



2016 6th International Conference on Information and Communication Technology for The Muslim World

22-24 November 2016
Jakarta, Indonesia



CONFERENCE INFORMATION

PAPERS BY SESSION

PAPERS BY AUTHOR

GETTING STARTED

TRADEMARKS

SEARCH

ORGANIZERS



PROCEEDINGS

**6th International Conference on
Information and Communication Technology
for the Muslim World**

———— ICT4M 2016 ————

Copyright © 2016 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved.

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries may photocopy beyond the limits of US copyright law, for private use of patrons, those articles in this volume that carry a code at the bottom of the first page, provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

Other copying, reprint, or republication requests should be addressed to: IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, P.O. Box 133, Piscataway, NJ 08855-1331.

The papers in this book comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interests of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors, the IEEE Computer Society, or the Institute of Electrical and Electronics Engineers, Inc.

IEEE Computer Society Order Number: E6013
BMS Part Number: CFP1654K-ART
ISBN: 978-1-5090-4521-1

Additional copies may be ordered from:

IEEE Computer Society
Customer Service Center
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314
Tel: + 1 800 272 6657
Fax: + 1 714 821 4641
<http://computer.org/cspress>
csbooks@computer.org

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
Tel: + 1 732 981 0060
Fax: + 1 732 981 9667
[http://shop.ieee.org/store/
customer-service@ieee.org](http://shop.ieee.org/store/customer-service@ieee.org)

IEEE Computer Society
Asia/Pacific Office
Watanabe Bldg., 1-4-2
Minami-Aoyama
Minato-ku, Tokyo 107-0062
JAPAN
Tel: + 81 3 3408 3118
Fax: + 81 3 3408 3553
tokyo.ofc@computer.org

Individual paper REPRINTS may be ordered at: <reprints@computer.org>

Editorial production by Randall Bilof
Cover art production by Mark Bartosik



IEEE Computer Society
Conference Publishing Services (CPS)
<http://www.computer.org/cps>

2016 6th International Conference on Information and Communication Technology for The Muslim World

ICT4M 2016

Table of Contents

Message from the Deputy Rector (Research & Innovation).....	xii
Message from the Dean 1.....	xiii
Message from the Dean 2.....	xiv
Message from the General Co-Chair.....	xv
Message from the Local Co-Chair 1.....	xvi
Message from the Local Co-Chair 2.....	xvii
Committee Members.....	xviii
Reviewers.....	xxii

Track 1: Ummah Cohesion, Education and Training

Influence of ITG on Organisation Performance: The Mediating Effect of Absorptive Capacity	1
<i>Binyamin Adeniyi Ajayi and Husnayati Hussin</i>	
Re-Emphasizing the Dimensions and Impacts of Complementary IT Resources through Governance	7
<i>Ajayi Binyamin Adeniyi, Ahlan Abdul Rahman, and Olanrewaju Rashidah Funke</i>	
Factors Affecting Instructors' Adoption of Learning Management Systems: A Theoretical Framework	13
<i>Nahel A O Abdallah, Abdul Rahman Ahlan, and Odeh Abed Abdullah</i>	
Impacts of Organizational Culture, Support and IT Infrastructure on Knowledge Management Success: An Imperial Study in Islamic Country, Saudi Arabia	19
<i>Abdulrahman A. Gharamah and Mohamad Fauzan Noordin</i>	

Adaptive Tutoring System User Preferences: Does Gender Matter?	24
<i>Faizal Hazri Mat Ripin, Rahmah Mokhtar, and Wahidah Mohd Zain</i>	
A Comprehensive Knowledge Management Process Framework for Healthcare Information Systems in Healthcare Industry of Pakistan	30
<i>Arfan Arshad, Mohamad Fauzan Bin Noordin, and Roslina Bint Othman</i>	
Acceptance and Use of Information and Communication Technology by Academicians: Towards a Conceptual Framework	36
<i>Shahmurad Chandio, Muhammad Sadry Abu Semen, Suhaila Samsuri, and Asadullah Shah</i>	
Certificate-Based Strategy to Auction Model for E-Procurement in Indonesia: A Review on Local Ethics and the Future Challenges	41
<i>Herlino Nanang and Ahmad F. Misman</i>	
A Review for Future Research and Practice in Using Computer Assisted Instruction on Vocabulary Learning among Children with Autism Spectrum Disorder	47
<i>Mariam Adawiah Dzulkifli, Elok Vradizza Feni Abdul, and Abdul Wahab Abdul Rahman</i>	
Undergraduate Students' Acceptance of Library Online Database System to Support Studies and Research	53
<i>Nur Athirah Azlan, Zahidah Zulkifli, Husnayati Hussin, Suhaila Samsuri, and Asma Md Ali</i>	
SAO Extraction on Patent Discovery System Development for Islamic Finance and Banking	59
<i>Roslina Othman, Mohamad Fauzan Noordin, Ria Hari Gusmita, Tengku Mohd Tengku Sembok, and Zahidah Zulkifli</i>	
Investigating Factors Affecting Knowledge Management and Sharing on Innovation in Universities: Pilot Study	64
<i>Mohammad Mozammel Haque, Abd. Rahman Ahlan, Mohamed Jalaldeen Mohamed Razi, and A'ang Subiyakto</i>	
An Adoption of Halal Food Recognition System Using Mobile Radio Frequency Identification (RFID) and Near Field Communication (NFC)	70
<i>Mohsen Khosravi, Mostafa Karbasi, Asadullah Shah, Imtiaz Ali Brohi, and Najma Imtiaz Ali</i>	

Track 2: Innovative Islamic Application

A Practical and Interactive Web-Based Software for Online Qur'anic Arabic Learning	76
<i>Matin Saad Abdullah, M.M. Hafizur Rahman, Al-Sakib Khan Pathan, and Imad Fakhri Al Shaikhli</i>	
My Emergency Assistant Device: A Conceptual Solution in Enhancing the Quality of Life for the Disabled and Elderly	82
<i>Umar Bin Qushem, Abdul Rahman Bin Ahmad Dahlan, and Ahmad Shahril Bin Mohd Ghani</i>	
Testing Sphinx's Language Model Fault-Tolerance for the Holy Quran	88
<i>Mohamed Yassine El Amrani, M.M. Hafizur Rahman, Mohamed Ridza Wahiddin, and Asadullah Shah</i>	
A Preliminary Study of Halal Virtual Inspection: A Case of Halal Certification in Malaysia	93
<i>Mohd Zabiedy Mohd Sulaiman, Nurulhuda Noordin, Nor Laila Md Noor, Ahmad Iqbal Hakim Suhaimi, and Wan Abdul Rahim Wan Mohd Isa</i>	
Towards Innovation Excellence: Why and How to Measure Innovation Performance?	99
<i>Lamyaa El Bassiti and Rachida Ajhoun</i>	
A Conceptual Model on Cloud Computing and SME Performance: Resource-Based View	105
<i>Noor Afzan Salleh and Husnayati Hussin</i>	
ScanMed: A Mobile Medicine Adherence Application with Intake Validation Using QR Code	112
<i>Rizal Mohd Nor, Noor Azizah Mohamadali, Khairul Azmi, Ahmad Marzuki, Leilanie Mohd Nor, and Mohar Yusof</i>	
TCP Skudai: A High Performance TCP Variant for Collaborative Virtual Environment Systems	118
<i>Abdulsalam Ya'u Gital, Abdul Samad Ismail, Haruna Chiroma, and Adamu Abubakar</i>	
Revolving Traditional EEG Device into Mobile Architecture	122
<i>Hafizuddin Muhd Adnan, Hamwira Yaacob, Wahab Abdul, and Marini Othman</i>	
Retrieval Profiling Framework for Thematic Interpretation of Al-Quran	128
<i>Ashraf Ali Salahuddin and Roslina Othman</i>	
User Perceptions on the Attractiveness of Islamic Websites (I-Webs)	134
<i>Madiyahah Sheikh Abdul Aziz and Marini Othman</i>	

Eliminating Unanswered Questions from Question Answering System for Khulafaa Al-Rashidin History	140
<i>Muhammad Zidny Naf'An, Dewi Erla Mahmudah, Syopiansyah Jaya Putra, and Asep Fajar Firmansyah</i>	
System Architecture Conceptual for Applying Malik Bennabi's Ruler on Intellectual Property of Islamic Finance and Banking	144
<i>Roslina Othman, Mohamad Fauzan Noordin, Ria Hari Gusmita, Zahidah Zulkifli, and Tengku Mohd Tengku Sembok</i>	
A Model for Measuring Well-Being of Medical Practitioners in EHR Implementation	148
<i>Maznah Ahmad and Mira Kartiwi</i>	
Frameworks for a Computational Isnad Authentication and Mechanism Development	154
<i>Nuzulha Khilwani Ibrahim, Suhaila Samsuri, Muhamad Sadry Abu Seman, Ahmed Elmogtaba Banga Ali, and Mira Kartiwi</i>	
Development Decision Support System of Choosing Medicine Using TOPSIS Method (Case Study: RSIA Tiara)	160
<i>Amanda Ayu Larasati, Anif Hanifa Setyaningrum, and Luh Kesuma Wardhani</i>	

Track 3: Research, Innovations, Commercialization and Entrepreneurship

Exploring the Influential Factors on Online Investment Platform	166
<i>Haneffa Muchlis Gazali, Adewale Abideen Adeyemi, and Syed Musa Syed Jaafar Alhabshi</i>	
Competitive Ability of Information and Communication Technology Patents: A Case Study of Patents Owned by Indonesian Institute of Sciences (LIPI)	171
<i>Prio Adi Ramadhani and Karno</i>	
Software Testing Techniques: A Literature Review	177
<i>Muhammad Abid Jamil, Muhammad Arif, Normi Sham Awang Abubakar, and Akhlaq Ahmad</i>	
Islamization of Undergraduate Medical Practice: Does Mobile Technology Play a Role?	183
<i>Ardilla Hanim Abdul Razak, Goh Kian Liang, and Mohd Shahidan Noor Rahin</i>	
Software Requirements Patterns and Meta Model: A Strategy for Enhancing Requirements Reuse (RR)	188
<i>Badamasi Imam Ya'u, Azlin Nordin, and Norsaremah Salleh</i>	
Online Shopping Satisfaction in Malaysia: A Framework for Security, Trust and Cybercrime	194
<i>Najma Imtiaz Ali, Suhaila Samsuri, Muhamad Sadry, Imtiaz Ali Brohi, and Asdullah Shah</i>	

Green Computing Knowledge among Students in a Ugandan University	199
<i>Isa Semakula and Suhaila Samsuri</i>	
Using Grounded Theory Approach to Identify Value-Based Factors in Software Development	205
<i>Noor Azura Zakaria, Suhaimi Ibrahim, and Mohd Naz'ri Mahrin</i>	
Information Security Behavior among Employees from the Islamic Perspective	211
<i>Omar Barzak, Nurul Nuha Abdul Molok, Shuhaili Talib, and Murni Mahmud</i>	

Track 4: Computer Networking and Internet of Things

Technological Entrepreneurship for IT/IS Innovations and Inventions	216
<i>Tamrin Amboala</i>	
Watermarking in Protecting and Validating the Integrity of Digital Information: A Case Study of the Holy Scripture	222
<i>Rashida Funke Olanrewaju, Fawwaz Eniola Fajingbesi, and Nur Azimah Binti Ishak</i>	
Persuasive Technology for Improving Information Security Awareness and Behavior: Literature Review	228
<i>Mohammed Abdullah Bawazir, Murni Mahmud, Nurul Nuha Abdul Molok, and Jamaludin Ibrahim</i>	
A New Taxonomy of Cyber Violent Extremism (Cyber-VE) Attack	234
<i>Nurhashikin Mohd Salleh, Siti Rahayu Selamat, Zurina Saaya, Rabiah Ahmad, and Zaki Masúd</i>	
Security Failures in EMV Smart Card Payment Systems	240
<i>Zubair Ahmad, Akram M. Zeki, and Akeem Olowolayemo</i>	
Time Aware Recommendation	244
<i>Alaoui Sara, Younes El Bouzekri El Idrissi, and Rachida Ajhoun</i>	
Facial Recognition System for Fatigue Detection Using Intel Realsense Technology	248
<i>Nenny Anggraini, Nurul Faizah Rozy, and Reza Ayatuna Lazuardy</i>	
A Conceptual Model of Green It Practices on Organisational Sustainability	254
<i>Sri Fatiany Abdul Kader Jailani, Lili Marziana Abdullah, Mira Kartiwi, and Husnayati Hussin</i>	
Analyzing Communication Overhead in Linearizing Peer to Peer System	260
<i>Abdulfattah Muhyiddeen, Rizal Mohd Nor, and M.M. Hafizur Rahman</i>	
Time-Cost Effective Factor of a Midimew Connected Mesh Network	264
<i>M.M. Hafizur Rahman, Mohammed N.M. Ali, Rizal Mohd Nor, Tengku Mohd Tengku Sembok, and M.A.H. Akhand</i>	

Automatic Emotion Recognition Based on EEG and ECG Signals While Listening to Quranic Recitation Compared with Listening to Music	269
<i>Sabaa Ahmed Yahya Al-Galal, Imad Fakhri Taha Alshaikhli, and Abdul Wahab Bin Abdul Rahman</i>	
Comparative Analysis of A* and Basic Theta* Algorithm in Android-Based Pathfinding Games	275
<i>Eka Risky Firmansyah, Siti Ummi Masruroh, and Feri Fahrianto</i>	

Track 5: Business Intelligence and Big Data

Application of the Naive Bayes Method to a Decision Support System to Provide Discounts (Case Study: PT. Bina Usaha Teknik)	281
<i>Fauzan Burdi, Anif Hanifa Setianingrum, and Nashrul Hakiem</i>	
Predicting Obesity from Grocery Data: A Conceptual Process Framework	286
<i>Nur'Aina Daud, Nor Laila Mohd Noor, Nurulhuda Noordin, Fauzi Mohd Saman, and Nur Islami Mohd Fahmi Teng</i>	
Deriving Specific Requirement Patterns for Collaborative Meeting and Appointment Scheduler Domain (CMASD)	292
<i>Farah Nur Atikah Suhaizad, Raida Rashiqa Burhanudin, and Azlin Nordin</i>	
Measuring Customer Satisfaction through Speech Using Valence-Arousal Approach	298
<i>Norhaslinda Kamaruddin, Abdul Wahab Abdul Rahman, and Aina Najwa Razman Shah</i>	
Big Data Initiatives by Governments -- Issues and Challenges: A Review	304
<i>Noor Zalina Zainal, Husnayati Hussin, and Mior Nasir Mior Nazri</i>	
Handwritten Bangla Numeral Recognition Using Deep Long Short Term Memory	310
<i>Mahtab Ahmed, M.A.H. Akhand, and M.M. Hafizur Rahman</i>	
Comparative Analysis of the Accuracy of Backpropagation and Learning Vector Quantisation for Pattern Recognition of Hijaiyah Letters	316
<i>Nimas Ayu Mailani, Victor Amrizal, and Nashrul Hakiem</i>	
Biometric Identification for Twins Using Photoplethysmogram Signals	320
<i>Nur Izzati Mohammed Nadzri, Khairul Azami Sidek, and Rizal Mohd Nor</i>	
EEG-Based Emotion Recognition in the Investment Activities	325
<i>Nurul Izzati Mat Razi, Marini Othman, and Hamwira Yaacob</i>	
Validity of Expert System, Diagnosis of the Disease Treatment with Prayer by Verse of the Koran Using Method of Certainty Factor Web-Based Application	330
<i>Fita Nur Fauziah, Feri Fahrianto, and Victor Amrizal</i>	

The Effect of E-CRM Features on Customers Satisfaction for Airline E-Ticket Services in Malaysia	336
<i>Nor Alina Binti Ismail and Husnayati Binti Hussin</i>	
Isnad Al-Hadith Computational Authentication: An Analysis Hierarchically	344
<i>Nuzulha Khilwani Ibrahim, Mohamad Fauzan Noordin, Suhaila Samsuri, Muhamad Sadry Abu Seman, and Ahmed Elmogtaba Banga Ali</i>	
Author Index	349

Persuasive Technology for Improving Information Security Awareness and Behavior: Literature Review

Mohammed Abdullah Bawazir
Department of Information System, KICT
International Islamic University Malaysia
Kuala Lumpur, Malaysia
Bawazir333@gmail.com

Murni Mahmud
Department of Information System, KICT
International Islamic University Malaysia
Kuala Lumpur, Malaysia
murni@iium.edu.my

Nurul Nuha Abdul Molok
Department of Information System, KICT
International Islamic University Malaysia
Kuala Lumpur, Malaysia
nurulnuha@iium.edu.my

Jamaludin Ibrahim
Department of Information System, KICT
International Islamic University Malaysia
Kuala Lumpur, Malaysia
jamaludinibrahim@iium.edu.my

ABSTRACT—The use of Persuasive Technology in various fields is rapidly increasing. It can be applied in many fields such as computing, marketing, sales, environment, education, and health. Persuasive Technology has been found effective in bringing a required change in users' behaviors and attitudes. However, the use of persuasive technology is scarce in the field of Information Security awareness. This paper reviews extensive literature review which focuses on a perspective on how to create awareness among users for good information security practices by applying Persuasive Technology techniques and approaches. The conceptual findings suggest there is a tremendous potential of Persuasive Technology to be applied to persuade users to change their behavior and perception toward Information Security practices.

Keywords—*Persuasive technology; information security awareness; literature review; information security; behavior*

I. INTRODUCTION

The advancement in the field of information technology has seen tremendous growth in the past few years. The technology has penetrated into the lives of people so much that the people can now shop, pay bills and even order groceries with just one click away. This advancement is extremely useful, and it saves a lot of time of the people. However, it is said that everything comes at a price and the price for this advancement is the increasing threat of information security to individuals as well as organizations. Therefore, to secure the confidential, integrity and availability of information of the individuals and also those of the organizations, persuasive technology must be used. Persuasive technology is a technology to bring about a change in the behavior and attitudes of the people with respect to various issues in information security. This technology can be used to secure the personal and top secret

information, the threats of which can cause harm to the person or the organization. A literature review was carried out to comprehensively determining utilized methods and approaches in the research area of using persuasive technology to improve users' information security awareness and behavior within the past years. Hence, the use of persuasive technology in securing information and changing user behavior is discussed in this conceptual paper.

II. DEFINITIONS AND MEANINGS

A. Meaning Of The Term 'Persuasion'

The term persuasion is well explained by Ijsselsteijn, de Kort, Midden, Eggen, and van den Hoven [1] as Persuasion is generally part and parcel of people relationship. Persuasive effort in a steady attempt to provide an effect on our awareness and behaviors, persuading us to spend money on one product rather than another, to select for a particular politics party, to stop cigarette smoking, to doing exercises much more, to deal with for environmental preservation, animal well-being, much better education or to eat a fruit. As per the author, humans are the best persuaders because they have a strong social impact on the society. However, Fogg [2] says, computers have a lot of advantages over human persuaders. The best advantage of computers is that they can cover a vast area at one time as against the humans who will not be able to be present at more than one place at one time.

According to Qudaih, Bawazir, Usman, and Ibrahim [3], persuasion forms a critical part in the field of human interaction. There are many human ways of persuasion which help in influencing the people to behave in a certain manner. In order to amplify the impact created by the persuaders on the minds of the users, the persuaders often use the technology for helping users to shape their attitude

and behavior. The technology also comprises of using the digital media to influence the people to behave in a certain manner.

B. Persuasive Technology (Captology)

Fogg [2] states that computers can be used as persuasive technology and can be so designed to bring about a change in the behaviors and attitudes of the people with respect to health, environment, education, fitness, personal improvement and also in personal finance. The computers also help in involving the community and developing personal relationships so as to influence the behavior of the consumers. Fogg [2] has termed this study of computers being used as a tool for persuasive technologies as "Captology". He gave some examples of the users of this technology such as Amazon gold box offer, America's Army, RSI guard, Sportbrain and Quitnet.com. This entire technology is designed to influence the prospective consumers to buy a product or influencing the employees to behave in a certain manner as is required by the organization. Fogg [2] prescribed the way in which to carry out the influence analysis which involves outlining the landscape, identification of the targets, and proposing the appropriate solutions.

Fogg [2] presented a new model in order to understand the behavior of humans which suggests that people behavior is influenced by these three factors ability, triggers, and motivation. The model assumes that if a person wants to achieve a target behavior, it is essential that the person must be motivated sufficiently, possess enough ability to be able to perform a certain kind of behavior and he is triggered to perform the target behavior. Also, it is assumed in the model that all the three above mentioned factors must occur simultaneously. Otherwise, the target behavior will certainly not happen. This model helps the employees to work in teams and promotes teamwork culture because the employees are able to understand the change in behavior. It is essential to understand the change in behavior to make the employees more efficient. The tools which are used to create persuasive products are very easy to use. This is due to the fact there have been many innovations that have taken place in the online videos and the social networks. [4] Fogg also proposed three steps method for the designers. The steps in that method are "Get specific, make it easy and trigger the behavior". Fogg in his book also offers "Behavior Design Boot Camps", which serves as a guide for the designers which helps them to use the persuasive technology to the full. In the year 2007, his famous "Facebook Class" helped many of his students to launch various types of apps at a very fast pace and most of them earned a huge amount of money before they had completed the course. Fogg says that this period can be said to be "a period of time when you could walk in and collect gold." [5]

In a conference held in Austria [6], it was stated that Persuasive Technology is a really lively multidisciplinary study area, concentrating on the design, development and

evaluation of interactive technologies targeted at changing users' awareness or behaviors throughout persuasion and social impact, although not via deception or coercion.

Fogg [7], have explained that in the era of cloud computing and further advancement in the technology, "there are many new opportunities for a more effective relationship between people and solutions." This has further increased the scope of the researchers.

In the qualitative study, for example, smoke cessation which was conducted in New Zealand context using a game that developed in "think-aloud" protocol to persuade people to quit smoking by recording their respond and comments and evaluate them, shows that the effectiveness of the game to change their behavior in this matter[8] . On the other hand, quantitative studies also show the improvement among the users, for instance, a mobile application that promoted healthy lifestyles persuading the majority of participants' awareness to improve health-related behavior modification [9].

III. INFORMATION SECURITY

A. Threat to Confidential Information

As per the views of Crossler, Johnston, Lowry, Hu, Warkentin and Baskerville [10], Information Security study is far achieving and contains technical, behavioral, philosophical, managerial, and organizational approaches that identify the protection and mitigation of risks to information assets. The authors believe that most of the confidential information of the organization is threatened due to the internal people of the organization. The authors state that "researchers estimate that nearly half of intrusions and security violations occur from within an organization by organizational insiders." The major areas that are researched by the authors are categorized into three parts namely, separating insider misbehavior from insider deviant behavior; revealing the mystery of the hacker world; improving information Cross-cultural InfoSec research and security compliance. Also, the authors have classified the threats internal to the organization into two parts, i.e. intentional and unintentional. Therefore, the organization must employ persuasive technology to reduce such malicious acts of the people internal to the organization.

B. Information Security Awareness

In accordance with Siponen [11], the approaches to information security awareness at present are quite detailed and theoretical and are not accomplishment oriented. Siponen further explained that information security awareness is of essential importance, as information security procedures or techniques might be misinterpreted, misused, or not utilized by end-users, therefore losing their actual usefulness. Also, the author believes that with an organization level, it's critical, for instance, to recognize, understand and quantify the background and hidden reasons for the 'human errors' under consideration.

As per the views of Lean-Ping and Chien-Fatt [12], the organizations must strive to promote the awareness regarding the information security, which has been highly jeopardized in the present times due to the increase in technology usage. All the flexibility, convenience, and ease-of-use features of technology include threats. The potential risks might be regarding financial losses, data losses, reputation risks, legislation risks or intellectual property. These risks can lead to the closure of the business carried on by the organization.

C. *Creation of Information Security Policy*

The views of Yeo, Rahim, and Ren [13] are quite similar to the other authors discussed above. Persuasive technology has proved to be very useful in the sales and marketing and now it is also being used in information security within the organization. In the research conducted by them, they have studied the use of persuasive technology in the field of information security. They have extended the application of persuasive technology in creating awareness among the employees of the company with respect to information security. They have used a theory-based approach, for evaluating the use of the web-based paradigm, i.e. persuasive technology. This will help in the improvement of awareness regarding the information security in the end users of the information. This will especially be useful for the IT researchers in the development of various effective information security strategies for improving the behaviors and attitudes of the end users regarding the information security. As mentioned in this research, there are three types of behavior of the end users which are, malicious, neutral and beneficial. On the basis of the behavior types, the policy must be created.

One of the methods generally employed by the organizations to deal with the misuse or loss of information is the framing of the Information Security Policy within the organization. The Information Security Policy details the guidelines that are required to be followed by the employees of the organization while using the information assets. The policy can be enforced using technology also [14]. Technology which uses persuasive strategies has been utilized to enhance various of target behaviors in varied domains, for example , health, education, sustainability, etc [14]. Therefore, it is often advised to use technology to implement the Information Security Policy in the organization.

IV. USING PERSUASIVE TECHNOLOGY

A. *Persuasive Technology for Information Security*

It has mentioned in the research[15] ,"Employees in organizations frequently violate information security policies. According to a survey by PWC, 87% of small and 93% of large organizations had a breach in information security in 2013; 36% of the security breaches are caused by the organizations' employees." Moreover, based on IBM Security Services 2014 Cyber Security Intelligence Index

magazine [16], it is disheartening, that over 95 percent of digital incident caused by human error. Such as poor patch, system misconfiguration, management, lost mobile devices or laptops, using default user names and passwords or easy-to-guess passwords and disclosure of regulated information via the use of an incorrect email address. Essentially the most common making contributions human fault? "Double clicking" on an infected attachment or unsafe URL. The authors [15] in their research report also stated that Persuasive strategies are used only hardly ever within the area of information security and not in a concentrated method to improve information security policy compliance. Therefore, it is believed to explore this area of persuasive technology extensively.

D'Arcy, Hovav and Galletta [17], also state that the misuse of the information resources which is intentional and happens within the company is the most serious threat that can cause serious disruption to the normal working of the company. Depending on the reports, industry statistics claim that between 50%-75% of security breach begin from inside an organization. Since there has been a tremendous increase in misusing the information by the employees or others closely related to the company, there is a need for the organization to understand how to reduce such a misuse. Hence in order to reduce the misuse of information critical to the organizations or an individual, persuasive technology must be used. This is a new area where this technology can be used. The outcome of the research conducted by the authors resulted in finding out the three practices to discourage the misuse of information and they are: creating awareness about the security policies among users, security training, and education and developing various awareness programs monitoring the computers regularly. The research further suggests that perceived severity of sanctions works more effectively in cutting IS misuse than a certainty of sanctions. Hence, the companies must use this latest technology in order to reduce such misuse of the information.

Hochleitner and Tscheligi [18] have discussed that the information security policy in the organization often gets violated by the employees of the company and such violations are very frequent and these add to the ever increasing expenses of the organization. There are many methods that are employed by the organizations in order to stop these violations. These methods include training and proper education regarding the importance of information security in the organization and various other awareness campaigns. These methods employed by the company have a short term effect on the attitudes of the employee with respect to the information security policy of the organization. For the promotion of the long-term awareness of the information security policy and its compliance, the authors have suggested a very innovative framework called PAINLESS "(Personalized Multimodal Persuasive Ambient Intelligence for Information Security at the Workplace)." The organization can employ this framework for detecting

any sort of violations caused by the information security policy. The concept of the PAINLESS framework is that this framework will make the use of various sensors which involve both the hardware and software sensors which will help in providing adequate information to the monitoring of the security policy and the alerting system as well. The persuasive technology is one method that is proposed under the framework as suggested above. The persuasive technology aims to change the behavior and attitude of the people in a certain sphere. This is done by implementing various strategies of persuasion. The persuasive technology has been used very rarely in the field of information security.

Information is considered to be an integral part of the organization and this information is required to be kept confidential in order to become successful in the long run. Any breach caused in the information security policy framed by the organization can lead to disastrous consequences. Therefore, the authors have suggested using the computer technology in order to persuade employees of the organization so that they understand the importance of keeping the information safe and secure and also to change their attitude towards the organization [3].

Kegel and Wieringa [19] have also expressed the views of the above-mentioned authors that the use of digitalization in the organization can cause a serious threat to the information in an organization. The security of information is hampered to a great extent due to the advancement in the technology. Nowadays all the organizations provide their employees the facility to do work from home. This poses a serious threat to the information security in the company. The organization has an option to use its self-designed persuasive tool in order to motivate the people to act in a certain manner. There are various factors that influence the ability of the system which leads to persuasion. Therefore, it is very important for the organizations to adapt to the persuasive technology in order to influence the behavior of the employees regarding the security of the information in the organization.

B. Persuasive Technology to Change Behavior regarding Information Security

Another popular approach is the Behavior Change Support System. A Behavior Change Support System is an efficient and common approach for changing people awareness and behavior. Depending upon the concepts of persuasion, system designed to be able to promote positive users awareness in the direction of organizational information security, enable users to create advised security actions, and enhance secure work practices as subjective norm in the organization [14].

It is always suggested that the organization must motivate their employees to adopt all the measures they can for the security of the information. According to the authors numerous security professionals experience the issue of weak passwords to an insufficient user motivation and

effort. On the other hand, the authors reveal that users generate insecure passwords because not enough motivation, but to misunderstanding the security threats, and how you can successfully protect themselves with the offered mechanisms [20]. The authors suggest that by using the persuasive technology the users can be motivated to create strong passwords.

Some of the authors also suggest that the end users must be diligent enough to update their antivirus regularly so as to prevent the system from unwanted intervention and unauthorized access. The people are required to be motivated for the same and they must stop procrastination. The antivirus is software that helps in detection of the malicious software programs which intent to destroy the confidential and important information [21].

Some of the researchers suggest that it will be better to persuade the developers of software to install and adopt various security tools while developing software. For this, the developers need to understand the vulnerabilities of the system and the software. There is available methods which can be properly discovered or reduce these vulnerabilities. Nevertheless, these kinds of methods are simply helpful if they are used. Software developers, system administrators and intelligence analysts require various kinds of security tools within their respective domains [22].

The major problem that the organizations have to face is they are not able to influence their employees to behave securely. The authors state that there have been a large amount of research in providing new security measures and instructions. Still the users do not create strong passwords. The Persuasive Authentication Framework can be used by the organizations to teach their users and employees the importance of Information Security and this mechanism applies persuasive technology in order to authentication mechanisms [23].

Some of the researchers also believe that the current security systems do not take into consideration the importance of humans in building safe and secure systems. The researchers believe that the password system must be very strong in order to secure the system and the information. "In an attempt to generate more memorable passwords, graphical password system has been developed" [24]. Therefore, many stronger authentication passwords must be created to keep the information safe and secure.

The persuasive technology must be implemented by the organizations for ensuring the creation of strong passwords. This will help to save the confidential information from the unauthorized access. The users within the organization depend on the security messages and communication to create essential decisions. A failure for making certain that these security messages are communicated in an easy to understand structure and format will lead to misconception, unclear and worst situation confusing users [25].

The users are required to be persuaded in order to make the information secure. Especially while doing online

shopping, the users are required to give their details very securely and keep their passwords secure. The continuing development and viability of e-commerce are mainly influenced by its capability to assure customer security and stop deceptive activities. A specific problem during these efforts is to confirm the identification of the particular person to be able to prevent incorrect access to his or her personal information [26]. Hence, the users are required to keep their passwords safe and secure as the leakage in the passwords can cause a financial loss to them. As outlined by Weirich and Sasse [27], "The mechanisms of the password are the first line of protection of most computer systems, and therefore affect almost every user on everyday basis". It should also be investigated that how much the user's willingness is impacted by the brand familiarity and also their willingness to engage themselves in the ever increasing security procedures. This will help the developers of the software to incorporate the appropriate security tools and measures.

Another critical element of information security aware behavior is email management. A vital factor of email management is worried about spam emails. Spam email is undesirable email that could contain commercial advertising and marketing, porn material or get-rich-quick strategies. The issues presented by spam have increased from simple disturbed to security problems, for instance, virus attacks. The flood of spam costs about approximately \$20 billion annually. However, by implementing persuasive technology to manage users' email, that will help user to reduce the likelihood of becoming attacked. Therefore, when you are security cautious and using methods against spammers, also by carrying out a good email management practice, such as, using anti-virus to scan email attachment, delete email from people you don't know and using spam and phishing filter[13].

Further, the researchers believe that the attitude of the users towards the information security must necessarily be changed. Therefore, a growing number of information technology systems and services are being developed for persuasive purposes, i.e. to change users' attitudes or behavior or both [28].

V. CONCLUSION

There are many types of information which may be confidential to the organization and the leakage or corruption of such information may cause serious harm to the organization, financially as well as socially. Vulnerabilities to any type of digital information are extremely hard to deal with. It requires adequate training and motivation to perform functions in a manner which will lead to the good conduct of the security practices. However, these are short-term ways to create awareness. The companies, thus, in order to create a long-term impact must make use of persuasive technology to secure the information that is critical to the company. Furthermore, creating long-term impact will enhance the sustainability of users'

security awareness and behavior as well as raise the awareness of current or future security issues. Based on the finding in some researches that have been conducted on persuasive technology with few security measures, it has been confirmed that has highly potential to change users' awareness and behavior toward information security. However, the limitation in this field is testing very few security measures which need to include other security topics in future research. Moreover, this field of research does not have any clear model or framework that helps designers to create more efficient system.

REFERENCES

- [1] W. IJsselsteijn, Y. d. Kort, C. Midden, B. Eggen, and E. v. d. Hoven, "Persuasive Technology for Human Well-Being: Setting the Scene," Eindhoven University of Technology, The Netherlands, Report, 2006.
- [2] B.J.Fogg, "How to Motivate & Persuade Users," Stanford University Tutorial, 2003.
- [3] H. A. Qudaih, M. A. Bawazir, S. H. Usman, and J. Ibrahim, "Persuasive Technology Contributions Toward Enhance Information Security Awareness in an Organization," *International Journal of Computer Trends and Technology (IJCTT)*, vol. 10, no. 4, pp. 180-186, Apr. 2014.
- [4] B. Fogg, "A Behavior Model for Persuasive Design," in *Proceedings of the 4th international Conference on Persuasive Technology*, 2009, p. 40.
- [5] J. Larson, "The Invisible, Manipulative Power of Persuasive Technology," *Pacific Standard*, p. 14, May 2014.
- [6] M. Almaliki and R. Ali, "Persuasive and Culture-Aware Feedback Acquisition," in *The 11th international conference on Persuasive Technologies*, Salzburg, Austria, 2016, pp. 27-38.
- [7] B. J. Fogg, "The behavior grid: 35 ways behavior can change," in *Proceedings of the 4th international Conference on Persuasive Technology*. ACM, 2009, p. 42.
- [8] R. Khaled, R. Fischer, J. Noble, and R. Biddle, "A qualitative study of culture and persuasion in a smoking cessation game," in *International Conference on Persuasive Technology*, Oulu, 2008, pp. 224-236.
- [9] S. Halko and J. A. Kientz, "Personality and persuasive technology: an exploratory study on health-promoting mobile applications," in *International Conference on Persuasive Technology*, Copenhagen, 2010, pp. 150-161.
- [10] R. E. Crossler, et al., "Future directions for behavioral information security," *computers & security*, vol. 32, no. 1, pp. 90-101, 2013.
- [11] M. T. Siponen, "A conceptual foundation for organizational information security awareness," *Information Management & Computer Security*, vol. 8, no. 1, pp. 31-41, 2000.
- [12] O. Lean-Ping and C. Chien-Fatt, "Information Security Awareness: An Application of Psychological Factors – A Study in Malaysia," Southern Cross Business School, Australia, Report, 2014.
- [13] A. C. Yeo, M. M. Rahim, and Y. Y. Ren, "Use of Persuasive Technology to Change EndUsers' IT Security Aware Behaviour: A Pilot Study," *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*, vol. 2, no. 10, pp. 1086-1092, 2008.
- [14] M. Busch, et al., "Persuasive Information Security A Behavior Change Support System to Help Employees Protect Organizational Information Security," Workshop, 2015.
- [15] M. Busch, P. Wolkerstorfer, C. Hochleitner, G. Regal, and M. Tscheligi, "Poster: Designing a Persuasive Application to Improve Organizational Information Security Policy Awareness, Attitudes and

- Behavior," Austrian Institute of Technology, Research Report, 2014.
- [16] I. G. T. Services, "IBM Security Services 2014 Cyber Security Intelligence Index," IBM Corporation Analysis of cyber attack and incident data from IBM's worldwide security operations Somers, NY 10589, 2014.
 - [17] J. D'Arcy, A. Hovav, and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research*, vol. 20, no. 1, pp. 79-98, Mar. 2009.
 - [18] C. Hochleitner, M. Tscheligi, M. Busch, and P. Wolkerstorfer, "PAINLEsS – Personalized Multimodal Persuasive Ambient and Peripheral Interaction for Information Security," CURE – Center for Usability Research & Engineering Workshop, 2014.
 - [19] R. H. P. Kegel and R. J. Wieringa, "Persuasive Technologies: A Systematic Literature Review and Application to PISA," 2014.
 - [20] A. Forget, S. Chiasson, P. C. v. Oorschot, and R. Biddle, "Persuasion for Stronger Passwords: Motivation and Pilot Study," School of Computer Science, Carleton University, Ottawa, Canada, Research Report, 2008.
 - [21] L. Zhang-Kennedy, S. Chiasson, and R. B. Carleton, "Stop Clicking on "Update Later": Persuading Users They Need Up-to-Date Antivirus Protection," Research Report, 2014.
 - [22] B. Jordan, B. Johnson, J. Witschey, and E. Murphy-Hill, "Designing Interventions to Persuade Software Developers to Adopt Security Tools," North Carolina State University, Raleigh, Research Report, 2014.
 - [23] A. Forget, S. Chiasson, and R. Biddle, "Persuasion as Education for Computer Security," in , Quebec City, 2007.
 - [24] S. Hande, N. Dighade, R. Bhusari, M. Shende, and P. H. Agrawal, "Image Based Authentication for Folder Security using Persuasive Cued Click-Points and SHA," *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 16, no. 2, pp. 124-128, Mar. 2014.
 - [25] N. H. Zakaria and N. Katuk, "Towards Designing Effective Security Messages: Persuasive Password Guidelines," in , Kedah, 2013.
 - [26] M. Nowak, et al., "Toward an Experimental Methodology for Studying Persuasion-Based Online Security," in , Boston, 2009.
 - [27] D. Weirich and M. A. Sasse, "Pretty Good Persuasion: A First Step towards Effective Password Security in the Real World," University College, 2002.
 - [28] H. Oinas-Kukkonen and M. Harjumaa, "Towards Deeper Understanding of Persuasion in Software and Information Systems," in , Sainte Luce, 2008.