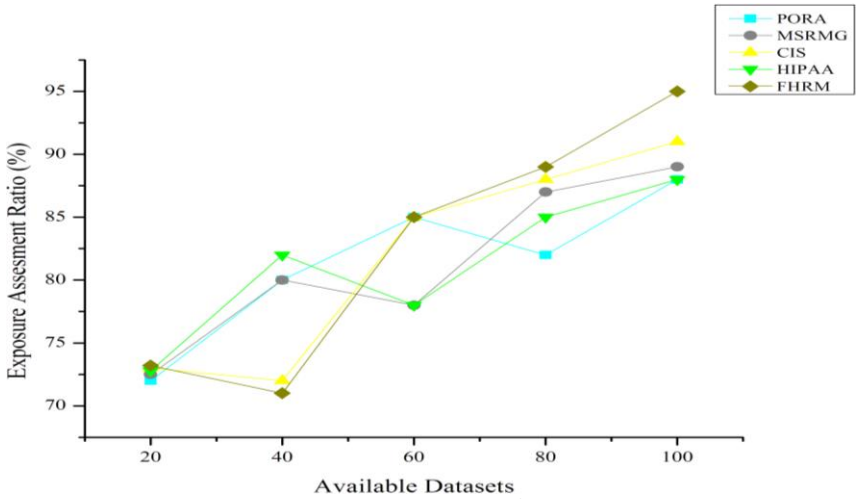


Fig. 5: Exposure Assessment Ratio of FHRM Method.

4) Accuracy

In the lack of trust in Electronic health records and Health Information Exchanges for your patients, they may not want to provide health care information to your patients because they feel that the confidentiality and accuracy of their electronic health information is at risk. That is one reason why ensuring the privacy and safety of health data is so essential to you. You and your patients will have a more comprehensive picture of the overall health of their patients when they trust you and health information technology (HITs) to share their health information, and together they will take more informed decisions. The proposed FHRM method which have high accuracy ratio compared PORA, MSRMG, CIS, HIPAA. The figure 6 shows the Accuracy ratio of FHRM method.

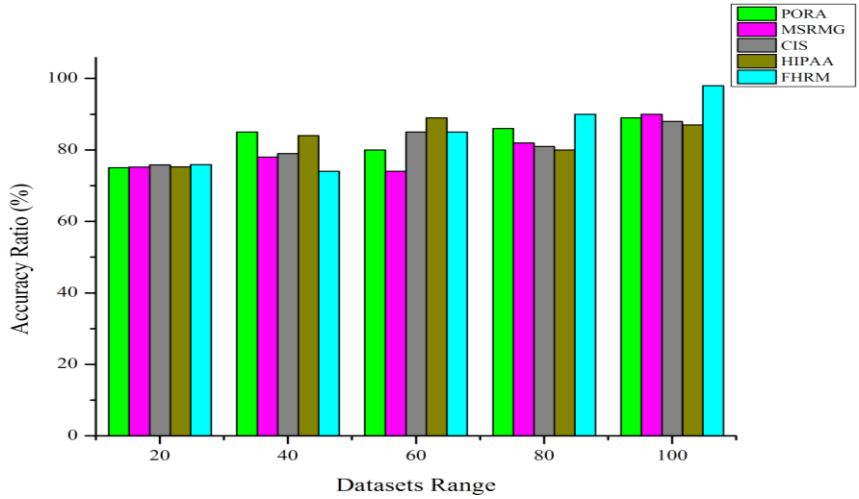


Fig. 6: Accuracy Ratio of FHRM Method.

5) Risk Estimation and Characterization

Once the hazard has been recognized, other risk assessment measures are intended to evaluate hazards connected with recognized hazards institutions. A wide vast range of analytical tools are used to identify the likelihood of an event in a specified interval, the sources and the magnitude of uncertainty and variability in the estimates, including quality, semiquantitative and quantitative methods. The proposed FHRM method which have high risk estimation ratio compared PORA, MSRMG, CIS, HIPAA. The figure 7 shows the risk estimation ratio of FHRM method.

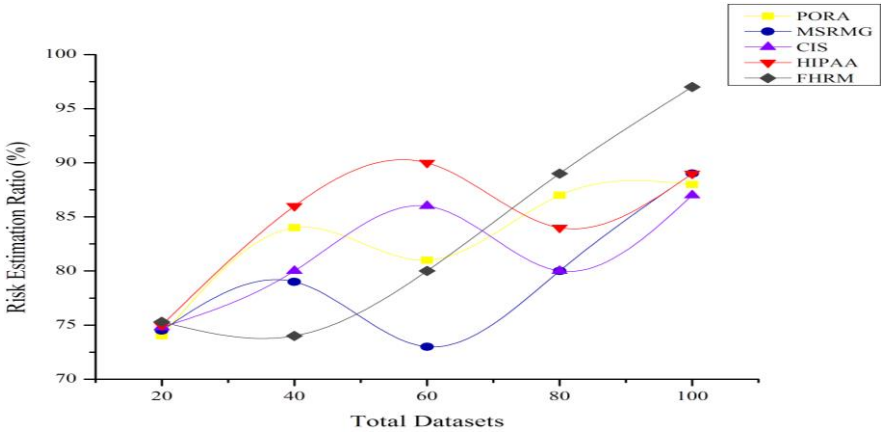


Fig. 7: Risk Estimation Ratio of FHRM Method.

5. Conclusion

This research performed an assessment of the safety of health information. Fire was a high probability / high impact risk factor among the risk for information security. Human, physical / environmental threats were among the risk variables of low probability. The risk factors for high probability require rapid corrective actions. Risks of information assets have a complex nature and different approaches address risk management of information security in medial field. The objective of this paper is to create the state-of - the-art information security risk management. In order to accomplish this, a Fuzzy based Healthcare Risk Management is suggested. This research aimed at exploring the core importance of the Fuzzy based Healthcare Risk Management (FHRM) from the views of health care consumers in the health sector. Therefore, before adverse effects occur, the underlying causes of such threats should be recognized and monitored. It is essential to note that data safety in health systems has to be taken into account at macro-level in terms of domestic interests and policies.

References

[1] Buntin, M. B., Burke, M. F., Hoaglin, M. C., & Blumenthal, D. (2011). The benefits of health information technology: a review of the recent literature shows predominantly positive results. *Health affairs*, *30*(3), 464-471. https://doi.org/10.1377/hlthaff.2011.0178.

[2] Kavaler, F., & Spiegel, A. D. (2003). *Risk management in health care institutions: a strategic approach*. Jones & Bartlett Learning.

[3] Carroll, R. (Ed.). (2009). *Risk management handbook for health care organizations* (Vol. 30). John Wiley & Sons.

[4] Sittig, D. F., & Singh, H. (2015). A new socio-technical model for studying health information technology in complex adaptive healthcare systems. In *Cognitive informatics for biomedicine* (pp. 59-80). Springer, Cham. https://doi.org/10.1007/978-3-319-17272-9_4.

[5] Buntin, M. B., Burke, M. F., Hoaglin, M. C., & Blumenthal, D. (2011). The benefits of health information technology: a review of the recent literature shows predominantly positive results. *Health affairs*, *30*(3), 464-471. https://doi.org/10.1377/hlthaff.2011.0178.

[6] Jamal, A., McKenzie, K., & Clark, M. (2009). The impact of health information technology on the quality of medical and health care: a systematic review. *Health Information Management Journal*, *38*(3), 26-37. https://doi.org/10.1177/183335830903800305.

[7] Kierkegaard, P. (2011). Electronic health record: Wiring Europe's healthcare. *Computer law & security review*, *27*(5), 503-515. https://doi.org/10.1016/j.clsr.2011.07.013.

[8] Amarasingham, R., Patzer, R. E., Huesch, M., Nguyen, N. Q., & Xie, B. (2014). Implementing electronic health care predictive analytics: considerations and challenges. *Health Affairs*, *33*(7), 1148-1154. https://doi.org/10.1377/hlthaff.2014.0352.

[9] Huang, C. D., Behara, R. S., & Goo, J. (2014). Optimal information security investment in a Healthcare Information Exchange: An economic analysis. *Decision Support Systems*, *61*, 1-11. https://doi.org/10.1016/j.dss.2013.10.011.

[10] Koh, H. C., & Tan, G. (2011). Data mining applications in healthcare. *Journal of healthcare information management*, *19*(2), 65.

[11] Smith, E., & Eloff, J. H. P. (2002). A prototype for assessing information technology risks in health care. *Computers & Security*, *21*(3), 266-284. https://doi.org/10.1016/S0167-4048(02)00313-9.

[12] Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, *22*(3), 469-490. https://doi.org/10.1287/isre.1100.0335.

[13] Harland, C., Knight, L., Lamming, R., & Walker, H. (2005). Outsourcing: assessing the risks and benefits for organisations, sectors and nations. *International Journal of Operations & Production Management*, *25*(9), 831-850. https://doi.org/10.1108/01443570510613929.

[14] Tinetti, M. E., Gordon, C., Sogolow, E., Lapin, P., & Bradley, E. H. (2006). Fall-risk evaluation and management: challenges in adopting geriatric care practices. *The Gerontologist*, *46*(6), 717-725. https://doi.org/10.1093/geront/46.6.717.

[15] Bahli, B., & Rivard, S. (2003). The information technology outsourcing risk: a transaction cost and agency theory-based perspective. *Journal of Information Technology*, *18*(3), 211-221. https://doi.org/10.1080/0268396032000130214.

[16] Haufe, K., Dzombeta, S., & Brandis, K. (2014). Proposal for a security management in cloud computing for health care. *The Scientific World Journal*, *2014*. https://doi.org/10.1155/2014/146970.

[17] Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare: promise and potential. *Health information science and systems*, *2*(1), 3. https://doi.org/10.1186/2047-2501-2-3.

[18] Pronk, N. P., Peek, C. J., & Goldstein, M. G. (2004). Addressing multiple behavioral risk factors in primary care: a synthesis of current knowledge and stakeholder dialogue sessions. *American journal of preventive medicine*, *27*(2), 4-17. https://doi.org/10.1016/j.amepre.2004.04.024.

[19] Ventola, C. L. (2014). Social media and health care professionals: benefits, risks, and best practices. *Pharmacy and Therapeutics*, *39*(7), 491.

[20] Lobach, D., Sanders, G. D., Bright, T. J., Wong, A., Dhurjati, R., Bristow, E., & Williams, J. W. (2012). Enabling health care decision making through clinical decision support and knowledge management. *Evid Rep Technol Assess (Full Rep)*, *203*(203), 1-784.