Contents lists available at GrowingScience

International Journal of Data and Network Science

homepage: www.GrowingScience.com/ijds

Extending UTAUT: The role of internet privacy concerns and security in predicting acceptance of Internet of Medical Things (IoMT)

Odai Enaizan[a*]

[a]*Management Information Systems, College of Haqel, University of Tabuk, Saudi Arabia*

C H R O N I C L E

Article history:
Received January 24, 2026
Received in revised format March 14, 2026
Accepted April 2 2026
Available online
April 2 2026

Keywords:
Security
IPC
Acceptance
IOMT and Usage

A B S T R A C T

Security and privacy are essential concerns for IoMT. Whilst existent research has investigated the associations between security and privacy with intention to use and acceptance, determinants related to formation of security and privacy for IoMT still remain largely unexplored. This study is an examination of security and privacy determinants of IoMT based upon UTAUT. Criterion sampling was employed in gathering 528 IoMT user datasets and revealed the following results: A) six determinants (authorization, availability, non-repudiation, data integrity, effort expectancy and performance expectancy) exerted an important and explicit positive effect upon the usage and acceptance of IoMT; B) six determinants (secondary usage, collection, improper access, errors, awareness and control) exerted a significant and direct negative effect upon acceptance and use of IoMT; C) three determinants (confidentiality, facilitating conditions and social influence) insignificantly affected behavioral intention in users within Jordan regarding use of IoMT. The integrated form of the model does predict 62.5% for privacy and security for IoMT.

© 2026 by the authors; licensee Growing Science, Canada.

1. Introduction

Significant improvements are expected for quality of care and efficiency within the healthcare industry, a case in point being the diversity in the range of developments of IoT (Internet of Things), often known as IoMT (Internet of Medical Things) (Mishra & Singh, 2023; Y. Sun et al., 2019). Medical devices equipped with sensors for interconnection within the sector of healthcare are known as IoMT(Vaiyapuri et al., 2021). Through the utilization of IoMT, hospital workloads can be decreased since unnecessary hospital visits can be restricted. In addition, a data transmission environment is provided that is safe for the interchange of sensitive medical data from within diverse medical sectors. The application of IoMT has become an appropriate option, however concerns have been raised over issues of trust, privacy and security, and these issues have received more attention from academic researchers in recent times(Somasundaram & Thirugnanam, 2020).Rapid IoMT development, however, has resulted in there being insufficient attention paid to matters of privacy and security of IoMT within healthcare systems. For instance, a consequence of the IoMT in healthcare systems having inadequate security could be that the privacy of patients is compromised because of eavesdropping, and the detection of episodes that are life threatening can be delayed because of DoS (Denial of Service) attacks to normal IoMT device operations. All IoMT within healthcare systems ought to just be accessed by devices or users that are authenticated and authorized (KUMAR & SIRAJUDDIN, 2024; Y. Sun et al., 2019).Personalized health data has to be stored and processed by IoMT devices, a number of which even possess actuation functions in support of the health of users, i.e., the insulin pump. So, there is an expectation that security levels needed for devices of IoMT are much higher when compared to typical computing devices and IoT (Stern et al., 2019). However, threats and security can still be overlooked within IoMT healthcare system design. The design of most IoMT devices are geared towards transmission and storage of data within the 'cloud', and it may then be processed and analyzed further. Such advancements within healthcare systems enable medical care providers to offer patients more accurate and quicker responses when monitored through healthcare and medical devices. However, there is the introduction of risk for the data of users that is stored within servers of the cloud since there is the possibility of it being stolen or abused (Williams & McCauley, 2016).

* Corresponding author
E-mail address aonaizan@ut.edu.sa (O. Enaizan)

ISSN 2561-8156 (Online) - ISSN 2561-8148 (Print)
© 2026 by the authors; licensee Growing Science, Canada.
doi: 10.5267/j.ijdns.2026.4.001

There has to be good protection of the privacy of the data of users, particularly in relation to their personal data. If, in a breach of security, such data has been stolen, it is both critical and challenging to retrieve and eliminate that data. In order to protect the data of patients, severe penalties and strong regulations from the healthcare professional have to be in place. However, the reality is that there are lots of examples where cloud servers have had security breaches from large enterprises, and this raises the question of whether it is truly possible to fully protect the sensitive health data of patients when stored that way (W. Sun et al., 2018). Indeed, since personal health data can have great value within illegal markets, greater numbers of malicious attackers have been targeting eHealth systems and medical servers(Enaizan et al., 2020). So, stronger security measures are required by medical service providers and that, inevitably, results in increased costs in the creation, running and maintenance of their medical services. As such, the aim of this study is to gain an understanding of determinants for the usage and acceptance of users of IoMT, and prediction of them, based upon the hybrid approach between ANN and PLS-SEM.

2. The literature review

2.1 Studies related to the acceptance and usage of IoMT

Within healthcare, 'IoT' is in reference to the IoMT. IoMT are designs for robotic devices aimed at providing elderly patients with mobility rehabilitation (Long & Hoang, 2017), and the development of systems for the collection, integration and access of patient information that is supportive in medical emergencies(B. Xu et al., 2014). However, the acceptance of users of a particular form of technology can be considered a major determinant with respect to the actual usage behavior(Gao & Bai, 2014). Moreover, Previous studies have tended to focus upon the implementation of technology and/or efficiency in economic terms and so the aforementioned research gap has continued to be somewhat overlooked. A large proportion of studies has taken a focus on analyses at the level of the individual or the organization with only rare examples of studies that have integrated those two levels within an investigation of IoMT. For a more complete understanding, a combination of both approaches is useful. Since IoMT is heterogeneous and complex, there is a need for it to be examined from the perspective of users in a way that encompasses factors that are user-related, organizational and social. Within this section, there is presentation of a review of extant literature with regard to factors and barriers that impact upon intention for IoMT use. The construct of intention to use signifies an aspect of the behavior of users that is important and is an indication of post-acceptance behavior in relation to the technology introduced (Zhanyou et al., 2020). It can be seen within the literature that there is still evolution of IoMT and, in fact, the use of it can be considered as still being in its infancy (Nakshbandi et al., 2023). There is an indication, then, that IoMT diffusion could have an association with the usage of IoMT. The suggestion from the examples is that a more detailed literature review could uncover further factors that have a bearing on intention for IoMT use. The literature shows that the sustained and successful use/the intention to use in regard to IoMT is affected by a certain limit of factors that have still not been researched well, particularly in the context of security and privacy(Al-Dhaen et al., 2021). In regard to the intention of using IoMT, mixed signals are given by medical professionals in relation to the acceptance of it and its continuous use. It is stated by some that there is value in using IoMT or, indeed, any intelligent device since a relative advantage is offered when compared with existing, more traditional techniques. However, others consider that complex technologies are difficult to use (Mavrogiorgou et al., 2019). Kamalov et al. (2023) provided a comprehensive literature review of IoMT privacy and security challenges and emphasized the role of trust in shaping users' willingness to adopt IoMT technologies. However, the study remains primarily descriptive and does not integrate privacy and security variables into a validated acceptance framework such as TAM or UTAUT, resulting in limited explanatory power regarding adoption behavior. Farooqi and Zafar (2024) analyzed security and privacy vulnerabilities in IoMT architectures and identified perceived risk and data confidentiality as major adoption barriers. Despite acknowledging adoption implications, the study does not empirically test these factors within UTAUT or UTAUT2, nor does it examine how privacy and security influence core constructs such as performance expectancy or facilitating conditions. Rajab et al. (2024) reviewed existing related studies in IoMT security and privacy models and highlighted the lack of standardized governance and compliance mechanisms. While their findings relate conceptually to the facilitating conditions constructed in UTAUT, the study does not investigate individual-level acceptance or behavioral intention, leaving a gap between organizational security readiness and user adoption behavior. Alharbi et al. (2025) proposed a machine-learning-based threat detection framework aimed at improving IoMT security resilience. Although the study demonstrates technical effectiveness, it does not assess how enhanced security influences users' perceived usefulness, trust, or behavioral intention within TAM, UTAUT, or UTAUT2, limiting its relevance to adoption research. Al-Turjman et al. (2025) conducted a systematic literature review on IoT adoption in healthcare and identified privacy and cybersecurity as key barriers. However, the review indicates that few empirical studies explicitly incorporate privacy and security as independent dimensions within UTAUT2. Most existing studies either treat these concerns as background issues or embed them indirectly within facilitating conditions, without formal measurement or hypothesis testing. Whilst the literature demonstrates no certainty with regard to the factors that have a bearing on intention for IoMT use, some studies have outcomes that show encouraging results in that respect. For example, the attitudes, behaviors and motivations of users (Abildgaard et al., 2016), training issue (Saarikko et al., 2017), relative advantages in use of IoMT, IoMT complexity, compatibility, and observability (Saarikko et al., 2017), AI awareness (Mansour et al., 2019), the age (Venkatesh et al., 2012)and the novelty-seeking behavior (Miladinovic & Hong, 2016) have been discovered to be certain factors identified within the literature that affect intention towards IoMT use embedded within responsible forms of AI. However, issues for security and privacy within the context of the IoMT that is embedded along with responsible forms of AI is not addressed by the research within those studies in scenarios when the two are concurrently diffusing and there the factors are interacting within one holistic model (Almotiri, 2025). Overall, these

studies collectively demonstrate that privacy and security issues are consistently recognized as barriers to IoMT acceptance. Nevertheless, empirical research that explicitly integrates privacy and security factors as distinct constructs within acceptance models, particularly UTAUT2, remains limited. Existing related studies tend to emphasize technical solutions, conceptual discussions, or partial adoption models, leaving a significant gap in understanding how privacy and security perceptions directly and indirectly influence IoMT acceptance and behavioral intention. Addressing this gap and issues is very important for developing a comprehensive and context aware IoMT adoption Model.

3. The research model and the development of hypotheses

3.1 Theories and models for acceptance of technology

Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al., 2003), Performance expectancy refers to perceived gains in job performance, effort expectancy indicates ease of use, social influence reflects perceived social pressure, and facilitating conditions denote the availability of supporting infrastructure (Venkatesh et al., 2003). Empirical evidence, including meta-analyses, confirms significant relationships among these constructs and behavioral intentions (Taiwo & Downe, 2013). However, inconsistencies in findings, particularly in social science contexts, have raised concerns about model validity, partly due to limited examination of moderating effects (Dwivedi et al., 2011; Taiwo & Downe, 2013). Moreover, Applications of UTAUT in emerging domains such as IoMT remain limited; thus, recent studies have extended the model by integrating security and privacy as key determinants of technology adoption. (Alalwan et al., 2017; Martins et al., 2014).

3.2 Individual factors

UTAUT has been applied with the context of healthcare in order to explore acceptance of HIT (Ariaeinejad & Archer, 2014) and (Slade et al., 2013; Alazzam et al., 2015). This also considers those factors individually.

EE (effort expectancy): EE has been defined as ‘‘the degree of ease associated with the use of any system’’ (Venkatesh et al., 2003). EE does have a strong impact upon the intention of users to employ health information systems and it has a positive impact upon acceptance of it. Particularly when technologies are new, the extent to which ease is associated with its use affects strongly acceptance behavior, especially in the case of older users (Kim & Park, 2012). Also, a relationship exists between intention to use and EE (Gardiyawasam Pussewalage & Oleshchuk, 2016). So, it is hypothesized here that:

$H_{1.a}$: *The effort expectancy has a positive impact on intention for use of IOMT.*

PE (performance expectancy): PE was defined by Venkatesh et al. (2003) as ‘‘the degree to which using a technology will provide benefits in performing certain activities’’. In regard to the intention of users to use new technology, a key role for acceptance is perception that technology will be helpful and beneficial (Arning & Ziefle, 2009). If, however, there are doubts and fears in users regarding the usefulness of technology, a negative influence can be created and the rate of adoption affected(Or et al., 2011). Previous research has established the relationships between intention for using healthcare services and usefulness (Hoque & Sorwar, 2017). The hypothesis that corresponds to that is as follows:

$H_{1.b}$: *The performance expectancy has a positive impact on intention for use of IOMT.*

FC (facilitating conditions): FC has been defined as ‘‘the degree to which an individual believes that an organizational and technical infrastructure exists to support the use of the system’’ (Venkatesh et al., 2003). FC is a determinant with a direct influence upon the behavioral intention as well as employment of technology (Mun et al., 2006). Further confirmed that fact within the context of use of a system for health information(Bhattacherjee & Hikmet, 2008). Within the context of the users of ICT that is health-related, the BI is significantly increased by the availability and ready access to technical support(Or et al., 2011; Kijsanayotin et al., 2009).So, for the purposes of this research, it is therefore hypothesized that:

$H_{1.c}$: *The facilitating conditions have a positive impact upon intention for use of IOMT.*

SI (social influence): During the early stages of any type of new technology, users of such systems do not have sufficient information with regard to its usability. In such cases, a user could be influenced by suggestions or opinions offered by relatives, healthcare providers and/or their homecare nurse, for example(Or & Karsh, 2009). There has been verification of the positive relationship existing between usage intention and SI within several previous studies(Kim & Park, 2012), (Kijsanayotin et al., 2009). As such, it is hypothesized that:

$H_{1.d}$: *The social influence has a positive impact on intention for use of IOMT.*

3.3 Privacy factors

Traditionally, privacy concerns have fit within the realms of research into business ethics(Hong et al., 2019). Particular to the context of online activity, IPC (internet privacy concern) can be defined as the concern that an individual has over the possibility of loss of privacy because of surreptitious or voluntary information disclosure upon websites(Dinev & Hart, 2005). That IPC definition is an extension from a traditional conceptualization of concern over information privacy that refers to the perception that an individual has of fairness in an information privacy context within an online environment (Hong et al., 2021). IPC is viewed as a relationship that is dyadic between an online entity, which may be either websites generally or a

particular website, and an individual. Previous research has adopted similar definitions in its study of IPC (Hong & Thong, 2013). In previous IPC conceptualizations, 6 key dimensions have been utilized most-commonly, i.e., secondary usage, collection, unauthorized access, errors, awareness and control. The definitions for those dimensions were adapted by the researchers for the current context for the research. To be specific, collection was considered the extent to which someone has concern over the volume of data that is individual-specific that is possessed by websites (Hong & Thong, 2013).Within a health information context, collection refers to the concern of an individual with regard to collection of health information and its storage by providers of healthcare (Angst & Agarwal, 2009). Often, health information is considered as having great sensitivity, with citizens generally viewing their own personal health information in that way (Bélanger & Crossler, 2011). It may be argued, therefore, that there is a likelihood that Irish citizens will express concern if they have the perception that large volumes of such information are being collected by healthcare providers. So, there ought to be examination of collection in a context of concerns over information privacy that pertain to EHRs. Secondary usage refers to the extent to which someone has concerns that the personal information that is collected for a purpose by a website is used for another purpose that has not been authorised by the individual (Hong & Thong, 2013).

Often, in regard to health information, it is posited that people have less concern when they disclose information initially because they have trusted relationships with their doctors; however, concerns set in if that information is shared(Caine & Hanania, 2013).Error refers to the extent to which people have concerns that protections against accidental and deliberate errors within the personal data that websites collect are inadequate(Smith et al., 1996).That dimension has relevance for concerns over health information privacy since medical data errors have the potential of impacting upon the health of individuals if they were to be prescribed inappropriate medications to which they had an allergic reaction, for instance. Moreover, within a recent study that gave access to personal EHR for patients, 32% of participants found errors within their particular personal medical information (Pussewalage & Oleshchuk., 2016). Improper access refers to the extent that a person has concerns that there is ready availability of personal information that is held by websites to other people that have not been authorised properly to work with or view the data(Smith et al., 1996).In respect to health information, concerns are repeatedly expressed by individuals that employers or that non-healthcare organizations could be able to access their particular personal health information(Angst, 2009). Fears have also been expressed by individuals that their history could be accessed by hackers or malicious employees and mental health impacts (Powell et al., 2006). Control refers to the extent to which someone has concerns that she/he has an inadequate degree of control over her/his personal information that is held within websites (Malhotra et al., 2006). Within the health information context, lots of studies have discovered that control over personal health information is desired by citizens. Also, it has been discovered that when individuals were not offered a degree of control by EHRs, higher levels of concern were expressed in regard to their information privacy (Powell et al., 2006). Also, the argument has been made that individuals ought to have the ability of exercising control in relation to who is able to access their particular EHR (Dinev et al., 2013). Lastly, awareness is in reference to the extent that someone has concerns over her/his awareness of the practices of information privacy for websites (Malhotra et al., 2006).Within the health information privacy context, it has been found that awareness has extreme importance and that in many cases it is lacking. For instance, a considerably large number of New Zealand respondents were uninformed and unaware with regard to EHRs and, thus, had greater concerns regarding privacy for their particular health information (Cecil et al., 2017). A lack in the awareness of patients with regard to how their particular health information is utilised by healthcare organisations has been highlighted repeatedly; see, for example (Sipior et al., 2013).

$H_{2.a}$: *Unauthorized access has a negative impact on intention for using IOMT.*
$H_{2.b}$: *Error has a negative impact on the intention of using IOMT.*
$H_{2.c}$: *Secondary use has a negative impact on the intention of using IOMT.*
$H_{2.d}$: *Collection has a negative impact on intention of using IOMT.*
$H_{2.e}$: *Control has a negative impact on the intention of using IOMT.*
$H_{2.f}$: *Awareness has a negative impact on the intention of using IOMT.*

3.4 Security factors

IoMT system success relies to a large degree upon security. There are five security requirements for those systems to provide confidentiality of data, integrity, availability of data, non-repudiation of it and authentication; these collectively are known as CIANA (Vyas & Pal, 2020). Due to the sensitivity and safety issues for the data of patients, there is a need for a group of requirements to enable the security of systems of IoMT to be ensured at all layers. The set of requirements derived from consideration of CIANA consists of the eleven security requirements that follow (Kasyoka et al., 2020). Confidentiality is defined as the ability for keeping data private whilst it is being gathered, stored or transmitted. Also, the data must solely be accessible for users who have been authorized. The techniques that are most commonly used in fulfilling that requirement are access control lists and data encryption; these are discussed further within the section below. The integrity requirement relates to capability for data to be protected from any kind of authorized tampering during the stages of data collection, data transmission and data storage. Integrity is in reference to the method to ensure that data is accurate and real, which means that the message received has content that does not have false insertion or unauthorized modification or deletion during the communication. Availability is defined as the ability of keeping IoMT systems running continuously and correctly, which can be achieved through the system being kept up-to-date, any changes to performance being monitored, provision if redundant storage for data or routes of transmission if there were to be DoS attacks, and by fixing any problems as quickly as possible. The requirement of availability assures that there is only accessibility of information to parties that are authorized.

If attackers are unable to compromise integrity and confidentiality in ongoing communication, users could try launching other kinds of attack, e.g., denying services of web servers so that a website is made unavailable to users that are legitimate. Non-repudiation relates to the ability of making each of the authorized users responsible for the actions of users (Bhushan et al., 2023). Authentication is in reference to the capability of validating user identity for those gaining access to the system. The form that is most secure is mutual authentication whereby both the client and the server authenticate one another prior to the exchange of any secure key/data. A mechanism of authentication validates identity for the parties that are communicating (identity authentication) or the messages sent during a communication (message authentication). Prior to starting a secure form of communication, the identities are verified mutually by both receiver and sender. Within an environment of IoMT communication, different entities are involved including IoMT devices (smart devices), different servers (fog servers/cloud), different users (static users/mobile), service providers of the cloud and gateway that require authentication amongst them depending upon the applications of IoMT (Adil et al., 2024).

$H_{3.a}$: *Data integrity positively impacts on intention of using IoMT.*
$H_{3.b}$: *Confidentiality has a positive impact on the intention of using IoMT.*
$H_{3.c}$: *Non-repudiation has a positive impact on the intention of using IoMT.*
$H_{3.d}$: *Authentication has a positive impact on the intention of using IoMT.*
$H_{3.e}$: *Availability has a positive impact on the intention of using IoMT.*

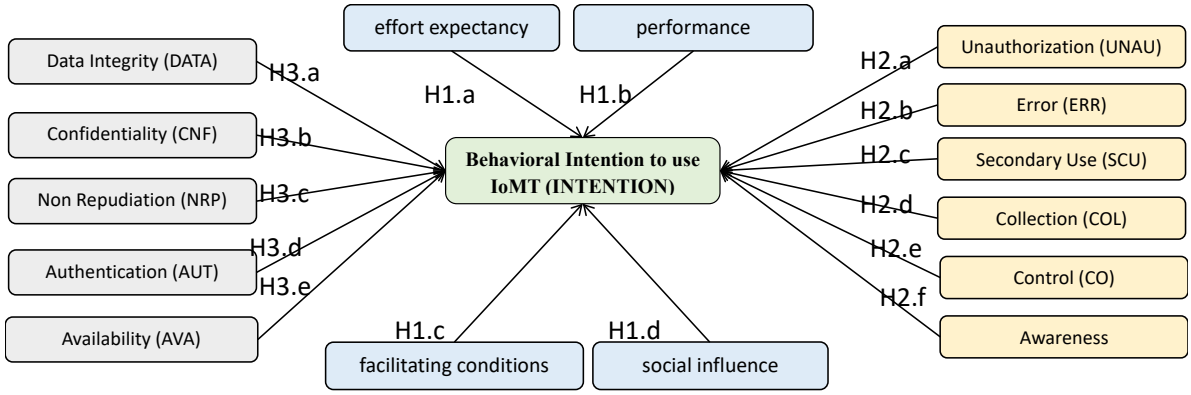

Fig. 1. The proposed conceptual model

4. Methodology

4.1 Population and sampling

The survey was self-administered and undertaken within Jordan from June to April of 2025 by way of online surveying. IoMT users are the target population with a random sampling method used as the sampling frame. In total there was a collection of 528 responses that were valid. Process of cleaning and examination of data were undertaken to address instances of outliers and missing values and normality. As such, those processes involved the deletion of 43 cases including instances of unanswered questions, outliers and missing data. In the end, 485 responses were considered usable and retained for further statistical analyses.

4.2 Instrument

A pilot study was conducted by using Cronbach's Alpha which is mentioned in Table 1.

Table 1
Instrument

Variables	Items	Alpha Value Pilot	Cronbach's Alpha
Behavioral intention to use IOMT (INTENTION)	4	30	0.795
Data Integrity (DATA)	5	30	0.841
Confidentiality (CNF)	4	30	0.701
Non-Repudiation (NRP)	5	30	0.801
Authentication (AUT)	4	30	0.913
Availability (AVAIL)	4	30	0.845
Unauthorization (UNAU)	3	30	0.867
Collection (COL)	4	30	0.842
Error (ERR)	4	30	0.834
Secondary Use (SCU)	4	30	0.853
Control (CO)	4	30	0.789
Awareness	4	30	0.718
Facilitating Conditions (FCC)	5	30	0.849
Performance Expectancy (PRE)	4	30	0.857
Effort Expectancy (EFE)	5	30	0.795
Social influence (SOCI)	5	30	0.916

4.3 Data Collection

The data collection process was conducted from 2025 using online questionnaires administered to the survey participants. Out of all distributed questionnaires, 498 complete and valid responses. This sample size was deemed adequate and statistically appropriate, surpassing the minimum threshold recommended for structural equation modeling according to (Hair et al., 2010).

4.2 Measurement model assessment

description of the measurement model assessment through the testing of discriminant and convergent validity. There was employment of discriminant and convergent validation to confirm construct validity for all of the scales. There was analysis of convergent validity through use of the three indices of factor loading, AVE and CR (construct reliability). Loading factors for each of the items has to be greater than 0.4 (Fornell & Larcker, 1981). AVE has to be greater than 0.5 and Cronbach's α (CR) has to be greater than 0.7 (Leguina, 2015). As can be seen in Table 2, all results were considered acceptable, and that shows that all scales had convergence validity.

Table 2
Convergent validity

Construct	Items	Loadings	CA	CR	AVE
Authentication	Q1	0.799	0.824	0.884	0.655
	Q2	0.831			
	Q3	0.795			
	Q4	0.813			
Non-repudiation	Q5	0.833	0.858	0.903	0.700
	Q6	0.856			
	Q7	0.820			
	Q8	0.838			
Confidentiality	Q10	0.855	0.881	0.918	0.737
		0.858			
	Q11	0.858			
	Q12	0.863			
Integrity	Q14	0.930	0.948	0.962	0.864
	Q15	0.940			
	Q16	0.925			
	Q17	0.923			
Availability	Q19	0.891	0.932	0.948	0.786
	Q20	0.879			
	Q21	0.885			
	Q22	0.896			
Collection	Q30	0.944	0.967	0.976	0.909
	Q31	0.949			
	Q32	0.949			
	Q33	0.943			
Secondary use	Q34	0.948	0.961	0.972	0.896
	Q35	0.952			
	Q36	0.957			
	Q37	0.958			
Unauthorized access	Q38	0.949	0.964	0.974	0.903
	Q39	0.955			
	Q40	0.947			
		0.951			
Error	Q41	0.958	0.970	0.978	0.919
	Q42	0.960			
	Q43	0.958			
	Q44	0.958			
Control	Q45	0.944	0.960	0.971	0.892
	Q46	0.945			
	Q47	0.940			
		0.950			
Awareness	Q48	0.958	0.973	0.980	0.924
	Q49	0.964			
	Q50	0.962			
Effort Expectancy	Q51	0.877	0.881	0.918	0.737
	Q52	0.842			
	Q53	0.847			
	Q54	0.866			
Performance Expectancy	Q55	0.863	0.888	0.923	0.749
	Q56	0.875			
	Q57	0.869			
	Q58	0.854			
Social Influence	Q59	0.865	0.882	0.918	0.737
	Q60	0.853			
	Q61	0.840			
	Q62	0.876			
Facilitating Conditions	Q63	0.877	0.892	0.925	0.754
	Q64	0.878			
	Q65	0.853			
	Q66	0.866			
Behavioral Intention	Q68	0.977	0.985	0.989	0.958
	Q69	0.978			
	Q70	0.978			
	Q71	0.981			

Discriminant validity is an indication of the degree to which there are discrepancies between 2 scales that are designed for measuring 2 different theoretical concepts(Hatcher & O'Rourke, 2013). So, that test was undertaken upon the dependent variable and the independent variable, particularly with consideration of the theoretical convergence of concepts in ways that can make us have complete uncertainty over differentiation between the measures. There is evidence for discriminant validity if AVE for two variables has a value that is higher than their squared correlation(Leguina, 2015).

Table 3
Discriminate validity

No.	Variables	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	**AUTH**	0.809															
2	**AVA**	0.291	0.887														
3	**AW**	-0.042	0.301	0.961													
4	**CNF**	0.444	0.292	0.034	0.859												
5	**COL**	-0.007	0.269	0.484	0.115	0.954											
6	**CON**	-0.025	0.333	0.415	0.022	0.447	0.945										
7	**Data**	0.310	0.403	0.327	0.341	0.252	0.281	0.929									
8	**EFE**	0.435	0.316	-0.100	0.440	0.081	0.052	0.363	0.865								
9	**ERR**	-0.028	0.255	0.472	-0.003	0.493	0.532	0.186	-0.014	0.958							
10	**FCC**	0.359	0.321	-0.028	0.385	0.097	0.052	0.328	0.409	0.000	0.868						
11	**INTENTION**	0.328	0.138	-0.443	0.271	-0.392	-0.454	0.155	0.359	-0.488	0.262	0.979					
12	**NRP**	0.397	0.319	-0.005	0.427	0.026	-0.020	0.372	0.404	0.016	0.370	0.336	0.837				
13	**PRF**	0.287	0.220	0.045	0.343	-0.089	-0.087	0.322	0.178	-0.086	0.354	0.325	0.407	0.858			
14	**SCI**	0.451	0.350	0.059	0.449	0.117	0.050	0.378	0.448	0.086	0.477	0.229	0.432	0.349	0.859		
15	**SCU**	0.034	0.285	0.389	0.063	0.458	0.461	0.293	0.096	0.515	0.041	-0.383	0.045	-0.018	0.168	0.946	
16	**UNAU**	-0.023	0.258	0.515	0.003	0.458	0.553	0.288	-0.012	0.486	-0.006	-0.466	-0.054	-0.126	0.072	0.477	0.950

Based upon Table 2 and upon Table 3, the results were acquired. The results demonstrate that the value of AVE was greater than value of SC for every variable pair that measures different sub-concepts, and that indicated that all scales had discriminant validity.

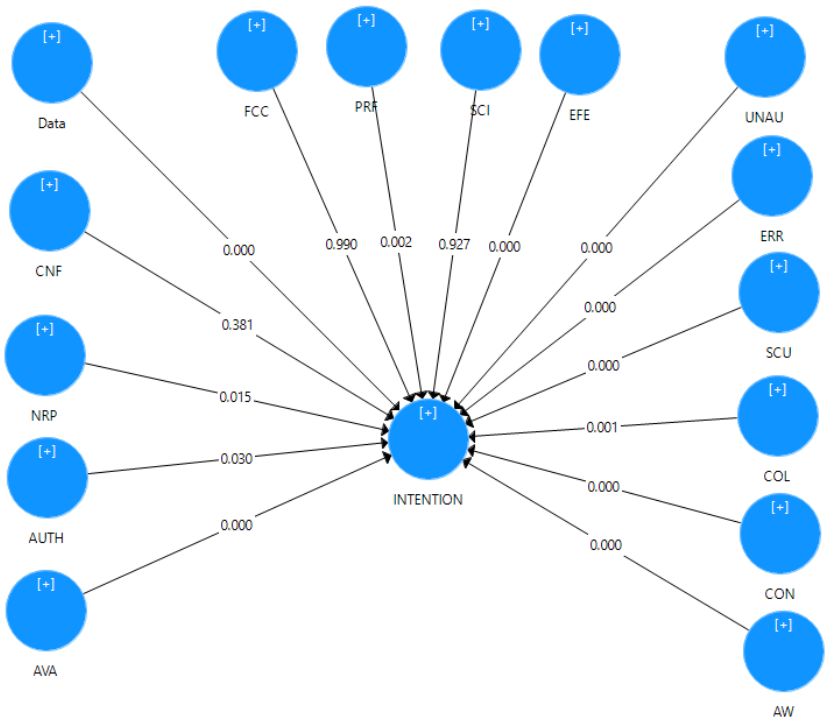

Fig. 2. Structural model assessment

4.3 Structural model assessment

Once the measurement model confirmation has been achieved, evaluation of the structure model is the next step. The structure model describes the causal relations that exist between various constructs (moderating, independent and dependent variables and control) for the testing of the formulated study hypotheses. It was shown by(Hair Jr et al., 2021)that path analysis (through use of one-tail testing) including standard error, beta coefficient, p-value, t-value, R2, Q2 and f2 are all important criterion for the assessment of the structural model within PLS-SEM and were reported and used. Meanwhile, it was argued by Henseler that the index of GoF (goodness-of-fit) was not suitable for the validation of the model within PLS using simulated data since it is unable to separate invalid models from valid ones; as such, it was not reported within this study(Henseler et al., 2014). There was development of the hypotheses within this research so that the research questions could be answered. For the testing of hypotheses, there was examination of statistical significance parameter estimates along with coefficient

values by using a method of bootstrapping that was based upon PLS-SEM(Hair Jr et al., 2021). There was utilization of the method of bootstrapping with 1000 (345 case data; 0.05, two-tailed) bias-corrected intervals for confidence and bootstrap re-sampling for examination of path coefficient significance (Ramayah et al., 2017). The t-value related to the test (one-tailed) have to be equal with or higher than 1.96 with a significance level of 5%.

Table 4
Direct effect

Path	Original sample	Sample mean	Standard deviation	T Statistics	P Values
AUTH → INTENTION	0.058	0.056	0.027	2.179	**0.030**
AVA → INTENTION	0.236	0.236	0.028	8.413	**0.000**
AW → INTENTION	-0.226	-0.227	0.028	8.066	**0.000**
CNF → INTENTION	0.024	0.025	0.027	0.876	**0.381**
COL → INTENTION	-0.097	-0.097	0.030	3.222	**0.001**
CON → INTENTION	-0.222	-0.219	0.034	6.556	**0.000**
Data → INTENTION	0.208	0.207	0.031	6.789	**0.000**
EFE → INTENTION	0.143	0.144	0.027	5.317	**0.000**
ERR → INTENTION	-0.163	-0.164	0.031	5.264	**0.000**
FCC → INTENTION	0.000	-0.002	0.029	0.012	**0.990**
NRP → INTENTION	0.059	0.058	0.024	2.452	**0.015**
PRF → INTENTION	0.081	0.084	0.026	3.119	**0.002**
SCI → INTENTION	-0.003	-0.002	0.028	0.092	**0.927**
SCU → INTENTION	-0.145	-0.143	0.026	5.568	**0.000**
UNAU → INTENTION	-0.138	-0.138	0.031	4.411	**0.000**

It is shown by results contained within Table 4 and by Fig. 4 that a positive, significant relationship exists between non-repudiation, data integrity, availability, authentication, effort expectancy and performance expectancy and the behavioral intention of using IoMT. Hence, there is support for those hypotheses. Furthermore, it is shown by the figure that a negative, significant relationship exists between errors, unauthorized access, collection, secondary use control and awareness with the behavioral intention of using IoMT. As such, there is support for the hypotheses; however, there is no support for social influence, facilitating conditions and confidentiality.

5. Discussion

5.1 Individual factors

With regard to direct effects, it was found that 62.5% of variance of the behavioral intention related to the model was explained by this finding. The contributors that are most important that have significant impact upon behavioral intentions have been found to be efforts to affect the performance expectancy and effort expectancy. Thus, there is support for H1.a and for H1.b(Keselman et al., 2008); this suggests that users that have better conditions for using e-health technologies do tend to favour the adoption of e-health services. Similar results have been reported with regard to effort expectancy having an impact upon system usage; that is, a significant and positive effect is exerted by effort expectancy upon intention for using systems of clinical decision support(Chang et al., 2007), systems for healthcare information(Pai & Huang, 2011), and systems for adverse event reporting(Wu et al., 2008). Also, it has been found that performance expectancy in Taiwan more strongly impacts on behavioral intention for use when compared to expectancy (Wu et al., 2007). It was found in (Mun et al., 2006). that perceived usefulness impacted on behavioral intention for using PDAs amongst physicians within the US. It was also found within (Pai & Huang, 2011). that perceived usefulness exerts an effect that is direct and positive upon intention to use. There is no support for H1.c and for H1. d, however, by social influence and facilitating conditions. Social influence and facilitating conditions have no effect of significance upon behavioral intent, as was shown by other related studies concerning the acceptance and use of technology (Venkatesh & Zhang, 2010).

5.2 Security factors

The five security dimensions are confidentiality, data integrity, non-repudiation, availability and authentication. The protection of personal information can be considered a driving force that is strong for the development of security policies. There is a need for healthcare organizations to give consideration to the assurance and analysis of policies for security in responding to particular issues and in putting forward policies for the protection of medical data. The research outcomes show that the integrity of data has a relationship to the acceptance and use of IoMT, and that supports H3a. Similar results have been reported wherein connection between intent and completeness had significance ($\beta = 0.365$)(Zendehdel et al., 2011). It has also been presented that a rise in use for data integrity intentions happens when reliable and accurate patient data is provided by a system (Ho & Chau, 2013). Lead healthcare professionals utilize the system as well as improving their work quality and reducing errors in medication. There is support for H3c; no one is able to refuse to send or receive records. It has been shown that a significant positive effect is exerted by non-repudiation on the user's intention (Eslami et al., 2014). There is support for H3d. This has similarity to (Tassabehji & Kamala, 2009), with evaluation of possible employment of biometric

authentication within b-banking (online banking) as a way by which adoption and use of it can be improved; it was found that the perceptions that users had of biometric authentication had a positive impact upon their attitudes and intentions for using b-banking. There is support for H3e, with similarity to (Vasileiadis, 2014) according to which data availability has a positive impact on intention in individuals for using m-commerce. Ensuring e-service security involves consideration for numerous issues of security, including availability (Taherdoost et al., 2014). The current study, however, finds confidentiality to be unrelated to the acceptance and use of IoMT. Thus, there is no support for H3.b; this has similarity with results acquired in (Pousttchi & Wiedemann, 2007) which showed confidentiality to not be exerting an influence upon intention to use.

5.3 The IPC model

The IPC model consists of error, awareness, control, authorization, secondary use and collection. Overall, the acceptance and use of IoMT are associated negatively with concerns over privacy. As such, this is supported for H2a, H2b, H2c, H2d, H2e and H2f. Negative associations between acceptance and use of IoMT and IPC show that there is a trend for privacy concerns amongst users of IoMT. So, high levels of concern over privacy lead to low levels of use and acceptance of medical systems amongst users. Further, it has been proved that concerns over privacy have a negative, direct effect upon behavioral intention within e-commerce (Dinev & Hart 2005). It was verified that privacy concerns impact negatively upon intention to use services that were location-based (H. Xu & Teo, 2004). Previous studies also found a relationship existing between secondary use, collection, control, unauthorization, error and awareness with the intention for use within an electronic system context (Enaizan et al., 2020; Eneizan et al., 2019).

6. Limitations

Research to date has primarily focused on the structural aspects of IoMT, limiting the generalizability of findings to specific populations from which samples were drawn. Consequently, such studies may not fully capture actual user behavior in real-world contexts. In addition, the geographical distribution within Jordan may significantly influence IoMT adoption, as behavioral patterns, technological awareness, and access to infrastructure can vary across regions, potentially affecting the consistency of results. Moreover, while survey-based approaches are effective for collecting quantitative data, they may lack the depth required to explore complex issues, user perceptions, and contextual factors influencing IoMT adoption.

Furthermore, the relatively limited sample size used in the current research restricts the representativeness of the findings and limits the inclusion of diverse perspectives relevant to the research problem. This constraint may reduce the statistical power of the analysis and affect the robustness of the conclusions. The study also did not sufficiently account for other influential variables, such as cultural factors, digital literacy levels, organizational readiness, and technological infrastructure, which may play a critical role in shaping user acceptance.

Another limitation of the study did not fully address emerging concerns related to data privacy, cybersecurity risks, and regulatory frameworks, which are increasingly critical in the context of IoMT adoption.

7. Potential future directions for research

7.1 Potential Future Research Directions

This study primarily focused on IoMT users and was limited to a relatively small number of empirical investigations. Future research should aim to employ larger, more heterogeneous samples across multiple healthcare contexts to enhance external validity and generalizability.

In addition, future studies should extend beyond end-users to include other critical stakeholders within the IoMT ecosystem, such as healthcare managers, policymakers, IT specialists, system developers, and regulatory bodies. Examining these groups would enable a more holistic understanding of organizational readiness, governance structures, and strategic decision-making processes influencing IoMT adoption. Moreover, there is a need for pre-implementation and readiness-based research that explores perceptions, resistance factors, and risk assessments prior to IoMT deployment. Longitudinal studies are also highly recommended to capture dynamic changes in user acceptance, trust, system usage, and performance outcomes over time, thereby addressing the limitations of cross-sectional designs.

Future research should also focus on extending and refining theoretical frameworks, such as UTAUT, by incorporating context-specific constructs including trust, perceived risk, data security, privacy concerns, ethical considerations, and regulatory compliance. Additionally, examining mediating and moderating variables—such as digital literacy, organizational culture, technological infrastructure, and health status—would enhance the explanatory and predictive power of existing models. Cross-cultural and cross-national comparative studies are also essential to investigate how socio-cultural, economic, and institutional differences influence IoMT adoption.

Another promising direction involves evaluating the long-term impacts of IoMT on healthcare quality, patient outcomes, cost efficiency, and sustainability. This includes assessing issues related to system scalability, interoperability between platforms, and the ethical implications of continuous health monitoring.

Finally, experimental and design-oriented research approaches (e.g., design science research) could be employed to develop, test, and validate innovative IoMT solutions, providing practical contributions alongside theoretical advancements.

8. Conclusion

This current research has analyzed the dimensions of security, privacy along with individual elements that impact upon the acceptance and usage of IoMT. This current study has been successful in achieving the objective of the research investigating factors that impact upon the acceptance and usage of IoMT within Jordan as well as in the development of a model as proposed. UTAUT was extended by the current research in order to attain the objectives, with it being considered that the known UTAUT was validated by significant, reliable analysis. Results achieved through use of the UTAUT could be helpful numerical findings and so could serve as a basis for decision-makers and justification for their decisions. The research outcomes may also contribute towards the knowledge of the developers of IoMT applications through enhancing applications of IoMT where weaknesses have been highlighted. Also, collected data has been presented within the findings from users by way of the research models. There has to be analysis of these models in order to demonstrate the impact that factors have upon acceptance and usage of IoMT within those medical organizations. Furthermore, outcomes contribute to the IoMT field, particularly with regard to acceptance and usage related to stored data records within medical organizations. Also, the suggestion is made that the features of user adaptation that are acknowledged in the IoMT and utilized, including privacy, security and the individual factors, and these findings can be re-used to assist in extension of UTAUT development.

References

Abildgaard, J. S., Saksvik, P. Ø., & Nielsen, K. (2016). How to measure the intervention process: An assessment of qualitative and quantitative approaches to data collection in the process evaluation of organizational interventions. *Frontiers in Psychology, 7,* 1380.

Adil, M., Khan, M. K., Kumar, N., Attique, M., Farouk, A., Guizani, M., & Jin, Z. (2024). Healthcare Internet of Things: Security threats, challenges, and future research directions. *IEEE Internet of Things Journal, 11*(11), 19046-19069.

Alazzam, M. B., Basari, H., Samad, A. B. D., Sibghatullah, A. S., Doheir, M., Yaacob, N. M., & Aris, F. (2015). Physicians' acceptance of electronic health records exchange: An extension of the with UTAUT2 model institutional trust. *Advanced Science Letters, 21*(10), 3248–3252.

Al-Dhaen, F., Hou, J., Rana, N. P., & Weerakkody, V. (2021). Advancing the Understanding of the Role of Responsible AI in the Continued Use of IoMT in Healthcare. Information Systems Frontiers, 1–20.

Alharbi, A. A., Alharby, M., & Hanandeh, A. A. (2025). Securing healthcare systems and optimizing data analytics through IoMT threat detection. *AIMS Mathematics, 10*(11), 25274–25306. https://doi.org/10.3934/math.20251119

Almotiri, S. H. (2025). AI driven IOMT security framework for advanced malware and ransomware detection in SDN. *Journal of Cloud Computing, 14*(1), 19.

Alotaibi, S., Alshammari, R., & Alsubaei, F. (2025). Blockchain-based security and privacy solutions for the Internet of Medical Things. *International Journal of Privacy and Confidentiality in Computing.*

Al-Turjman, F., Zahmatkesh, H., & Mostarda, L. (2025). Exploring factors affecting the adoption of IoT in healthcare: A systematic literature review. Healthcare, 13(23), 3157. https://doi.org/10.3390/healthcare13233157

Angst, C. M. (2009). Protect my privacy or support the common-good? Ethical questions about electronic health information exchanges. *Journal of Business Ethics, 90*(2), 169–178.

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly, 33*(2), 339–370.

Ariaeinejad, R., & Archer, N. (2014). Importance of Mobile Technology in Successful Adoption and Sustainability of a Chronic Disease Support System. *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering, 8*, 870–875.

Arning, K., & Ziefle, M. (2009). Different perspectives on technology acceptance: The role of technology type and age. Symposium of the Austrian HCI and Usability Engineering Group, 20–41.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017–1041.

Bhattacherjee, A., & Hikmet, N. (2008). Reconceptualizing organizational support and its effect on information technology usage: Evidence from the health care sector. *Journal of Computer Information Systems, 48*(4), 69–76.

Bhushan, B., Kumar, A., Agarwal, A. K., Kumar, A., Bhattacharya, P., & Kumar, A. (2023). Towards a secure and sustainable internet of medical things (iomt): Requirements, design challenges, security techniques, and future trends. *Sustainability, 15*(7), 6177.

C. Sipior, J., T. Ward, B., & Connolly, R. (2013). Empirically assessing the continued applicability of the IUIPC construct. *Journal of Enterprise Information Management, 26*(6), 661-678.

Caine, K., & Hanania, R. (2013). Patients want granular privacy control over health information in electronic medical records. *Journal of the American Medical Informatics Association, 20*(1), 7–15.

Chang, I.-C., Hwang, H.-G., Hung, W.-F., & Li, Y.-C. (2007). Physicians' acceptance of pharmacokinetics-based clinical decision support systems. *Expert Systems with Applications, 33*(2), 296–303.

Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce, 10*(2), 7–29. https://doi.org/10.2753/JEC1086-4415100201

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems, 22*(3), 295–316.

Dwivedi, Y. K., Rana, N. P., Chen, H., & Williams, M. D. (2011). A Meta-analysis of the Unified Theory of Acceptance and Use of Technology (UTAUT). IFIP International Working Conference on Governance and Sustainability in Information Systems-Managing the Transfer and Diffusion of It, 155–170.

Enaizan, O., Zaidan, A. A., Alwi, N. M., Zaidan, B. B., Alsalem, M. A., Albahri, O. S., & Albahri, A. S. (2020). Electronic medical record systems: Decision support examination framework for individual, security and privacy concerns using multi-perspective analysis. *Health and Technology, 10*(3), 795-822.

Eneizan, B., Mohammed, A. G., Alnoor, A., Alabboodi, A. S., & Enaizan, O. (2019). Customer acceptance of mobile marketing in Jordan: An extended UTAUT2 model with trust and risk factors. *International Journal of Engineering Business Management, 11*, 1847979019889484.

Farooqi, M., & Zafar, S. (2024). Security and privacy challenges in the Internet of Medical Things: A comprehensive review. *Journal of Information Security and Applications, 75,* 103532.

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. Sage Publications Sage CA: Los Angeles, CA.

Gao, L., & Bai, X. (2014). A unified perspective on the factors influencing consumer acceptance of internet of things technology. *Asia Pacific Journal of Marketing and Logistics*.

Gardiyawasam Pussewalage, H. S., & Oleshchuk, V. A. (2016). Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. *International Journal of Information Management, 36*(6), 1161–1173. https://doi.org/10.1016/j.ijinfomgt.2016.07.006

Hair Jr, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2021). A primer on partial least squares structural equation modeling (PLS-SEM). Sage publications.

Hair, J. F., Anderson, R. E., Babin, B. J., & Black, W. C. (2010). Multivariate data analysis: A global perspective (Vol. 7). Pearson Upper Saddle River, NJ.

Hatcher, L., & O'Rourke, N. (2013). A step-by-step approach to using SAS for factor analysis and structural equation modeling. Sas Institute.

Henseler, J., Dijkstra, T. K., Sarstedt, M., Ringle, C. M., Diamantopoulos, A., Straub, D. W., Ketchen Jr, D. J., Hair, J. F., Hult, G. T. M., & Calantone, R. J. (2014). Common beliefs and reality about PLS: Comments on Rönkkö and Evermann (2013). *Organizational Research Methods, 17*(2), 182–209.

Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *Mis Quarterly, 37*(1), 275–298.

Hong, W., Chan, F. K. Y., & Thong, J. Y. L. (2019). Drivers and inhibitors of internet privacy concern: a multidimensional development theory perspective. *Journal of Business Ethics, 168*, 1–26.

Hong, W., Chan, F. K., & Thong, J. Y. (2021). Drivers and inhibitors of internet privacy concern: a multidimensional development theory perspective. *Journal of Business Ethics, 168*(3), 539-564.

Hoque, R., & Sorwar, G. (2017). Understanding factors influencing the adoption of mHealth by the elderly: An extension of the UTAUT model. *International Journal of Medical Informatics, 101*, 75–84.

Jia, M., Wang, L., Guo, Q., Gu, X., & Xiang, W. (2017). A low complexity detection algorithm for fixed up-link SCMA system in mission critical scenario. *IEEE Internet of Things Journal, 5*(5), 3289–3297.

Kamalov, F., Pourghebleh, B., Gheisari, M., Liu, Y., & Moussa, S. (2023). Internet of Medical Things privacy and security: Challenges, solutions, and future trends. *Sustainability, 15*(4), 3317. https://doi.org/10.3390/su15043317

Kasyoka, P., Kimwele, M., & Mbandu Angolo, S. (2020). Certificateless pairing-free authentication scheme for wireless body area network in healthcare management system. *Journal of medical engineering & technology, 44*(1), 12-19.

Keselman, A., Logan, R., Smith, C. A., Leroy, G., & Zeng-Treitler, Q. (2008). Developing informatics tools and strategies for consumer-centered health communication. *Journal of the American Medical Informatics Association, 15*(4), 473–483.

Kijsanayotin, B., Pannarunothai, S., & Speedie, S. M. (2009). Factors influencing health information technology adoption in Thailand's community health centers: Applying the UTAUT model. *International Journal of Medical Informatics, 78*(6), 404–416.

Kim, J., & Park, H.-A. (2012). Development of a health information technology acceptance model using consumers' health behavior intention. *Journal of Medical Internet Research, 14*(5), e133.

Kumar1, B. S., & Sirajuddin, M. (2024). Security issues and intelligent solutions for IOMT-enabled healthcare systems. Handbook of Research on Artificial Intelligence and Soft Computing *Techniques in Personalized Healthcare Services, 91*.

Leguina, A. (2015). A primer on partial least squares structural equation modeling (PLS-SEM). Taylor & Francis.

Long, V. N., & Hoang, N. A. (2017). Development of IoT based lower limb exoskeleton in rehabilitation. *2017 14th International Conference on Ubiquitous Robots and Ambient Intelligence (URAI)*, 824–826.

Malhotra, N. K., Kim, S. S., & Patil, A. (2006). Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research. *Management Science, 52*(12), 1865–1883.

Mansour, N., Rafeh, W., Afram, G., & Zaatari, G. (2019). The Role of Self-Awareness, Augmented Artificial Intelligence and Enhanced Leadership Competencies in Developing Future Academic Physicians. *Middle East Journal of Family Medicine, 17*(10).

Mavrogiorgou, A., Kiourtis, A., Touloupou, M., Kapassa, E., & Kyriazis, D. (2019). Internet of medical things (IoMT): acquiring and transforming data into HL7 FHIR through 5G network slicing. *Emerg. Sci. J, 3*(2), 64-77.

Miladinovic, J., & Hong, X. (2016). A study on factors affecting the behavioral intention to use mobile shopping fashion apps in Sweden.

Mishra, P., & Singh, G. (2023). Internet of medical things healthcare for sustainable smart cities: current status and future prospects. *Applied Sciences, 13*(15), 8869.

Mun, Y. Y., Jackson, J. D., Park, J. S., & Probst, J. C. (2006). Understanding information technology acceptance by individual professionals: Toward an integrative view. *Information & Management, 43*(3), 350–363.

Nakshbandi, G., Moor, C. C., & Wijsenbeek, M. S. (2023). Role of the internet of medical things in care for patients with interstitial lung disease. *Current Opinion in Pulmonary Medicine, 29*(4), 285-292.

Or, C. K. L., & Karsh, B. T. (2009). A Systematic Review of Patient Acceptance of Consumer Health Information Technology. *Journal of the American Medical Informatics Association, 16*(4), 550–560. https://doi.org/10.1197/jamia.M2888

Or, C. K. L., Karsh, B.-T., Severtson, D. J., Burke, L. J., Brown, R. L., & Brennan, P. F. (2011). Factors affecting home care patients' acceptance of a web-based interactive self-management technology. *Journal of the American Medical Informatics Association, 18*(1), 51–59.

Pai, F.-Y., & Huang, K.-I. (2011). Applying the technology acceptance model to the introduction of healthcare information systems. *Technological Forecasting and Social Change, 78*(4), 650–660.

Powell, J., Fitton, R., & Fitton, C. (2006). Sharing electronic health records: the patient view. *Journal of Innovation in Health Informatics, 14*(1), 55–57.

Pussewalage, H. S. G., & Oleshchuk, V. A. (2016). Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. *International Journal of Information Management, 36*(6), 1161-1173.

Rajab, R. M., Abuhmida, M., Wilson, I. D., & Ward, R. P. (2024). A review of IoMT security and privacy related frameworks. In Proceedings of the European Conference on Cyber Warfare and Security (ECCWS).

Ramayah, T., Yeap, J. A., Ahmad, N. H., Halim, H. A., & Rahman, S. A. (2017). Testing a confirmatory model of Facebook usage in SmartPLS using consistent PLS. *International Journal of Business and innovation, 3*(2), 1-14.

Rasool, R. U. (2022). Security and privacy of Internet of Medical Things. *Journal of Network and Computer Applications, 198*, 103287. https://doi.org/10.1016/j.jnca.2022.103287

Saarikko, T., Westergren, U. H., & Blomquist, T. (2017). The Internet of Things: Are you ready for what's coming? *Business Horizons, 60*(5), 667–676.

Sadhu, S., Yanambaka, V. P., Abdelgawad, A., & Yelamarthi, K. (2022). Prospect of Internet of Medical Things: Security challenges and cryptographic solutions. *IEEE Access, 10*, 56045–56059. https://doi.org/10.1109/ACCESS.2022.3179204

Slade, E. L., Williams, M. D., & Dwivedi, Y. K. (2013). Mobile payment adoption: Classification and review of the extant literature. *The Marketing Review, 13*(2), 167–190.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167–196.

Somasundaram, R., & Thirugnanam, M. (2020). Review of security challenges in healthcare internet of things. *Wireless Networks*, 1–7.

Stern, A. D., Gordon, W. J., Landman, A. B., & Kramer, D. B. (2019). Cybersecurity features of digital medical devices: an analysis of FDA product summaries. *BMJ Open, 9*(6), e025374.

Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and privacy in the medical internet of things: a review. Security and Communication Networks, 2018.

Sun, Y., Lo, F. P.-W., & Lo, B. (2019). Security and privacy for the internet of medical things enabled healthcare systems: A survey. *IEEE Access, 7,* 183339–183355.

Taherdoost, H., Sahibuddin, S., & Jalaliyoon, N. (2014, March). Perceived barriers and benefits of Web based services. In *2014 International Conference on Computational Science and Computational Intelligence (Vol. 2, pp. 34-39). IEEE.*

Taiwo, A. A., & Downe, A. G. (2013). The theory of user acceptance and use of technology (UTAUT): A meta-analytic review of empirical findings. *Journal of Theoretical & Applied Information Technology, 49*(1).

Tassabehji, R., & Kamala, M. A. (2009, December). Improving e-banking security with biometrics: Modelling user attitudes and acceptance. *In 2009 3rd International Conference on New Technologies, Mobility and Security (pp. 1-6). IEEE.*

Taylor, K., Sanghera, A., Steedman, M., & Thaxter, M. (2018). Medtech and the Internet of Medical Things: How connected medical devices are transforming health care. Deloitte.

Vaiyapuri, T., Binbusayyis, A., & Varadarajan, V. (2021). Security, Privacy and Trust in IoMT Enabled Smart Healthcare System: A Systematic Review of Current and Future Trends. I*nternational Journal of Advanced Computer Science and Applications, 12*, 731–737.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425–478.

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarterly, 36*(1), 157–178.

Vyas, A., & Pal, S. (2020). Preventing security and privacy attacks in WBANs. In Handbook of computer networks and cyber security (pp. 201–225). Springer.

Williams, P. A. H., & McCauley, V. (2016). Always connected: The security challenges of the healthcare Internet of Things. 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), 30–35.

Wu, J.-H., Shen, W.-S., Lin, L.-M., Greenes, R. A., & Bates, D. W. (2008). Testing the technology acceptance model for evaluating healthcare professionals' intention to use an adverse event reporting system. *International Journal for Quality in Health Care, 20*(2), 123–129.

Xu, B., Da Xu, L., Cai, H., Xie, C., Hu, J., & Bu, F. (2014). Ubiquitous data accessing method in IoT-based information system for emergency medical services. *IEEE Transactions on Industrial Informatics, 10*(2), 1578–1586.

Xu, H., & Teo, H.-H. (2004). Alleviating consumers' privacy concerns in location-based services: a psychological control perspective. ICIS 2004 Proceedings, 64.

Zendehdel, M., Paim, L., Bojei, J., & Osman, S. (2011). The effects of trust on online Malaysian students buying behavior. Australian *Journal of Basic and Applied Sciences, 5*(12), 1125–1132.

Zhanyou, W., Dongmei, H., & Yaopei, Z. (2020). How to improve users' intentions to continued usage of shared bicycles: A mixed method approach. *PLoS One, 15*(2), e0229458.

© 2026 by the authors; licensee Growing Science, Canada. This is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC, BY) license (http://creativecommons.org/licenses/by/4.0/).