Available online at www.ijcmit.com

International Journal of Contemporary Management and Information Technology (IJCMIT)

Volume 6, No 2, 2026, pp. 1-6

e-ISSN: : 2773-5036

Multi-dimensional Aspects Related to Internet Privacy Concerns and Security in Relation to the Acceptance and Usage of Internet of Medical Things (IOMT).

[1]Ibrahem Altuwim, [1]Fayez Al-qaisi, [1]Abdalaziz Alghaythi, [1]Abdulaziz Salami [1]Odai Enaizan

[1], Management Information Systems, College of Haqel, University of Tabuk, KSA,
*Corresponding to aonaizan@ut.edu.sa

Article history
Submitted: 28 October, 2025
Revised: 05 January 2026
Accepted: 27 January 2026

Keywords:
Privacy, security, IOMT, acceptance and healthcare

Abstract

A The Internet of Medical Things (IoMT) has the potential to much improve healthcare services by means of better data availability and real-time monitoring. Still, security and privacy concerns are big obstacles to its adoption. This research investigates the factors affecting Saudi Arabian users' behavioral intention to adoption IoMT systems with particular attention to privacy and security issues. Using the Unified Theory of Acceptance and Use of Technology (UTAUT), the study employs a quantitative method and analyzes survey data acquired from 191 respondents. The suggested model assesses how behavioral intent is impacted by performance expectancy, effort expectancy, social influence, security, privacy. The empirical results indicate that performance expectancy, effort expectancy, social influence, facilitating conditions, and security have a positive influence on the adoption of IoMT, while privacy has a major negative effect. High explanatory power allows the model to explain 43.6% of the variance in behavioral intention. Emphasizing the requirement of applying tight security precautions to resolve privacy issues and enhance trust in IoMT systems, the findings have significant practical consequences for Saudi Arabian healthcare decision-makers and technology innovators.

1. Introduction

This Wireless health parameter monitoring is made possible by the Internet of Medical Things (IoMT) which lowers needless hospital stays and the related healthcare expenses. The IoMT industry encompasses wearable and home-based real-time health monitoring devices as well as point-of-care (POC) devices utilized in hospitals or other medical facilities. Wearable medical IoT devices can identify inadvertent falls in senior citizens. Even though falls are unavoidable for older adults chronic injuries can be avoided by keeping an eye on their surroundings and preventing accidents. Customers now have access to online storage services and automated detection technologies thanks to digital healthcare which is drastically changing traditional medical monitoring systems. Patients physicians and people living in remote areas can now readily obtain high-quality healthcare services because of this technological breakthrough. [1]. Thermometers glucose meters ECG readers ultrasounds and other healthcare center equipment with cloud storage and internet access allow users to keep an eye on their health. Technological developments that allow for direct patient-physician communication and insulin dosage adjustments are crucial for improvised healthcare. The idea of the smart bed which can change the beds position and angle according to the patients level of comfort has started to be implemented in contemporary healthcare facilities. Traditional home healthcare solutions are being revolutionized by IoMT-powered devices. For instance a smart drug dispensing system automatically uploads a persons clinical history to the cloud. This system lets doctors know when a patient forgets to take their medication and lets patients know when they need it. Urbanization industrial adaptation and technological advancements are driving up demands on the healthcare system. These devices can be used to enable routine healthcare monitoring. [2] with [3]. The Saudi King and government plan to increase private healthcare spending in Saudi Arabia from 25% to 35% by 2020 with regard to e-healthcare services.[4]. Saudi Arabias Vision 2030 seeks to make the Kingdom a prominent nation with a thriving economy and a leader in the Middle East and Asia. The provision of reasonably priced e-healthcare services to citizens is another aspect of this objective and vision. There is an urgent need to investigate ways to secure and make tamper-resistant smart hospital management systems in order to reach the goal of highly effective secure and reliable systems. Additionally the Saudi

Arabian economy will benefit from a smart hospital management system in numerous ways. Patients and foreign investors will be drawn to the Arab healthcare sector by sophisticated hospital services and advanced security measures. A smart hospital management system must digitize all services offered by healthcare providers. However there are risks associated with integrating a traditional IoT and IoM environment in a smart hospital management system according to current IoT security and hacking statistics [5]. The goal of this proposed work is to develop a methodical procedure for using IoT and IoM devices to manage smart hospitals [6]. Our studys second major focus is Saudi Arabias smart hospital management system security. The difficulties that smart healthcare organizations face are substantial and grave. This study offers a novel approach: investigating methods for setting up safe smart hospital management systems in Saudi Arabia an area that hasn't been studied before.

2. Literature Review

The Internet of Medical Things (IoMT) has great potential to improve patient outcomes and healthcare efficiency user perceptions of security and privacy have a big impact on its adoption. Concerns about perceived risk trust data confidentiality and regulatory compliance have been found to be important elements influencing patient and healthcare professional acceptance. As a result current research highlights the direct and indirect effects of privacy and security considerations on behavioral intention to adopt IoMT systems by incorporating them into technology acceptance models. [7].

This section examines pertinent research that discusses security and privacy as factors influencing IoMT adoption and acceptance. Kamalov and others. In order to facilitate the safe deployment of Internet of Medical Things (IoMT) systems [8] (2023) examined privacy and security issues. The study looked at encryption techniques security flaws data privacy risks and a lack of standardization. The results demonstrated that while contemporary security measures lower risks communication and interoperability flaws continue to erode trust and impede IoMT adoption. Alhumaid & Co. [9] (2025) looked into what influences the adoption of IoT technologies including IoMT applications in settings related to healthcare. Within a framework of technology acceptance the study concentrated on perceived utility usability and privacy and security perceptions. The findings showed that while privacy and security concerns indirectly lower willingness to adopt IoMT systems positive user attitudes boost adoption intention. Mabina & Co. [10] (2024) investigated the security privacy and ethical issues influencing IoMT adoption in emerging healthcare systems. Weak data protection laws moral dilemmas inadequate encryption techniques and ignorance were among the factors examined. The findings demonstrated that IoMT adoption is severely hampered by inadequate privacy and regulatory frameworks highlighting the need for more robust governance. Joseph and others. [11] (2025) looked at the impact of cybersecurity risks on IoMT adoption in connected medical devices. Weak encryption insecure communication protocols and unauthorized access were the main topics of the study. Results showed that high perceived security risks lower acceptance and trust confirming security as a crucial factor in IoMT adoption. IoMT device security was analyzed by Akinbi and Paul Raj [12] (2025) to find weaknesses affecting user confidence. The study looked into communication vulnerabilities encryption defects and authentication weaknesses. The findings indicated that unless addressed security flaws limit the adoption of IoMT technologies by endangering data privacy and undermining user confidence. .

2.1 Models and theories of technology acceptance

2.2.1 UTAUT Theory

Studies using the UTAUT2 model to assess the adoption and use of information and communication technologies (ICTs) are still limited. Therefore, the UTAUT2 model is used in this study. This model was developed by modifying the UTAUT model [13] to make it more customer-centric. The UTAUT2 model is well-suited for assessing technology adoption and customer acceptance.

The UTAUT2 framework modifies structures based solely on skills, gender, and age. Because the target audience doesn't need to use machines, free usage is less common. UTAUT2 adds three more structures: the cost of habit versus money, and the pleasurable incentive. Rationalizing behavioral goals and user behavior, the pleasurable incentive, and price values contribute to clarifying the purpose of actions and habits. Unlike UTAUT, UTAUT2 extensions achieve significant improvements in behavioral intent variability (56–74%) and time used (40–52%) [13] (Venkatesh Thong and Xu, 2012). However, [14] argues that the value-for-money concept should be removed if the system is made available to the public.

2.2 Theoretical model proposal

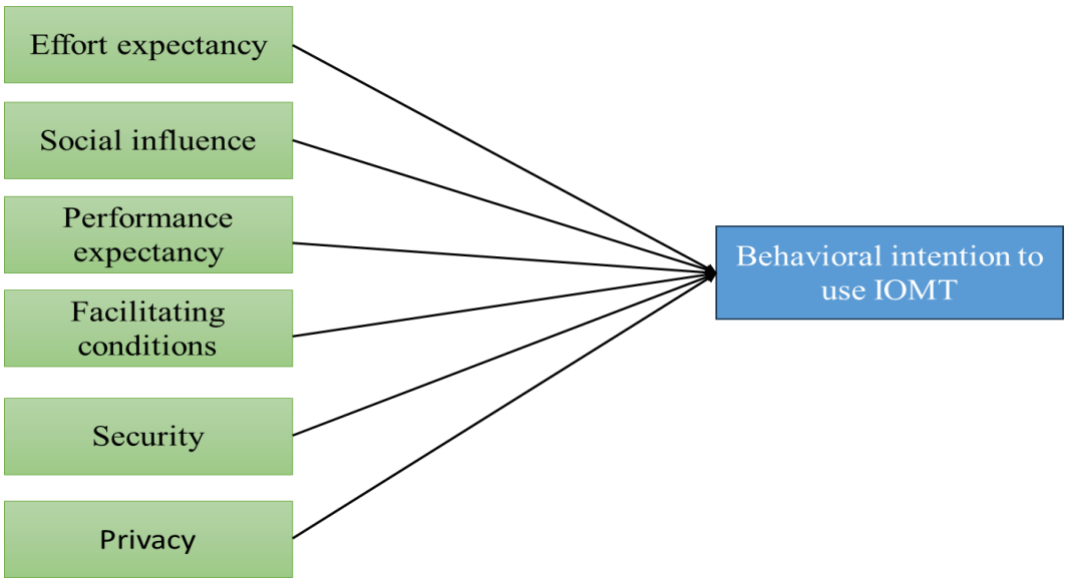

Figure 1 Proposed framework

3 Methodology

3.1 Population and sampling

Amid July and September 2024, electronic questionnaires were used to conduct a self-administered survey in Saudi Arabia. The sampling frame was based on a random sampling method. Two hundred valid responses were collected from patients. Missing, outlier, and normal values were processed through data cleaning and screening procedures. As a consequence of these procedures, 9 cases were excluded, including those that did not answer their questions, those lacking data, and anomalies. Ultimately, 191 acceptable responses were retained for statistical analysis.

3.2 Instrument

The specialists used a five-point Likert scale questionnaire to collect data and participant responses. Responses ranged from (1) strongly disagree to (5) strongly agree on a scale of one to five. Cronbach's alpha coefficient, shown in Table 2, was used to assess the reliability of the pilot study.

Table 1 Instrument

Variables	Items	Cronbach's alpha
Behavioral intention to use IOMT	4	0.834
Facilitating conditions	5	0.748
Performance expectancy	4	0.851
Effort expectancy	5	0.724
Social influence	5	0.842
Privacy	4	0.884
Security	5	0.795

4. Test The Hypotheses of The Study

This study's model explained 43.6% of the variance in business intelligence, demonstrating its goodness of fit and showing that the majority of factors predicting mobile IoT adoption were included. This variance is also explained by the current study's model's high degree of similarity to the capabilities of the original UTAUT model [15]. Overall, six path relationships were tested in this study, and the results indicated six statistically significant (hypothetically) significant relationships with the behavioral intention to adopt mobile IoT.

Hypotheses:

H 1 The effort expectation has a positive influence on intention for use of IOMT.,

H2: The performance expectation has a positive influence on intention for usage of IOMT.

H3: The Social influence has a positive influence on intention for usage of IOMT.

H4: Facilitating circumstances has a positive impact on intention for usage of IOMT.

H5: security has a positive impact on intention for usage of IOMT.

H6: The privacy has a negative influence on intention for usage of IOMT.

Table2: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.660a	.436	.432	3.32623
a. Predictors: (Constant), SOL, privacy, EFE, PEXP, PCC, security				

Table3: ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	7436.523	6	1239.421	112.025	.000b
	Residual	9636.567	871	11.064		
	Total	17073.090	877			
a. Dependent Variable: INT						
b. Predictors: (Constant), SOL, privacy, EFE, PEXP, PCC, security						

Table4: Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	8.014	.648		12.358	.000
	security	.092	.038	.078	2.416	.016
	privacy	-.355	.021	-.474	-17.168	.000
	PEXP	.266	.035	.226	7.551	.000
	EFE	.160	.037	.131	4.368	.000
	PCC	.135	.043	.100	3.170	.002
	SOL	.079	.028	.085	2.804	.005
a. Dependent Variable: INT						

5. Discussion

In the acceptance and use of medical process management technologies in general, effort expectancy is positively correlated. The first hypothesis (H1) was proposed, defended, and supported in this study. [16] also emphasize the importance of effort expectancy, noting that 15% of all barriers to adopting electronic health records in Saudi Arabia were related to effort expectancy. Additionally, perceived performance is positively correlated. The second hypothesis (H2) was proposed and supported in this study. It was also noted that perceived deficits in IT performance are a significant barrier in healthcare, and studies on the adoption of electronic health records in Saudi Arabia have indicated that a lack of perceived benefit or perceived performance contributes to 15% of the total barriers [16].

However, social influence is positively correlated. Hypothesis H3 was proposed, promoted, and supported in this study. Social networks play a crucial role in the adoption or acceptance of IoT technologies, as it has been generally observed that IoT users seek help and advice from their families, peers, and colleagues to clarify any doubts they have about the product [17].

In addition, enabling conditions are positively correlated. Hypothesis H4 was proposed, promoted, and supported in this study. Enabling conditions have a statistically significant combined positive effect on IoT adoption motivations [19]. Furthermore, security is positively correlated. Hypothesis H5 was proposed, promoted, and supported in this study. Al-Qahtani's study [19] indicated that privacy and security issues are major obstacles preventing the Saudi healthcare sector from adopting IoT technology. Al-Qahtani, A. (2020). Moreover, [20] found that privacy and security are the primary concerns of patients regarding their health records, and a study by [21] provided empirical evidence on the role of privacy and security from the perspective of personal health records. However, an inverse relationship exists between privacy and security. This study introduces and supports the H6 hypothesis, asserting that violations of personal information privacy should be addressed by managing the security challenges rather than through individual resistance. In this way, translucent protection standards will be important for the successful transition to smart cities. Brown [20].

6. Conclusion

The present study analysed the privacy, security, and utaut factors that influence the acceptance of iomt. The study successfully achieved its objective of examining the factors affecting the acceptance and use of these services in Saudi Arabia and developing a proposed model. This study expanded the scope of the UTAUT test to achieve its objectives, validating it through reliable statistical analyses. The results obtained using UTAUT can be used as numerical data, thus providing a basis and justification for decisions of decision-makers'. This result may also contribute to enhancing the knowledge of developers of electronic medical process management (IOMT) applications by improving existing applications based on the weaknesses highlighted by the study. Furthermore, this result strengthens the position of IOMT, particularly regarding the acceptance and use of stored data records in healthcare institutions. It is also expected that adaptive user characteristics such as security, privacy, aspects of UTAUT and reuse of these results, which are recognized and used in IOMT, will help in creating UTAUT.

Acknowledgment

The authors extend their appreciation to the Deanship of Research and Graduate Studies at University of Tabuk for funding this work through Research no. S-0217-1443.

References

[1] Sakib, SM Nazmuz. "Internet of Medical Things (IoMT) for Remote Healthcare Monitoring Using Wearable Sensors." International Journal of Computing and Related Technologies 4, no. 2 (2023): 36-50.

[2] Manickam, Pandiaraj, Siva Ananth Mariappan, Sindhu Monica Murugesan, Shekhar Hansda, Ajeet Kaushik, Ravikumar Shinde, and S. P. Thipperudraswamy. "Artificial intelligence (AI) and internet of medical things (IoMT) assisted biomedical systems for intelligent healthcare." Biosensors 12, no. 8 (2022): 562.

[3] Aljabr, Ahmad Abdullah, and Kailash Kumar. "Design and implementation of Internet of Medical Things (IoMT) using artificial intelligent for mobile-healthcare." Measurement: Sensors 24 (2022): 100499.

[4] Alhakami, Hosam, Abdullah Baz, Mohammad Al-shareef, Rajeev Kumar, Alka Agrawal, and Raees Ahmad Khan. "A Framework for Securing Saudi Arabian Hospital Industry: Vision-2030 Perspective." Intell. Autom. Soft Comput 36, no. 3 (2023): 2773-2786.

[5] 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.

[6] 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

[7] Hameed, Shilan S., Wan Haslina Hassan, Liza Abdul Latiff, and Fahad Ghabban. "A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches." PeerJ Computer Science 7 (2021): e414.

[8] Kamalov, Firuz, Behrouz Pourghebleh, Mehdi Gheisari, Yang Liu, and Sherif Moussa. "Internet of medical things privacy and security: Challenges, solutions, and future trends from a new perspective." Sustainability 15, no. 4 (2023): 3317.

[9] Alhumaid, Khadija, Kevin Ayoubi, Maha Khalifa, and Said Salloum. "Factors Determining Acceptance of Internet of Things in Medical Education: Mixed Methods Study." JMIR Human Factors 12, no. 1 (2025): e58377.

[10] Mabina, Alton, Neo Rafifing, Boago Seropola, Thapelo Monageng, and Pulafela Majoo. "Challenges in IoMT Adoption in Healthcare: Focus on Ethics, Security, and Privacy." Journal of Information Systems and Informatics 6, no. 4 (2024).

[11] Joseph, Blaise, H. Priya, G. Reethikaa, S. Rasi, Divya P. Chandran, Sriragasudha Konda Chandrasekaran, and Felyshia Shireen ES. "The Internet of Medical Things (IoMT): Analysing Cybersecurity Threats in Connected Healthcare Devices." Journal of Pioneering Medical Sciences 14, no. 10 (2025).

[12] Akinbi, Alex, and Preethi Paul Raj. "A systematic security analysis of medical internet of things (MIoT) ecosystems in threat modeling scenarios." Frontiers in the Internet of Things 4 (2025): 1712430.

[13] Venkatesh, Viswanath, James YL Thong, and Xin Xu. "Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology." MIS quarterly (2012): 157-178.

[14] Raman, Arumugam, and Yahya Don. "Preservice teachers' acceptance of learning management software: An application of the UTAUT2 model." International education studies 6, no. 7 (2013): 157-164.

[15] Aldhaen, F. S. (2022). Study of the Continuous Intention to use Artificial Intelligence Based Internet of Medical Things (IoMT) During Concurrent Diffusion. The Influence Diffusion of Innovation Factors Has as Determinants of Continuous Intention to Use Ai-Based IoMT (Doctoral dissertation, University of Bradford).

[16] Alqahtani, Asma, Richard Crowder, and Gary Wills. "Barriers to the adoption of EHR systems in the Kingdom of Saudi Arabia: an exploratory study using a systematic literature review." Journal of Health Informatics in Developing Countries 11, no. 2 (2017).

[17] Gao, Lingling, and Xuesong Bai. "A unified perspective on the factors influencing consumer acceptance of internet of things technology." Asia Pacific Journal of Marketing and Logistics 26, no. 2 (2014): 211-231.

[19] Alqahtani, Asma. "A model of electronic health record systems adoption by primary healthcare physicians in the Kingdom of Saudi Arabia." PhD diss., University of Southampton, 2020.

[20] Kisekka, Victoria, and Justin Scott Giboney. "The effectiveness of health care information technologies: evaluation of trust, security beliefs, and privacy as determinants of health care outcomes." Journal of medical Internet research 20, no. 4 (2018): e9014.

[21] Lafky, Deborah Beranek, and Thomas A. Horan. "Personal health records: Consumer attitudes toward privacy and security of their personal health information." Health Informatics Journal 17, no. 1 (2011): 63-71.