Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.021560
Article

Tech Science Press

A Framework for Securing Saudi Arabian Hospital Industry: Vision-2030 Perspective

Hosam Alhakami[1,*], Abdullah Baz[2], Mohammad Al-shareef[3], Rajeev Kumar[4], Alka Agrawal[5] and Raees Ahmad Khan[5]

[1]Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Makkah, 21955, Saudi Arabia
[2]Department of Computer Engineering, College of Computer and Information Systems, Umm Al-Qura University, Makkah, 21955, Saudi Arabia
[3]Security Forces Hospital, Makkah, 21955, Saudi Arabia
[4]Department of Computer Science and Engineering, Babu Banarasi Das University, Lucknow, 226028, Uttar Pradesh, India
[5]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, 226025, Uttar Pradesh, India
*Corresponding Author: Hosam Alhakami. Email: hhhakam@uqu.edu.sa
Received: 07 July 2021; Accepted: 10 August 2021

Abstract: Recent transformation of Saudi Arabian healthcare sector into a revenue producing one has signaled several advancements in healthcare in the country. Transforming healthcare management into Smart hospital systems is one of them. Secure hospital management systems which are *breach-proof* only can be termed as effective smart hospital systems. Given the perspective of Saudi Vision-2030, many practitioners are trying to achieve a cost-effective hospital management system by using smart ideas. In this row, the proposed framework posits the main objectives for creating smart hospital management systems that can only be acknowledged by managing the security of healthcare data and medical practices. Further, the proposed framework will also be helpful in gaining satisfactory revenue from the healthcare sector by reducing the cost and time involved in managing the smart hospital system. The framework is based on a hybrid approach of three key methods which include: employing the Internet of Medical Things (IoMT) and blockchain methodologies for maintaining the security and privacy of healthcare data and medical practices, and using big data analytics methodology for raising the funds and revenue by managing the bulk volume of healthcare data. Moreover, the framework will also be helpful for both the patients and the doctors, thus enabling the Kingdom of Saudi Arabia (KSA) to meet its goals of Vision-2030 by ensuring low cost, yet credible, healthcare services.

Keywords: Smart healthcare; healthcare industry; data; security

1 Introduction

Healthcare services are the most important of the basic amenities that a country provides for its citizens. Current era of digitalization has led to major transformations in the healthcare services offered worldwide. Every country is employing digitalized healthcare or e-health services for better experience and for

minimizing infrastructural requirements. E-health services are more efficacious with optimal accessibility besides reducing the time and cost invested otherwise. But digitalization process in the healthcare sector has also raised many challenging dilemmas for the security practitioners. Security threats like the attacks on confidentiality, data breaches, integrity breach of data and many other threats are continuously increasing. Hence, the success and credibility of smart hospital management systems depends on creating breach-proof information systems in healthcare.

Furthermore, in the context of the e-healthcare services in KSA, the Saudi Arabian king and the government intend to raise the private healthcare expenditure to 35% from 25% by 2020 [1–5]. The kingdom of Saudi Arabia vision 2030 aims to establish the kingdom as a leader of Middle East Asia and be a country of excellence with a thriving economy. This aim and vision also includes the provision of e-healthcare services for the citizens at an affordable cost. For accomplishing the objective of highly effective, secure and dependable smart hospital management systems, there is an imminent need to explore methodologies to secure the systems and render them tamper-proof. Moreover, smart hospital management system will help the KSA economy in many ways. Advance security measures and smart hospital services of Arabian healthcare sector will attract the patients and foreign investors for investment. A secure smart hospital system will help the KSA in raising its economy from other sources besides oil [6–10]. The proposed research work aims to provide a secure smart hospital management system for Kingdom of Saudi Arabia. The study tries to reduce the security threats related to electronic healthcare sector and provides a module for designing secure and systematic smart hospital management system.

Smart hospital management system includes the use of IoT and IoMT in their infrastructure. Digitalization of every service provided by a healthcare service provider is also essential for smart hospital management system. But the current situation of IoT security and breach statistics show that it is risky for implementing normal IoT and IoMT environment in a smart hospital management system for KSA [11–17]. In the proposed work, our aim is to create a systematic process for managing smart hospital through IoT and IoMT devices [18–20]. Safeguarding the smart hospital management system for kingdom of Saudi Arabia is the second significant topic for our study. The challenges associated with smart healthcare organizations are massively high and critical. This research work propositions a unique endeavour which is to work on mechanisms for creating secure smart hospital management systems for KSA, a research work hitherto not attempted.

2 Review of Related Literature

Smart hospital system is a vast topic for researchers and very limited work is available in the field till now. Unfortunately, there is no specific literature on managing the smart hospital of the Saudi Arabia with different types of security approaches. Some researchers have defined data security in healthcare sector through blockchain-based security. For managing the large volume of data in healthcare sector, some researchers have used big data analytics, while the others have only talked about healthcare data privacy and a cloud-based system for managing data online. The researchers of this study have categorized the literature review of the proposed work into different attributes of smart hospital. This was done because even after exhaustive reviews, the researchers could not find a specific study that summarized the whole smart hospital management system. We found the studies based on different approaches and tried to combine them for producing an effective and efficient framework for smart hospital management system. Some of the pertinent work related to smart hospital management system in healthcare has been outlined below:

2.1 Literature Review on IoMT Devices in Healthcare

Sandeep Pirbhulal et al. analyzed and found the IoMT related threats of data privacy and validity of data and tried to solve that problem. Authors proposed a bio-metric based security framework that provides a data

privacy and security assurance on patient's data [8]. The proposed framework works on a time-domain based biometric features and is directly used by IoMT devices for wearable security model. Liyakathunisa Syed et al. provide a novel smart healthcare framework for ambient assisted living. The work provides wearable process for elderly people by giving them better medical treatment through sensors and data analytics mechanisms [9]. The proposed study discusses about the sensors that are placed on the patient's body and directly connects to the IoMT devices that fetch the smart data from patients. This data is analyzed for further treatment procedures.

2.2 Literature Review on IoT Devices in Healthcare

Elias Yaacoub et al. provides a secure IoT data transfer from patient to hospital. The proposed study is divided into three tiers and relevant security measures are also implemented on every tier [10]. The author uses IoT devices for secure communication between patients to hospital in a novel manner.

2.3 Literature Review on Blockchain Approach in Healthcare

Asaph Azaria et al., define and analyze data privacy and access permission using the blockchain technology. The authors provide an implemented approach called "MedRec" in their paper which uses the blockchain technique and categorization process of data to manage the privacy of healthcare data and prevent it from unauthorized access [11]. Mian Zhang et al. talk about blockchain in their paper. The research study shows that a blockchain is a good approach for healthcare security but it also has many drawbacks. Blockchain has serious issues related to the storage capacity of data over the block and privacy concerns [12]. In the end, the research states that block is a better option for securing healthcare data but it needs to be friendlier to the large volume of data and there is a need for further research in this context.

2.4 Literature Review on Big Data Analytics Approach in Healthcare

Siyang Qin et al. provide a process of identifying tourist behavior through big data analytics and real time tracking [13]. The proposed approach in this paper provides a great idea for healthcare sector smart patient monitoring system. Through some advance research we can achieve better and effective big data analytics approaches and their impact on healthcare. Agusti Solanas et al., provide a brief understanding of current challenges and issues of data and smart healthcare. The study provides a systematic transformation of data and talks about the challenges associated with transformation stage. The paper helps a lot in managing big data approaches in our proposed study [15]. With the help of this study, the challenges and issues that occur at every transformation phase of data can get reduced. Yichuan Wang et al., tells that Big Data Analytics (BDA) is beneficial for organizations, yet implementing BDA to leverage profitability is a fundamental challenge confronting practitioners. The authors have developed a conceptual model of BDA success that aims to investigate how BDA's capabilities interact with complementary organizational resources and organizational capabilities in multiple configuration solutions leading to higher quality of care in healthcare organizations [14].

2.5 Literature Review on Hexplet Approach

S. M. Darwish proposed a unique and novel database integrity management approach called hexplet in his work. Hexplet is a technology that is used for identifying unauthorized modification in a database through machine learning algorithms and methodologies [20]. Besides being an inventive approach, hexplat can also be effective in reducing the attack ratio.

3 Need and Importance

Data in a healthcare organization is the most valuable asset. In the current era of digitalization, every treatment of the patient is based on their electronic medical record in KSA. However, the smart hospital

management systems are beset with several challenges and issues. We have tried to solve these issues and challenges in our proposed study. Towards this intent, we have categorized the challenges that the smart hospital management systems in KSA are likely to contend with. These are:

3.1 Increasing Expenditure on Healthcare Sector

The biggest problem associated with Saudi healthcare sector is expenditure. Healthcare services in KSA are free for citizens and future ratio of healthcare sector by vision 2030 shows that expenditure on healthcare sector in KSA would be the biggest challenge for the Saudi government. Right now, the healthcare sector in KSA is driven by open consumption at 74.2% (2016) and 25.8% by private segment. This is expected to increase to 28.1% by 2025. A report shows that the top 15 countries of world are spending 3 times to 8 times more in comparison to KSA [18]. The biggest reason for this situation is the lack of effective management of revenue from healthcare sector. It is essential for KSA to invest and produce smart healthcare services while ensuring astute management of the revenue generated through the sector. This will also be a major boost to the country's vision 2030.

3.2 Availability of Doctors & Easy Access to Medical Services

Waiting time for any special surgery or operation by the patients is another big challenge for KSA government to solve under the roadmap of vision 2030. Saudi Arabian healthcare sector needs time management for providing accessible and prompt medical services for the patients.

Fig. 1, above, illustrates the average percentage of time that the patients spend on waiting for a doctor for a mere checkup in KSA. The figure clearly shows that 52% of the citizens have to wait for at least 30–60 min to be examined by a doctor. If the condition of the patient is critical, this waiting time could be life-threatening. Smart hospital management systems will reduce this anomaly in time through various IoT and IoMT smart services.

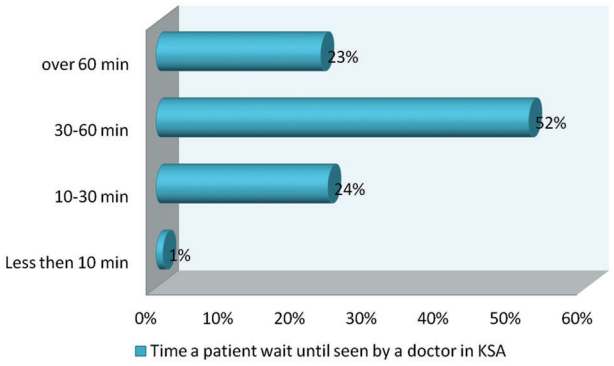

Figure 1: Percentage ratio of average time a patient spend on doctor

Transformation Challenges: KSA healthcare sector is suffering from revenue problem because of their cost expenditure on healthcare services. It is a challenging task for experts to transform the Saudi healthcare sector to a revenue generation sector for KSA by Vision 2030.

The challenges and issues cited above illustrate the basic dilemmas of Saudi healthcare system. However, there are certain attributes of Smart Management Hospital systems which can be equally challenging for the security experts. This study analyses them and aims at finding solutions for each of these challenges. They are listed as:

3.3 Challenges Associated with IoMT

Digitalized healthcare services have seen tremendous increase in the use of IoMT. There are several issues associated with IoMT that need to be solved. The biggest challenge for IoMT is the leakage of sensitive data from IoMT devices. Lack of sufficient memory in IoMT devices is also a major debacle for experts. According to a study, by 2023, the sector of healthcare security will see a whopping count of $8.7 billion [3]. IoMT is one of the biggest assets for healthcare security and this phenomenal growth of market will also affect the use and adoption of IoMT.

3.4 Challenges Associated with IoT

Same as IoMT, the IoT devices are also a main and significant attribute for smart hospitals. IoT enabled infrastructure opens a door for intelligence based hospitals that need less employees and reduced maintenance cost. The biggest issue in IoT is the easy surface for attacks. IoT devices are easily hacked and breached by attackers. There is a need of secure connection and data transformation platform for IoT devices. Misbalanced situation in healthcare organizations creates a threat for IoT breaches in healthcare sector. Misbalanced refers to old infrastructure with new IoT system. It is essential for all healthcare organizations that are implementing IoT devices in the infrastructure to update and sensitize their employees for the IoT environment [4].

Above Fig. 2 describes the per year installation of IoT devices in healthcare sector [16]. This ratio of implementation shows that by 2020 we need to solve the challenges associated with IoT devices for better security measures in healthcare sector. Vision 2030 of KSA is the most ambiguous research work for Saudi Arabia and this growing statistics of IoT implementation in healthcare comparatively shows that IoT implementation in Saudi Arabian healthcare sector is an essential option for developing and transforming KSA healthcare.

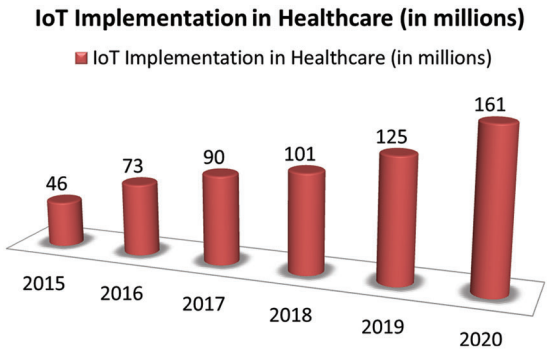

Figure 2: Year wise implementation of IoT devices in healthcare sector [16]

3.5 Challenges Associated with Information Providing Portal for Patients

Every healthcare organisation has a separate information providing portal for delivering information related services to patients. In a smart hospital environment, it is necessary for organizations to deliver healthcare services with information on m-health platforms, thereby helping in easy access of services and data by the patients.

The security threats with particular reference to Smart hospitals has increased in the current scenario due to massive use of internet and networked devices. An online survey journal “HIPPA” conducted a study on the data breach attacks on healthcare organizations done in the time period of 2009–19. This study shows that in comparison to 2009, the data breach attack on the healthcare industry at present is the worst [5]. In Fig. 3,

the graph of attacks illustrates that data breach on the healthcare industry requires some guaranteed safeguards for securing smart hospitals.

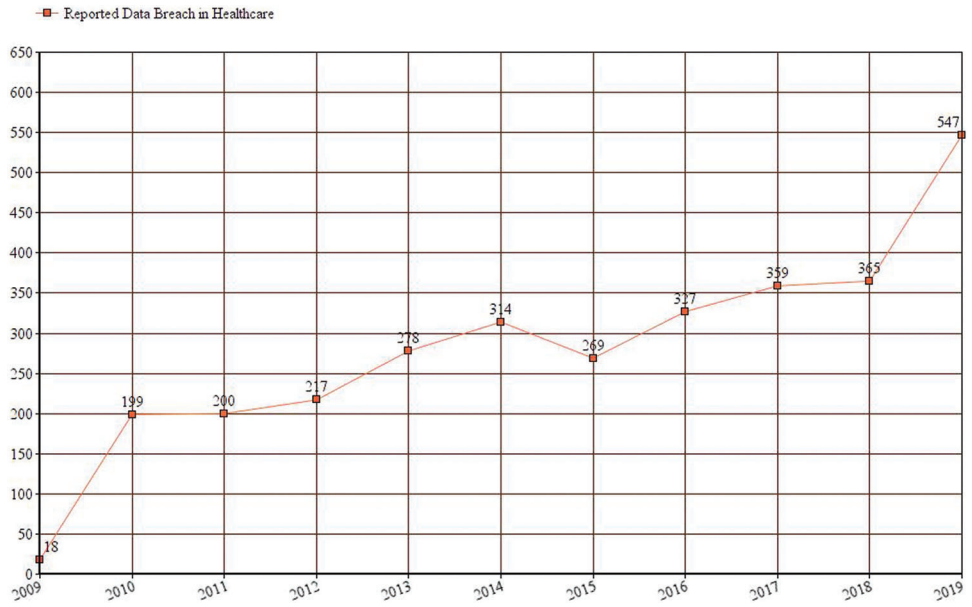

Figure 3: Data breaches on the healthcare industry in the last 10 years

The study published in HIPPA journal also shows the current scenario of attacks on healthcare sector. Saudi Arabia's vision 2030 opens a market for bad intruders to penetrate the Saudi Arabian healthcare organizations. To tackle the bad actors and intruders in the organizations, Saudi Arabian healthcare organizations need to safeguard their services and infrastructure through a secure smart hospital management system. Complex and huge infrastructural systems are also a major challenge for smart hospitals. An online news website "Arab News" describes the seriousness of healthcare issues in KSA. The report tells that extra 110,000 beds will be needed by 2030 in KSA and the report's findings also illustrates that the healthcare's digital infrastructure in KSA is going to be very complex and large by 2030 [6].

Fig. 4 describes the need of patient tracking system in KSA for the citizens. 68.20% citizens strongly agree on implementing a smart hospital service in regular healthcare organization [17]. This type of survey shows that KSA's citizens would welcome easy and smart services in healthcare sector. Our study will help the KSA to fulfill this need by providing the citizens with a secure and latest smart hospital management system environment.

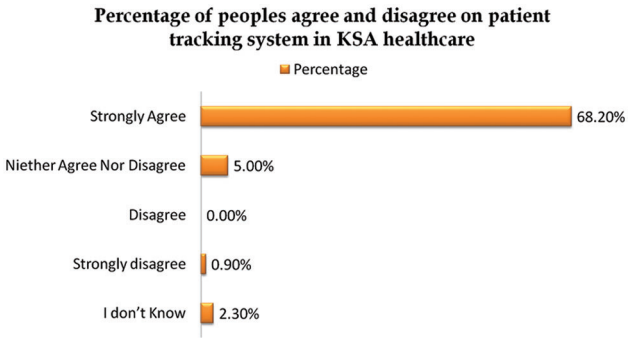

Figure 4: KSA citizen percentage votes for patient tracking services in KSA healthcare

Many researchers have discussed healthcare security and conducted their critical review. Although many researchers have dwelt upon the problems and vulnerabilities of smart healthcare systems worldwide and in KSA; there is no common and secure smart hospital security mechanism for healthcare sector. Some of the research problems in this regard are listed as follows:

- Development of a framework for securing smart hospital management system is a challenging task and needs in-depth analysis to be used.
- To bridge the gap between the IoT and IoMT devices, secure communication and effective implementation of security approaches for preventing data breaches in healthcare system.
- There is a need for a mechanism to increase the revenue of healthcare sector in KSA while ensuring that the citizens can access the best possible healthcare amenities.

From the foregoing discussion, it is apparent that there is not even a single efficacious mechanism available for addressing the secure smart hospital management system and increasing the revenue of healthcare sector in KSA.

4 Theoretical Framework

A smart hospital management system shows the wellness and progressive approach of any country. Developing a secure and effective management system for smart hospitals is a challenging task for expert researchers. After analyzing the needs and studying the articles related to smart hospitals management systems challenges and infrastructure, we have classified our proposed model into different domains of a smart hospital. We have covered all the attributes of smart hospitals that are necessary in every smart hospital services. We have categorized our whole smart hospital model on two basic devices-

- IoMT Devices
- IoT Devices

The deferent classification of proposed model is illustrated as follows:

For Managing Patient's Data Security in Smart Hospital and Providing Smart Medical Services in Smart Hospital Management System: In a smart hospital system, managing the security of patient's digital data and storing the data without any type of manipulation is of vital importance. For addressing this issue, in the proposed smart hospital management system we use blockchain approach at every data transaction level for reducing the threat of data breach and manipulation in smart hospital system. Our approach is to connect all the IoMT devices directly with the centralized healthcare database. If any update is done in the patient's private EMR or other medical information, then that update is firstly verified by a machine learning based hexplet approach for validating authentic modification. Hexplet will enhance the security attribute of smart hospital management system and provide a cross-verification characteristic in database security. A replica of healthcare information will be saved as a mirror file or copy file in hexplet and at the time of any type of modification or alteration in the specific file the hexplet approach will verify that modification session through machine learning-based approach. Fig. 5 illustrates the pictorial idea of this approach.

For Providing Smart Patients Services in Smart Hospital Management System:- For providing smart patient services as real time patient tracking and facilitating patients with smart appointment services, we have used IoT infrastructure to manage and provide the smart patient services in our smart hospital. We connect the patient in a hospital with an IoT device that will help the doctors and hospital staff to track the patient and monitor the patient's medical condition in real time. We use a secure blockchain cloud for securely storing the IoT based medical and private patient data for further use by the hospital or by the doctor. As a security approach, we try to use blockchain approach for secure communication between IoT

devices. For secure storage medium, we have used blockchain cloud [21–24] approach that helps the smart hospital to manage the data securely at storage level. Fig. 6 describes the idea briefly.

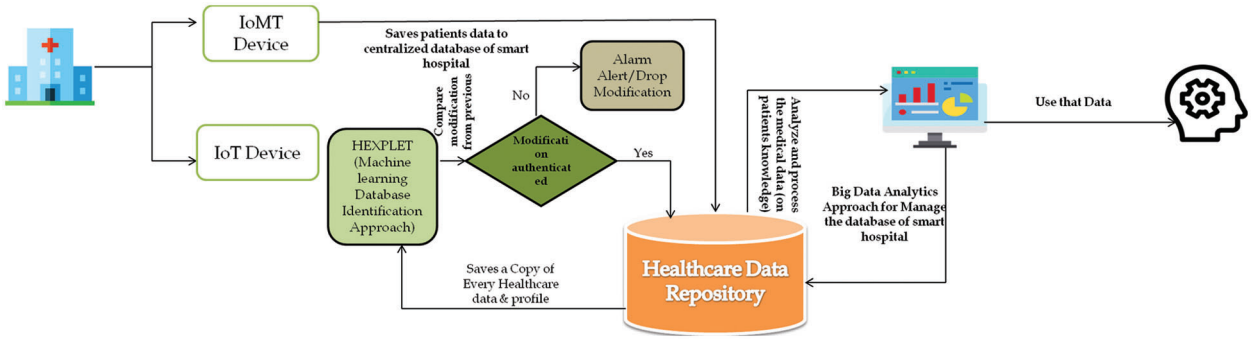

Figure 5: Managing smart medical data securely

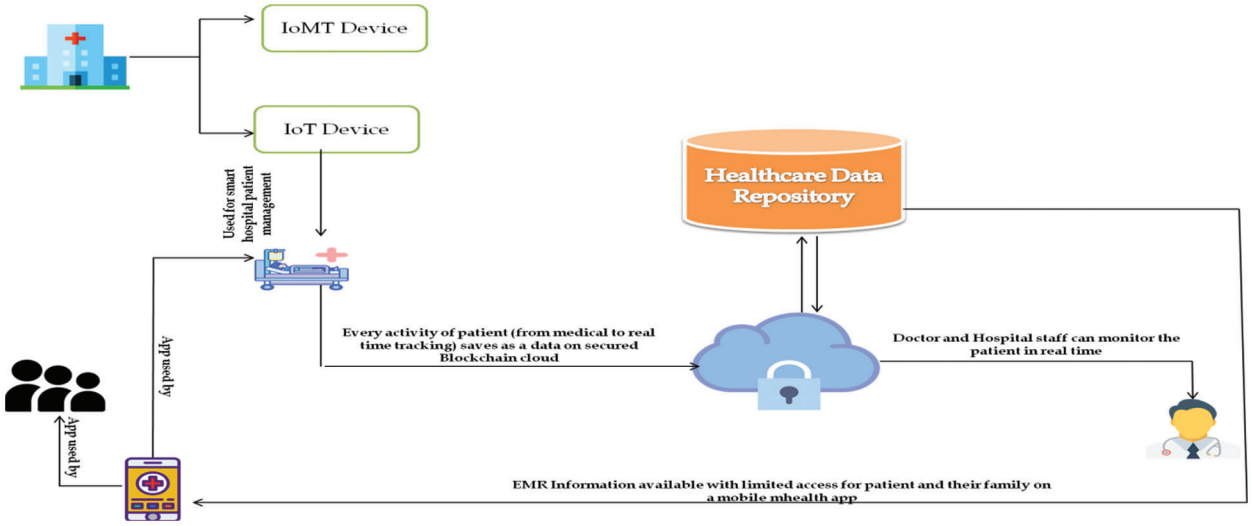

Figure 6: Managing smart patient data securely

For Increasing the Revenue of Hospital by Managing the Large Volume of Healthcare Data in Smart Hospital Management System:- In order to manage the vast smart hospital management system in KSA, our study may help the smart hospitals to produce the revenue from database management system in their hospital. Big data analytics provides a platform for smart hospitals to produce the revenue through managed data in our proposed study. Healthcare situation in KSA demands a large scale of revenue for better transformation of healthcare sector into smart healthcare sector. Our proposed study will help these organizations to manage their expenditure through their own analyzed zero investment data. Fig. 7 illustrates the approach workflow.

This research also focuses on securing Saudi Arabian smart hospital systems through various approaches. The following Fig. 8 describes the step-wise process of the full theoretical framework used for this purpose.

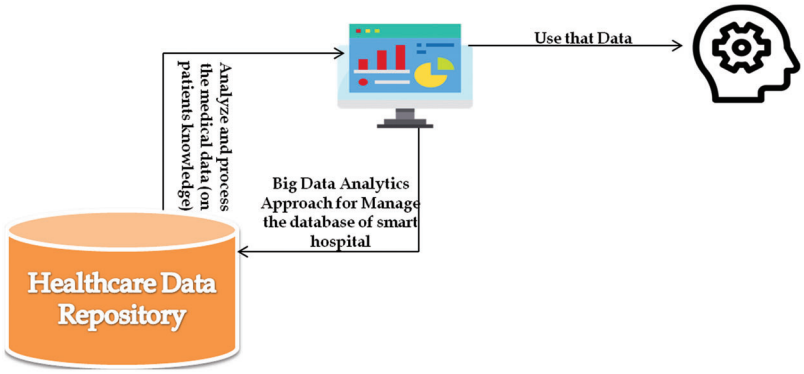

Figure 7: Managing database securely

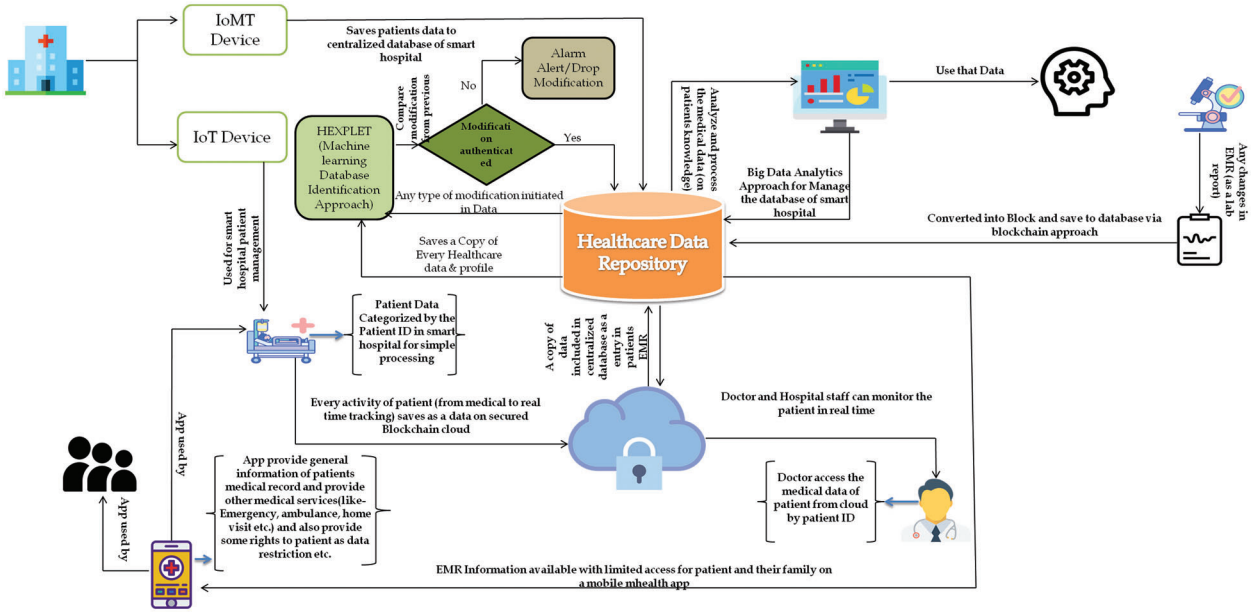

Figure 8: Theoretical framework

Fig. 8 envisages the combined overview of the proposed work in securing smart hospital management system through the use of different smart approaches. At the initial stage itself, we have categorized the smart hospital into two devices that are mainly used in smart hospital management systems. Then we have tried to manage the data security between communication and transfer through blockchain approach, hexplet technology and then tried to manage the large volume of data through big data analytics techniques. Big data analytics approach provides a new revenue generating platform for hospitals to facilitate the revenue needs in KSA.

5 Performance Simulation

We performed a comparative study to assess the effectiveness of the proposed unified framework by simulating the efficacy of the outcomes of the proposed and other similar frameworks. A study and numerical quantification of this sort reveals an obvious understanding of the efficacy of the unified system suggested. For assessment, we selected six different frameworks, including the proposed one.

L&T Technology Services Limited Framework (F1) [13]; Sensor-Cloud Infrastructure (S-CI) Framework (F2) [14]; Knowledge Management Framework (F3) [15]; Smart Hospital Management Information System Framework (F4) [16]; Smart e-Health System (F5) [17]; and Proposed Unified Framework (F5) [17]. The initial serial numbers were allocated by the experts for all the selected versions. In addition, we adopted the common hybrid multi criteria decision-making approach, called the analytical hierarchy process combined with fuzzy set theory (Fuzzy-AHP) [25–31], to conduct a numerical simulation of success and prioritisation of frameworks.

This technique was used as a tool to simulate the effectiveness of the unified framework proposed vis-à-vis the different frameworks that were selected for the comparison. This gives an idea of the frameworks' results. Fuzzy-AHP is a tool that offers specific outcomes that are generally acceptable and validated [18]. It is a well-established technique. Performance simulation can assist the scientists in selecting the most appropriate system. The adopted prioritisation approach operates on the roles of the membership, and the numerical assessment is adopted by [19]. Table 1 illustrates the triangular fuzzy number in a pair-wise comparison matrix for each particular framework in order to perform the numerical evaluation. After the pair-wise fuzzy numbers were established, the examiners defuzzified the values by following the alpha cut approach [18]. The value acquired by the alpha cut approach and the defuzzified value of the triangular fuzzy numbers are represented in Table 2. Further, Table 3 and Fig. 9 define the final weights and rankings.

Table 1: Triangular fuzzy numbers for every specific framework

	F1	F2	F3	F4	F5	F6
L&T Technology Services Limited Framework (F1)	1.00000, 1.00000, 1.00000	1.00011, 1.51571, 1.93310	0.48906, 0.63720, 1.00000	0.41520, 0.57430, 1.00000	0.22150, 0.28710, 0.41520	0.31460, 0.46100, 0.87050
Sensor-Cloud Infrastructure (S-CI) Framework (F2)	-	1.00000, 1.00000, 1.00000	0.57430, 0.66570, 0.80220	0.30390, 0.39360, 0.56610	0.26790, 0.35210, 0.51760	0.16630, 0.19690, 0.25310
Knowledge Management Framework (F3)	-	-	1.00000, 1.00000, 1.00000	1.00000, 1.31950, 1.55180	0.30090, 0.43520, 0.80270	0.80270, 0.87050, 1.00000
Smart Hospital Management Information System Framework (F4)	-	-	-	1.00000, 1.00000, 1.00000	0.53860, 0.91430, 1.58360	0.60830, 1.05920, 1.68290
Smart e-Health System (F5)	-	-	-	-	1.00000, 1.00000, 1.00000	0.41520, 0.63720, 1.17910
Proposed Unified Framework (F6)	-	-	-	-	-	1.00000, 1.00000, 1.00000

Table 2: Defuzzified TFN value

	F1	F2	F3	F4	F5	F6
L&T Technology Services Limited Framework (F1)	1.00000	1.49120	0.69100	0.64100	0.30270	0.52680
Sensor-Cloud Infrastructure (S-CI) Framework (F2)	0.67060	1.00000	0.67700	0.41430	0.37240	0.20330
Knowledge Management Framework (F3)	1.44700	1.47710	1.00000	1.29770	0.49350	0.85200
Smart Hospital Management Information System Framework (F4)	1.56000	2.41370	0.77060	1.00000	0.96360	1.10240
Smart e-Health System (F5)	3.30360	2.68530	2.02630	1.03780	1.00000	0.71720
Proposed Unified Framework (F6)	1.89820	4.91880	1.17370	0.90710	1.39430	1.00000
C.R. = 0.038600						

Table 3: Final ranking

S. No.	Frameworks	Weights	Ranks
1	L&T Technology Services Limited Framework (F1)	0.10370	5
2	Sensor-Cloud Infrastructure (S-CI) Framework (F2)	0.07520	6
3	Knowledge Management Framework (F3)	0.15860	4
4	Smart Hospital Management Information System Framework (F4)	0.18470	3
5	Smart e-Health System (F5)	0.23690	2
6	Proposed Unified Framework (F6)	0.24090	1

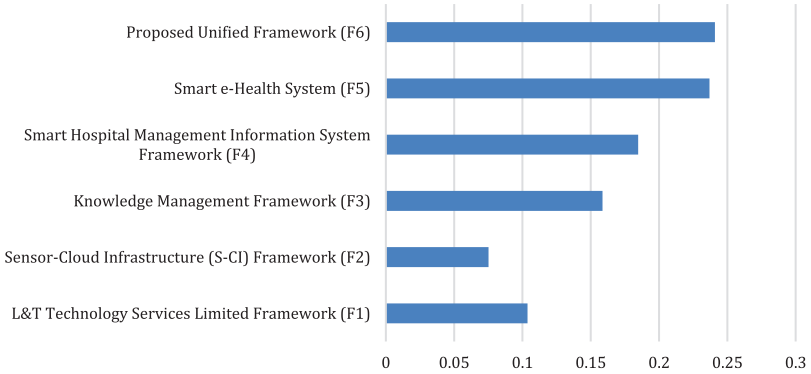

Figure 9: Graphical diagram of significance

It is a daunting task to recognize secure healthcare framework and its functionality to achieve a healthy and systematic workflow; however, as discussed in this report, different successful mechanisms are present in relevant fields to achieve this ideal aim. For researchers and experts, therefore, it is a confusing task to determine which system is effective and which is not. This section illustrates an optimal pathway to simplify this task and represents a structured and numerically measured order of effectiveness. The results

obtained from numerical evaluation show that in all selected frameworks, the proposed unified framework has the highest effect ratio with a weight of 0.24090 and a consistency ratio (CR) value of 0.038600.

F6 > F5 > F4 > F3 > F1 > F2 is the descending order of the prioritisation for the selected frameworks. The findings addressed in this performance simulation section represent the highest efficiency and priority of the proposed unified system and the lowest Sensor-Cloud Infrastructure (S-CI) framework. Overall, the proposed unified structure is one of the most appropriate structures and philosophies that can be adopted by the researchers and potential practitioners in their domain.

6 Conclusions

This research endeavour envisions a real time framework to facilitate breach-free and secure e-healthcare services for the patients, doctors and healthcare organisations in the Kingdom of Saudi Arabia. In the wake of digitalisation of health services in KSA and the Saudi government's dedicated initiatives to provide impetus to smart hospital management systems, this framework proposes a highly cost-effective, three-tier methodology for accomplishing efficacious mechanism for securing the digital data of patients. Furthermore, this framework draws inspiration from the vision-2030 of the KSA that seeks to carve the Kingdom's niche as a thriving economy on the global landscape. Contributing to the country's overarching mission, this academic framework is a unique attempt to engage the practitioners' expertise in the provision of affordable, accessible, credible and secure digital health services for the citizens of KSA. Healthcare became the nodal research area of this framework because the authors analysed that KSA was currently spending 73.6 billion US dollars on healthcare. The public expenditure on healthcare in KSA is 74.2% (2016), and the private sector's investment in this sector is 25.8%. This is expected to increase to 28.1% by 2025. Moreover, in line with the government's Vision-2030 and the National Transformation Program (NTP), the Ministry of Health (MoH) is expected to spend approximately US $71 billion on healthcare till 2020. Thus, the proposed mechanism's key objective is to contribute towards accomplishing the target of highly accessible and yet safe digital healthcare services at viable costs in Saudi Arabia.

Digitalized healthcare services have transformed the means and ways in which the patients can seek medical care. However, ironically, through the same digital platform many patients are becoming victims of data pilferage. The constant attacks on patients' data have led to financial losses and misappropriation of vital personal data. Hence, the need of the hour is for the academic scholars, cyber security professionals, research hubs and healthcare organisations to collate their efforts and create effective safeguards to ward off security threats particularly in the field of healthcare.

Acknowledgement: The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: (20UQU0067DSR). This project was supported by Security Forces Hospital Makkah Institutional Review Board (IRB) number (0443-041021), Security Forces Hospital, Makkah, Saudi Arabia.

Funding Statement: This Project was funded by the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: (20UQU0067DSR) and Security Forces Hospital Makkah Institutional Review Board (IRB) number (0443-041021), Security Forces Hospital, Makkah, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] D. Halperin, T. S. H. Benjamin, B. Ransford, S. S. Clark, B. Defend *et al.,* "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Proc. of the IEEE Symp. on Security and Privacy*, Oakland, CA, USA, pp. 129–142, 2008.

[2] C. Li, A. Raghunathan and N. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proc. of the 2011 IEEE 13th Int. Conf. on e-Health Networking, Applications and Services*, Columbia, MO, USA, pp. 150–156, 2011.

[3] H. Almohri, L. Cheng, D. Yao and M. Alemzadeh, "On threat modeling and mitigation of medical cyber-physical systems," in *Proc. of the IEEE/ACM Int. Conf. on Connected Health: Applications, System*, Philadelphia, PA, USA, pp. 114–119, 2017.

[4] Confickered! Medical Devices and Digital Medical Records are Getting Hacked. "MassDevice," 2009. [Online]. Available: https://www.massdevice.com/confickered-medical-devices-and-digital-medical-records-are-getting-hacked/.

[5] NoMoreClipboard Notice to Individuals of a Data Security Compromise. "Business wire," 2015. [Online]. Available: https://www.businesswire.com/news/home/20150610005964/en/NoMoreClipboard-Notice-to-Individuals-of-a-Data-Security-Compromise.

[6] Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices. "GAO: U. S. government accountability office," 2012. [Online]. Available: https://www.gao.gov/products/GAO-12-816.

[7] FDA's Role in Regulating Medical Devices. "U. S. food & drug administration," 2018. [Online]. Available: https://www.fda.gov/medical-devices/home-use-devices/fdas-role-regulating-medical-devices.

[8] Y. Xu, D. Tran, Y. Tian and H. Alemzadeh, "Poster abstract: Analysis of cyber-security vulnerabilities of interconnected medical devices," in *Proc. of the 2019 IEEE/ACM Int. Conf. on Connected Health: Applications, Systems and Engineering Technologies*, Arlington, VA, USA, pp. 23–24, 2019.

[9] Hospital Networks Are Leaking Data, Leaving Critical Devices Vulnerable. "Wired magazine," 2014. [Online]. Available: https://www.wired.com/2014/06/hospital-networks-leaking-data/.

[10] R. Kumar, M. T. J. Ansari, A. Baz, H. Alhakami, A. Agrawal *et al.,* "A multi-perspective benchmarking framework for estimating usable-security of hospital management system software based on fuzzy logic, ANP and TOPSIS methods," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 15, no. 1, pp. 240–263, 2021.

[11] T. Yaqoob, H. Abbas and M. Atiquzzaman, "Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices-a review," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3723–3768, 2019.

[12] A. Attaallah, H. Alsuhabi, S. Shukla, R. Kumar, B. K. Gupta *et al.,* "Analyzing the big data security through a unified decision-making approach," *Intelligent Automation and Soft Computing*, vol. 32, no. 2, pp. 1071–1088, 2022.

[13] A. Algarni, M. Ahmad, A. Attaallah, A. Agrawal, R. Kumar *et al.,* "A hybrid fuzzy rule-based multi-criteria framework for security assessment of medical device software," *International Journal of Intelligent Engineering and Systems*, vol. 13, no. 5, pp. 51–62, 2020.

[14] A. Algarni, A. Attaallah, M. Ahmad, A. Agrawal, R. Kumar *et al.,* "A fuzzy multi-objective covering-based security quantification model for mitigating risk of web based medical image processing system," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 1, pp. 481–489, 2020.

[15] A. H. Almulihi, F. Alassery, A. I. Khan, S. Shukla, B. K. Gupta *et al.,* "Analyzing the implications of healthcare data breaches through computational technique," *Intelligent Automation and Soft Computing*, vol. 3, no. 2, pp. 1763–1779, 2022.

[16] N. Christoulakis, G. Christou, E. Athanasopoulos and S. Ioannidis, "HCFI: Hardware-enforced control-flow integrity," in *Proc. of the Sixth ACM Conf. on Data and Application Security and Privacy*, New York, NY, USA, pp. 38–49, 2016.

[17] A. I. Newaz, A. K. Sikder, L. Babun and A. S. Uluagac, "HEKA: A novel intrusion detection system for attacks to personal medical devices," in *Proc. of the 2020 IEEE Conf. on Communications and Network Security*, Avignon, France, pp. 1–9, 2020.

[18] L. Zhou and Y. Makris, "HAFIX: Hardware-assisted flow integrity extension," in *Proc. of the 52nd Annual Design Automation Conf.*, San Francisco, CA, USA, pp. 1550–1555, 2015.

[19] S. Gao and G. Thamilarasu, "Machine-learning classifiers for security in connected medical devices," in *Proc. of the 2017 26th Int. Conf. on Computer Communication and Networks*, Vancouver, BC, Canada, pp. 1–5, 2017.

[20] A. Ray and C. Rance, "An analysis method for medical device security," in *Proc. of the Symp. and Bootcamp on the Science of Security*, New York, NY, USA, Article 16, pp. 1–2, 2014.

[21] R. Kumar, A. K. Pandey, A. Baz, H. Alhakami, W. Alhakami *et al.,* "Fuzzy-based symmetrical multi-criteria decision-making procedure for evaluating the impact of harmful factors of healthcare information security," *Symmetry*, vol. 12, no. 4, pp. 1–21, 2020.

[22] A. Ali and F. A. Khan, "Key agreement schemes in wireless body area networks: Taxonomy and state-of-the-art," *Journal of Medical Systems*, vol. 39, no. 10, pp. 1–14, 2015.

[23] D. Karaolan, A. Levi and V. Tuzcu, "Deriving cryptographic keys from physiological signals," *Pervasive and Mobile Computing*, vol. 39, no. 4, pp. 65–79, 2017.

[24] K. Sahu, F. A. Alzahrani, R. K. Srivastava and R. Kumar, "Hesitant fuzzy sets based symmetrical model of decision-making for estimating the durability of web application," *Symmetry*, vol. 12, no. 6, pp. 1770–1792, 2020.

[25] A. Attaallah, M. Ahmad, M. Tarique, A. K. Pandey, R. Kumar *et al.,* "Device security assessment of internet of healthcare things," *Intelligent Automation & Soft Computing*, vol. 27, no. 2, pp. 593–603, 2021.

[26] S. A. Khan, M. Alenezi, A. Agrawal, R. Kumar and R. A. Khan, "Evaluating performance of software durability through an integrated fuzzy-based symmetrical method of ANP and TOPSIS," *Symmetry*, vol. 12, no. 4, pp. 1–15, 2020.

[27] F. A. Alzahrani, M. Ahmad, M. Nadeem, R. Kumar and R. A. Khan, "Integrity assessment of medical devices for improving hospital services," *Computers, Materials & Continua*, vol. 67, no. 3, pp. 3619–3633, 2021.

[28] V. Torra and Y. Narukawa, "The index and the number of citations: Two fuzzy integrals," *IEEE Transactions on Fuzzy Systems*, vol. 16, no. 6, pp. 795–797, 2008.

[29] W. Alosaimi, R. Kumar, A. Alharbi, H. Alyami, A. Agrawal *et al.,* "Computational technique for effectiveness of treatments used in curing sars-cov-2," *Intelligent Automation & Soft Computing*, vol. 28, no. 3, pp. 617–628, 2021.

[30] K. Sahu, F. A. Alzahrani, R. K. Srivastava and R. Kumar, "Evaluating the impact of prediction techniques: Software reliability perspective," *Computers, Materials & Continua*, vol. 67, no. 2, pp. 1471–1488, 2021.

[31] R. Kumar, M. Zarour, M. Alenezi, A. Agrawal and R. A. Khan, "Measuring security durability of software through fuzzy-based decision-making process," *International Journal of Computational Intelligence Systems*, vol. 12, no. 2, pp. 627–642, 2019.