FACTORS AFFECTING RFID SUBCUTANEOUS MICROCHIPS USAGE

Svetlana Čičević[1],
Andreja Samčović[1], *,
Magdalena Dragović[2]

[1]Faculty of Transport and Traffic Engineering,
University of Belgrade,
Belgrade, Serbia
[2]Faculty of Civil Engineering,
University of Belgrade,
Belgrade, Serbia

Abstract:

Microchips are used for many years for different purposes. Nevertheless, recently applications of radio frequency identification technology have been progressed tremendously with the potential to permeate throughout society as valuable tool for enabling automatic identification and management. However, they are perceived as threats at several levels that impede its implementation. Most of the research discusses the adoption of Radio Frequency Identification (RFID) devices from the provider's point of view. Thus, it would be of interest to examine the factors of RFID subcutaneous microchip (RFID-SM) usage, adoption and diffusion by individuals from various perspectives, particularly in developing countries. Knowledge upon the factors that drive RFID adoption is a crucial step in creating the policies required for its successful implementation. This quantitative, descriptive study investigated whether young people in Serbia would be willing to use subcutaneous microchip. Preliminary findings indicate that positive attitudes prevail for the perceived usefulness and ease of use, while suspicions of confidentiality and privacy are strong, and what is most surprising none of the respondents showed willingness to use microchip implants for everyday home activities. Since the process of individual users' acceptance of technology is very complex, the full range of variables should be investigated from broader perspective.

Keywords:

subcutaneous microchip, implant, acceptance of technology, adoption, privacy concerns.

1. INTRODUCTION

RFID is a wireless proximity communication method, which can be used as a standalone technology or it can be complementary to existing technologies [1]. Radio Frequency Identification (RFID) involves systems and technologies that transmit and automatically identify objects and people based on radio waves [2]. RFID is one of the key technologies that build up the Internet of Things, a pervasive network environment. RFID plays a fundamental role in the so-called digital factory or 4.0 Industry, aiming to increase the level of automatization of industrial processes. For many industries, RFID is not only a new alternative to existing tracking methods but is also a solution for a range of previously cost-prohibitive innovations in internal control and supply chain coordination [3]. RFID

Correspondence:
Andreja Samčović

e-mail:
andrej@sf.bg.ac.rs

DOI: 10.15308/Sinteza-2019-235-243

usually consists of tags, readers and middleware. RFID operates similarly on a barcode that stores serial numbers for identifying products and related information on a microchip [4]. However, unlike a barcode, RFID offers the advantage of allowing the tracking without the line of sight. Ultra high-frequency (UHF) RFID technology is selected over the most extended near-field communication (NFC) and high-frequency (HF) RFID technology to minimize hardware infrastructure. In particular, UHF RFID also makes the coverage/reading area conformation easier by using different kinds of antennas. Information is stored in a database, which is accessed from end-user mobile devices (tablets, smartphones) where the position and status of the assets to be tracked are displayed [5]. This allows for better time management and better human resource utilization.

This paper is structured as follows. After the introduction some important applications of considered RFID technology are mentioned and described. The Technology Acceptance Model is presented in the next section, because we used that model in our study. The corresponding methodology and obtained results are shown in the following section. Before the conclusion we discussed our results.

Applications of RFID technology

Embedded radio-frequency identification, sensor technologies, biomedical devices and a new breed of nanotechnologies are now being commercialized within a variety of contexts and use cases. RFID is present in a wide variety of applications. These applications include access control procedures, supply management, and protection against theft. There is a rapid increase in the use of RFID systems in the transport sector (toll collection), as well as in supply chain management infrastructures [6], logistic, automotive industry, livestock production [7], food production and public sector [8]. RFID has potential applications across a wide range of sectors and activities such as defense, agriculture, culture and other domains. Both industry and governments are strong promoters of RFID technology.

RFID microchip is used in shops, passports, proximity cards, ignition keys, contactless credit-cards, smart bracelets, smart finger rings, smart watches, etc. [9]. Additionally, RFID technology is starting to penetrate the medical and healthcare sector (in palliative care, home care and preventive care applications, including telehomecare applications) [10], enabling locating elderly or children in the case of their uncontrolled departure from home (Alzheimer's disease, kidnapping). RFID system is also used in hospitals for tracing the distribution of medicines, equipment, healing procedures, patient movements, but in these cases the RFID labels were attached or fixed to observed item [11]. In the year 2012 first results of wirelessly controlled drug delivery microchip testing were published [12]. The use of microchips also brings some risks such as safety of device, privacy of patients' records and coercion to consent to the implantation of the devices. Additional, there is a social and ethical risk.

However, like any wireless technology, including cell phones, wireless networks and Bluetooth connections, RFID devices provide remote readability. In theory, any technology that relies on radio frequency (RF) is inherently insecure. As a result, businesses and legislative bodies continuously seek ways to understand and lock down wireless security issues.

There are a massive number of devices with sensors that track and record different aspects of your life, with the goal of aggregating the data for the user to peruse (Fig 1). There are, of course, drawbacks to measuring multiple bodily functions with different devices. It has been pointed out that some devices are occasionally cumbersome, can interfere with everyday tasks, and even make the users even more aware of their bodily limitations - all of which can cause frustrations [13,14,15,16]. Natural user interfaces (NUI) is another field which shows promising relevance to the studies in quantified self [17] by transferring some of the functionality from the devices themselves onto in-home surfaces.

Some issues arise with implanting people with microchips though. Issues include, being able to track a person's previous and current location, their purchasing habits, legal and privacy concerns, as well as hacking their personal and financial information. There are potential health problems as well. For example, non-ionizing radiation from microwave radio frequency and magnetic fields could cause various health issues. A potential benefit could include storing a person's complete medical history, or at the bare minimal the drugs that they are taking or are allergic to [18]. Some health issues include adverse tissue reaction, migration of implanted transponder, electromagnetic interference, electrical hazards, and magnetic resonance imaging incompatibility [19]. There are legal and legislative issues as well dealing with RFID technology. Even though the scanner that reads the sensor has to be close to the body to read the chip, there still is the possibility of identity theft. Parts of the problem are security, confidentiality and data integrity. There is a need for more laws dealing with RFID to protect privacy.

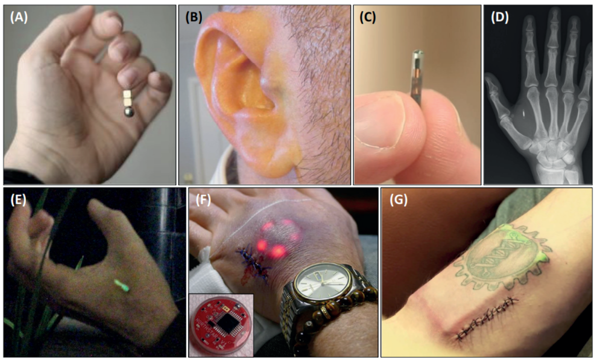


Fig. 1. Subdermal implants: (A) A neodymium magnet in a finger. (B) Magnets in the tragus of an ear. (C) A RFID tag. (D) RFID tags implanted in the webbing between the metacarpal bones of the index finger and thumb, positioned parallel to the index metacarpal. (E) Tritium lighting implants. (F) LEDs in hand. (G) Continual temperature sensor in forearm. Source: [20]

Concern is growing that RFID systems have the potential to be used as tools for surveillance, which could very much undermine the dignity and autonomy of employees. Recent studies have shown that the RFID technology is safe enough to be used for personal identification and some attempts were made to use RFID subcutaneous microchip implants (RFID-SM) [21,22,23]. The number of people willing to get chipped has increased since the technology's commercial arrival in 2002, despite the fact that adoption rates have been very low. Nevertheless, some researchers still explore the potential negative impact of enforced micro-chipping [24], while others look for highly positive effects of RFID implants.

2. TECHNOLOGY ACCEPTANCE MODEL (TAM)

Since its introduction almost three decades ago, by [25,26], TAM has become one of the most frequently used models used to explain behavioral intention, in general, and technology system acceptance, in particular [27].

Of the suite of theories that explain technology acceptance, TAM appears the most popular. It explains IT usage as a function of a four-stage process:

- External variables (user training) influences use beliefs about using the system;
- User beliefs influence their attitudes about using a system;
- User attitudes influence their intentions to use a system;
- The user intentions determine level of usage of the system [28].

It provides the framework to measure users' perceptions and intentions to use technology within and across organizations. Through research TAM has been empirically proven to be a robust model for understanding end-user adoption of technology and for examining the acceptance of new and developing technology by users with different characteristics in different organizations. The flexibility of TAM to be extended and modified to take into account other relevant factors makes it a powerful framework [29].

TAM comprises core variables of user motivation (i.e., perceived ease of use, perceived usefulness, and attitudes toward technology) and outcome variables (i.e., behavioral intentions, technology use). Of these variables, perceived usefulness (PU) and perceived ease of use (PEU) are considered key variables that directly or indirectly explain the outcomes [27]. Overall, perceived ease of use and perceived usefulness, the most important factors in the TAM, refer to the degrees to which a person believes that using technology would be free from effort (PEU) and that using technology would enhance their job or task performance (PU).

In the Technology Acceptance Model 2 (TAM 2) [30], TAM is extended by including additional key determinants of perceived usefulness and usage intention constructs. They aimed to determine the antecedents of external factors that affect perceived usefulness. These external factors are divided into two groups as social influence processes (subjective norm, voluntariness and imagination) and cognitive instrumental processes (job relevance, output quality, result demonstrability and perceived ease of use). Perceived ease of use and perceived usefulness positively affect the attitudes toward an information system; and further, positively affect the individuals' intentions to use and the acceptance of the information system. In addition, perceived ease of use positively affects the perceived usefulness, and both of perceived ease of use and perceived usefulness are influenced by external variable. Shroff et al. [31] reported that by manipulating these two determinants, system developers can have better control over users' beliefs about the system and so can predict their behavioral intention and actual usage of the system. Some authors found significant direct relations between perceived usefulness and behavioral intention [32,33], others did not [34,35].

A variety of TAM models exist, with or without external variables, with or without direct effects of certain variables on outcome variables. In the literature, many studies mentioned the relationship among trust, perceived risks and behavioral intention [36]. The perception of trust in any relationship will elevate the perception of security. Generally, people feel unsafe or insecure in unpredictable situations. Trust plays a crucial role in reducing consumer perception of the risk of vulnerability [37]. In other words, people will feel safer about any particular product or transaction if they trust their partners or providers [38].

Despite its prominence, the existing body of research does not draw a clear picture about specific relations within the TAM. Whereas some studies confirmed the hypothesized relations fully, others did not [39,40]. This finding is further substantiated by significant variation of TAM relations across studies and samples from multiple occupations and domains, thus consequently calls for a systematic synthesis [41,42]. Finally, Ajibade [43] argues that the TAM model was more appropriate for individual use and acceptance of technology rather than in a corporate or institutional application that requires integration of information technology.

Studies from psychology research have widely stated that an individual's demographic and personality characteristics are important predictors, having moderating effects on Information Technology (IT) adoption [6,44]. IT adoption researches have confirmed the importance of the role of users when it comes to adopting new information systems [45]. Younger people are more prone to adopt new technologies. Bearing in mind the above mentioned, our study was conducted in order to examine the readiness to adopt RFID-SM by focusing on the individual users' point of view. The subjects in this research were undergraduate students because they represent the largest group of potential RFID-SM users.

3. METHODOLOGY

Data collection

The study was performed as a web survey used to collect data about attitudes toward RFID-SM usage in Serbia. Online survey was conducted using a convenience sample of 100 respondents. The participants were students enrolled in Traffic Psychology courses offered at the Faculty of Transport and Traffic Engineering. The sample consists of 56% of women and 44% of men. The average age of the respondents is 24.5.

Measures

Questionnaire on adoption of RFID systems and subcutaneous microchips were used. The students' attitudes towards various aspects of RFID-SM usage were investigated. The questionnaire items were proposed based on the literature review, relying primarily on extended Technology Acceptance Model (TAM). In addition to the three original components of TAM (Perceived Usefulness, Perceived Ease of Use, and Behavioral Intentions to Use), two external variables (Health Concerns and Perceived Trust) were also included. PU (Perceived Usefulness) has seven items which are in accordance with items proposed by [46] in the original TAM model. Five of them were adopted from [1], and two additional items on storing information about organ donation and a general statement on saving lives in different medical conditions were added from [47].

PEU (Perceived Ease of Use) and PT (Perceived Trust) items were adopted based on [48] and [49], respectively. PT (Perceived Trust) refers to an individual's trust that the state, banks and healthcare systems will be able to ensure security and protection of human rights in the fields of identification, tracking and archiving of personal data, financial transactions, and patient data on treatments and organ donation. Items composing HC (Health Concern) construct which possible threats of RFID-SM usage were found based on extensive literature review of medical research papers [46,50,51]. The component HC refers to four possible threats of RFID-SM usage: the possibility of movement in the body, effect on emotional behavior, health threats due to possible allergies, and health threats because of impacts on the nervous system. The items of output variable BIU (Behavioral Intentions to Use) are adapted from [45]. BIU reflects four different possible types of the RFID-SM usage (healthcare purposes, for identification purposes, for shopping and payment, and for everyday home usage). BIU items were measured as dichotomous variables. Furthermore, manifest variable PP (Painful Procedure) was included.

Items of HC, PT, and PEU, as well as the last item of PU, were measured on a 5-point Likert-type scale of agreement ("strongly disagree" to "strongly agree"), while the first six items of PU were measured on a 5-point scale of acceptability ("very bad idea" to "very good idea"), while the items of BIU were measured as dichotomous variable (yes/no).

4. RESULTS

Descriptive statistics were calculated for 23 measured items as well as for five dimensions. The means of items are measured on the 5-point scale ranged from 1.72 to 5.00. Standard deviations of all items are in the range from 0.32 to 1.68, indicating a fairly narrow spread of scores around the means. The means of three components are 4.2 for PU, 4.58 for PEU, and 4.88 for PP, which indicate that although the majority of respondents considered the implantation procedure to be very painful (Fig. 2), their estimates for perceived usefulness and perceived ease of use were very high, in other words, they rated RFID microchips usage as effortless and enhancing. The mean of HC is equal to 3.21, which indicates that the respondents are not quite sure if the consequences of microchips usage could have harmful effects on their health. The mean of PT is equal to 2.83, which indicates that the average perceived trust on security issues assured by state, banks, and healthcare system is rather low (Fig. 3).

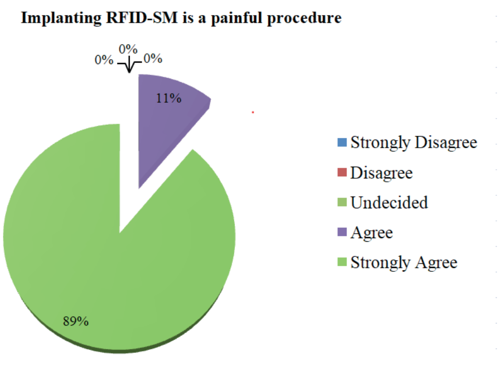


Fig. 2. Attitude toward implantation procedure

On average, respondents agree mostly with the statement that subcutaneous microchips cannot be stolen (high-security protection). Also, they are convinced that subcutaneous microchips have very high life-saving potential (M = 4.89). Likewise, they show a high degree of agreement with the statement that subcutaneous microchips can integrate multiple functions at the same time, as well as for storing medical information for accident or emergency situations (M = 4.78, for both statements). Students highly rated the feature that microchips are always available (M = 4.61). The features of monitoring the health of the user (M = 4.55) and for warning about potential health problems or complications (M = 4.27) received high ratings, too.

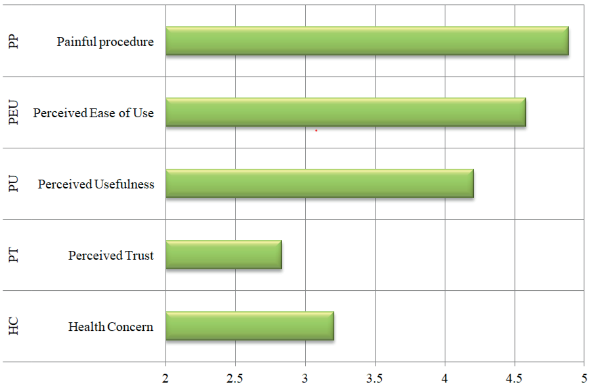
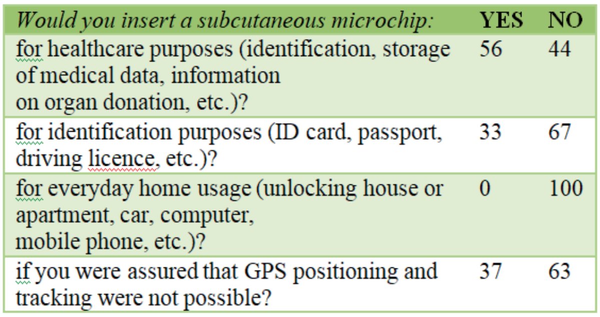


Fig. 3. Readiness to adopt RFID subcutaneous microchip

If we examine the four items of HC closely, we can see that respondents are worried due to treats of possible allergies (M = 3.78), and an impact on emotional behavior (M = 3.27). On the other hand, they are less concerned due to possibility of microchip movements in their bodies (M = 2.94) and with respect to the effects on the nervous system (M = 2.78). The respondents declare that they do not trust that the banks (M = 1.72), the state (M = 3.00) and healthcare system (M = 3.78) can provide the appropriate level of safety and security related to RFID-SM usage (Fig. 1). Obviously, the banks deserve the lowest level of trust among the respondents. When it comes to individual's intention of the RFID usage and a willingness to adopt the RFID microchip implants, the highest proportion of the respondents would primarily consider using the RFID-SM for healthcare purposes (56%), rather than for personal identification (33%).

If they could be assured that Global Positioning System (GPS) and tracking were not possible 37% would be ready to use RFID microchip implants. What is very interesting and surprising is that none of the respondents would use microchip implants for everyday home tasks (unlocking house or apartment, car, computer, mobile phone, etc.) (Table I).

Table 1. Behavioral Intentions to Use RFID subcutaneous microchip



Would you insert a subcutaneous microchip:	YES	NO
for healthcare purposes (identification, storage of medical data, information on organ donation, etc.)?	56	44
for identification purposes (ID card, passport, driving licence, etc.)?	33	67
for everyday home usage (unlocking house or apartment, car, computer, mobile phone, etc.)?	0	100
if you were assured that GPS positioning and tracking were not possible?	37	63

5. DISCUSSION AND CONCLUSIONS

The aim of the study was to research the attitudes of potential RFID-SM users. Nevertheless, concerns among potential users about privacy issues, personal data security, and implants' impact on health are evident. Our study indicates that a lack of trust presents a significant obstacle for adoption. Obviously, more research must be done to prove the reliability and harmlessness of RFIDSM and its technical possibilities.

This article presents preliminary and partial results of the survey conducted in Serbia, therefore, further research needs to include the results of the surveys gathered in other European countries to establish whether similarities in the attitudes toward RFID-SM adoption exists.

Currently, the only comparison can be done with the findings of the [23,47]. While similar values were obtained for HC and PT dimensions, the PEU and PU dimensions in our sample show much higher mean values. These differences can be attributed to age differences between the two samples. Thus, the sample that includes only undergraduate students limits the generalization of the study. However, a student sample is the appropriate context because students represent an important segment of future users. The new research design should take special care to include more representative sample of older people, who have no internet access or experience with new technologies.

According to [52,53] TAM has proven to be a useful theoretical model in helping to understand and explain usage behavior in technology acceptance.

Though, limitations of research that rely on TAM to date still remain the involvement of students and self-reports. They revealed that although TAM is useful, it has to be integrated into a broader model which would include variables related to both human and social change processes.

Nowadays, there are various technologies which can be used by any individual without having any technology competence. Although these devices minimize technology competencies, the variables predicting acceptance of people for using these devices may also show variety. In the future, technology will continue to change and as users we will also continue to adapt ourselves and learn how to cope with the new features of upcoming technologies. During this process, investigating personal variables that affect this adaptation process will be still important. Therefore, the study of technological innovation acceptance requires psychological models and theories to explain and rationalize whether users benefit from new devices [29].

The instrument used in the current research to assess students' opinions is based on the self reported design. Another opportunity for future work is to extend the survey to address objective measures of actual system usage.

There is ample concern, even among engineers, that the RFID chip's unique numerical code, though encrypted, may be discovered or copied, placing the owner at risk of identity theft, which could result in the fabricated identity being almost undetectable [24]. Uberveillance (or the omnipresent surveillance) can be, to a certain extent, circumvented with the development of specified social, legal and engineering advances.

As Li [55] suggests in order to utilize the full advantages of RFID and at the same time to keep the threats as small as possible, it will be a matter of implementing the principles of modern data protection laws, data economy and the most rapid possible anonymization of personal referenced data in RFID systems early in the design process and in market introduction.

ACKNOWLEDGMENT

This paper is partially supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia (Projects No. 32025, 32048, 36022, and 36006).

REFERENCES

[1] C. M. Roberts, "Radio Frequency Identification (RFID)", Computers & Security, Vol. 25, No. 1, pp. 18-26, 2006. http://dx.doi.org/10.1016/j.cose.2005.12.003

[2] Y.L. Chong, A. Liu, M.J. Luo, & O. Keng-Boon, "Predicting RFID adoption in healthcare supply chain from the perspectives of users", International Journal of Production Economics, Vol. 159, pp. 66–75, 2015. http://doi.org/10.1016/j.ijpe.2014.09.034

[3] M.T. Lu et al., "Improving RFID adoption in Taiwan's healthcare industry based on a DEMATEL technique with a hybrid MCDM model", Decision Support Systems, Vol. 56, pp. 259-269. 2013. doi: 10.1016/j.dss.2013.06.006

[4] E. Ngai, K.K. Moon, F.J. Riggins, & C.Y. Yi, "RFID research: An academic literature review (1995–2005) and future research directions", International Journal of Production Economics, Vol. 11, No. 2, pp. 510–520, 2007. doi:10.1016/j.ijpe.2007.05.004

[5] Á.Y. López Y, J. Franssen, G. Álvarez Narciandi, J. Pagnozzi, I. González-Pinto Arrillaga, F. Las-Heras Andrés, "RFID Technology for Management and Tracking: e-Health Applications", Sensors (Basel), Vol. 18, No. 8, 2663, 2018. doi:10.3390/s18082663

[6] L.-Y. Leong, K.-B. Ooi, A.Y.-L. Chong, B. Lin, "Modeling the stimulators of the behavioral intention to use mobile entertainment: does gender really matter?", Computers Human Behaviour, Vol. 29, pp. 2109–2121, 2013. doi:10.1016/j.chb.2013.04.004

[7] O.S. Iyasere, S.A. Edwards, M. Bateson, M. Mitchell, & J.H. Guy, "Validation of an intramuscularly-implanted microchip and a surface infrared thermometer to estimate core body temperature in broiler chickens exposed to heat stress", Computers and Electronics in Agriculture, Vol. 133, pp. 1–8, 2017. http://doi.org/10.1016/j.compag.2016.12.010

[8] Y.K. Dwivedi, K.K. Kapoor, M.D. Williams, & J. Williams, "RFID systems in libraries: An empirical examination of factors affecting system use and user satisfaction", International Journal of Information Management, Vol. 33, No. 2, pp. 367–377, 2013. http://doi.org/10.1016/j.ijinfomgt.2012.10.008

[9] A. Juels, "RFID security and privacy: a research survey", IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, pp. 381–394, 2006. http://doi.org/10.1109/JSAC.2005.861395

[10] J.D. Baker, "The Orwellian Nature of Radio-Frequency Identification in the Perioperative Setting", AORN Journal, Vol. 104, No. 4, pp. 281–284, 2016. http://doi.org/10.1016/j.aorn.2016.08.012

[11] Z.Y. Mehrjerdi, "Radio frequency identification: the big role player in health care management ", Journal of Health Organization and Management, Vol. 25, No. 5, pp. 490-505, 2011. https://doi.org/10.1108/14777261111161851

[12] R. Farra, F.N. Sheppard, L. McCabe1, M.R. Neer, M.J. Anderson, T.J. Santini, J.M. Cima, & R. Langer, "First-in-Human Testing of a Wirelessly Controlled Drug Delivery Microchip", Science Translational Medicine Rapid Publication, Vol. 4, No. 122, 2012: 1-10. doi:10.1126/scitranslmed.3003276

[13] C. Buse, "E-scaping the ageing body? Computer technologies and embodiment in later life",Ageing And Society, Vol. 30, No. 6, pp. 987-1009, 2010. http://dx.doi.org/10.1017/s0144686x10000164

[14] P. Freund, "Civilised Bodies Redux: Seams in the Cyborg", Social Theory & Health, Vol. 2, No. 3, pp. 273-289, 2004. http://dx.doi.org/10.1057/palgrave.sth.8700031

[15] D. Lupton, "M-health and health promotion: The digital cyborg and surveillance society", Social Theory & Health, Vol. 10, No. 3, pp. 229-244, 2012. http://dx.doi.org/10.1057/sth.2012.6

[16] M. Ruckenstein, "Visualized and Interacted Life: Personal Analytics and Engagements with Data Doubles", Societies, Vol. 4, No. 1, pp. 68-84, 2014. http://dx.doi.org/10.3390/soc4010068

[17] S. Nair, "QS x NUI", Proceedings of the 2016 ACM International Joint Conference On Pervasive And Ubiquitous Computing Adjunct - Ubicomp '16, 2016. http://dx.doi.org/10.1145/2968219.2968316

[18] P. Fuhrer, D. Guinard, O. Liechti, "RFID: From Concepts to Concrete Implementation, in Proceedings of the International Conference on Advances in the Internet, Processing, Systems and Interdisciplinary Research, IPSI – 2006, February 10-13, 2006, Marbella, Spain.

[19] E. Smith, Charles, "Human Microchip Implantation", Journal of Technology Management & Innovation, Vol. 3, 2008. 10.4067/S0718-27242008000100015.

[20] A.K. Yetisen, Biohacking.Trends in Biotechnology, Vol. 36, No. 8, August 2018.

[21] C. Madrid, T. Korsvold, A. Rochat, M. Abarca, "Radio frequency identification (RFID) of dentures in long-term care facilities", J Prosthet Dent, Vol. 107, No. 3, pp. 199-202, 2012. doi: 10.1016/S0022-3913(12)60057-2.

[22] M.P. Soares dos Santos, J.A. Ferreira, A. Ramos, J.A. Simões, R. Morais, N.M. Silva, P.M. Santos, M.J. Reis, T. Oliveira, "Instrumented hip implants: electric supply systems", Journal of Biomechanics, Vol. 18, No. 46, pp. 2561-2571, 2013. doi: 10.1016/j.jbiomech.2013.08.002.

[23] B. Werber, A. Baggia, A. Žnidaršič, "Behaviour Intentions to Use RFID Subcutaneous Microchips: A Cross sectional Slovenian Perspective", BLED 2017 Proceedings, Vol. 4, 2017. https://aisel.aisnet.org/bled2017/4

[24] M.G. Michael, K. Michael (Eds.), Uberveillance and the Social Implications of Microchip Implants: Emerging Technologies. United States: IGI Global, 2014.

[25] F.D. Davis, "A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results", Thesis (Ph. D), Sloan School of Management, Massachusetts Institute of Technology, USA, 1986. http://hdl.handle.net/1721.1/15192

[26] F.D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology", MIS Quarterly, Vol. 13, No. 3, pp. 319–340, 1989. doi:10.2307/249008

[27] N. Marangunić, A. Granić, "Technology acceptance model: A literature review from 1986 to 2013", Universal Access in the Information Society, Vol. 14, No. 1, pp. 81–95, 2015. 10.1007/s10209-014-0348-1

[28] A. Burton-Jones, G.S. Hubona, "The mediation of external variables in the technology acceptance model", Information & Management, Vol. 43, pp. 706-717, 2006.

[29] A. Alomary, J. Woollard, "How Is Technology Accepted by Users? A Review of Technology Acceptance Models and Theories", Proceedings of the IRES 17th International Conference, London, United Kingdom, 21 November 2015, ISBN: 978-93-85832-48-2

[30] V. Venkatesh, F.D. Davis, "A theoretical extension of the technology acceptance model: Four longitudinal field studies", Management Science, Vol. 46, No. 2, pp. 186–204, 2000. doi: 10.1287/mnsc.46.2.186.11926

[31] R.H. Shroff, C.C. Deneen, & E.M.W. Ng, "Analysis of the technology acceptance model in examining students' behavioural intention to use an e-portfolio system", Australasian Journal of Educational Technology, Vol. 27, No. 4, pp. 600-618, 2011. doi: 10.14742/ajet.940

[32] E.Y.M. Cheung, J. Sachs, "Test of the technology acceptance model for a web-based information system in a Hong Kong Chinese sample", Psychological Reports, Vol. 99, No. 3, pp. 691-703, 2006. 10.2466/PR0.99.3.691-703

[33] B. Pynoo, J. Tondeur, J. van Braak, W. Duyck, B. Sijnave, P. Duyck, "Teachers' acceptance and use of an educational portal", Computers & Education, Vol. 58, No. 4, pp. 1308-1317, 2012. 10.1016/j.compedu.2011.12.026

[34] Ö. Kirmizi, "Measuring technology acceptance level of Turkish pre-service English teachers by using technology acceptance model", Educational Research and Reviews, Vol. 9, No. 23, pp. 1323-1333, 2014. doi:org/10.5897/ERR2014.1970

[35] T. Teo, V. Milutinovic, "Modelling the intention to use technology for teaching mathematics among pre-service teachers in Serbia", Australasian Journal of Educational Technology, Vol. 31, No. 4, pp. 363-380, 2015. 10.14742/ajet.1668

[36] J.M.O. Egea, M.V.R. González, "Explaining physicians' acceptance of EHCR systems: An extension of TAM with trust and risk factors", Computers in Human Behavior, Vol. 27, No. 1, pp. 319–332, 2011.

[37] P.A. Pavlou, "Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model", International Journal of Electronic Commerce, Vol. 7, No. 3, pp. 101–134, 2003. https://doi.org/10.1080/10864415.2003.11044275

[38] A. Ta, V. Prybutok, "A mindful product acceptance model", Journal of Decision Systems, Vol. 27, No. 1, pp. 19-36, 2018. doi: 10.1080/12460125.2018.1479149

[39] W.R. King, J. He, "A meta-analysis of the technology acceptance model", Information & Management, Vol. 43, No. 6, pp. 740-755, 2006. 10.1016/j.im.2006.05.003

[40] B. Šumak, M. Heričko, M. Pušnik, "A meta-analysis of e-learning technology acceptance: The role of user types and e-learning technology types", Computers in Human Behavior, Vol. 27, No. 6, pp. 2067-2077, 2011. 10.1016/j.chb.2011.08.005

[41] C.H. Hsiao, C. Yang, "The intellectual development of the technology acceptance model: A co-citation analysis", International Journal of Information Management, Vol. 31, No. 2, pp. 128-136, 2011. 10.1016/j.ijinfomgt.2010.07.003

[42] J. Schepers, M. Wetzels, "A meta-analysis of the technology acceptance model: Investigating subjective norm and moderation effects", Information & Management, Vol. 44, No. 1, pp. 90-103, 2007. 10.1016/j.im.2006.10.007

[43] P. Ajibade, "Technology Acceptance Model Limitations and Criticisms: Exploring the Practical Applications and Use in Technology-related Studies, Mixed-method, and Qualitative Researches", Library Philosophy and Practice (e-journal), 1941, 2011. htp://digitalcommons.unl.edu/libphilprac/1941

[44] A.Y.-L. Chong, "Mobile commerce usage activities: the roles of demographic and motivation variables", Technol. Forecasting Soc. Change, Vol. 80, pp. 1350–1359, 2013. http://dx.doi.org/10.1016/j.techfore.2012.12.011

[45] V. Venkatesh, M. Morris, G. Davis & F. Davis, "User acceptance of information technology: Toward a unified view", MIS Qarterly, Vol. 27, No. 3, pp. 425-478, 2003. doi: 10.2307/30036540

[46] J.E. Katz, R.E. Rice, "Public views of mobile medical devices and services: A US national survey of consumer sentiments towards RFID healthcare technology", International Journal of Medical Informatics, Vol. 78, pp. 104–114, 2009. http://doi.org/10.1016/j.ijmedinf.2008.06.001

[47] B. Werber, A. Baggia, A. Žnidaršič, "Factors Affecting the Intentions to Use RFID Subcutaneous Microchip Implants for Healthcare Purposes, Organizacija, Vol. 51, No. 2, 2018. Retrieved from http://organizacija.fov.uni mb.si/index.php/organizacija/article/view/842

[48] F.D. Davis, R.P. Bagozzi & P.R. Warshaw, "User acceptance of computer technology: a comparison of two theoretical models", Management Science, Vol. 35, pp. 982-1003, 1989. doi: 10.1287/mnsc.35.8.982

[49] C. Smith, "Human Microchip Implantation", Journal of Technology Management & Innovation, Vol. 3, No. 3, pp. 151-160, 2008. doi: https://doi.org/10.4067/S0718-27242008000100015

[50] K.R. Foster, J. Jaeger, "RFID inside: The murky ethics of implanted chips", IEEE Spectrum, Vol. 44, No. 3, pp. 24–29, 2007. https://doi.org/10.1109/MSPEC.2007.323430

[51] P. Rotter, B. Daskala & R. Compano, "RFID implants: Opportunities and challenges for identifying people", IEEE Technology and Society Magazine, Vol. 27, No. 2, pp. 24–32, 2008. https://doi.org/10.1109/mts.2008.924862

[52] P. Legris, J. Ingham, P. Collerette, "Why do people use information technology? A critical review of the technology acceptance model", Information & Management, Vol. 40, No. 3, pp. 191–204, 2003. doi: 10.1016/S0378-7206(01)00143-4

[53] Q. Ma, L. Liu, "The technology acceptance model: A meta-analysis of empirical findings", Journal of Organizational and End User Computing, Vol. 16, No. 1, pp. 59–72, 2004. http://dx.doi.org/10.4018/joeuc.2004010104

[54] A. Dillon, "User acceptance of information technology", in W. Karwowski (Eds.), Encyclopedia of Human Factors and Ergonomics. London: Taylor and Francis, 2001.

[55] L. Peng, C. Xu, L. Chen, R. Wang, "RFID Privacy Risk Evaluation Based on Synthetic Method of Extended Attack Tree and Information Feature Entropy", International Journal of Distributed Sensor Networks, Vol. 12, pp. 1-9, 2015. http://dx.doi.org/10.1155/2015/146409