

# **2017 International Conference on Research and Innovation in Information Systems (ICRIIS 2017)**

**Langkawi, Malaysia  
16-17 July 2017**



**IEEE Catalog Number: CFP1739N-POD  
ISBN: 978-1-5090-3036-1**

**MICROSOFT CORP.  
EXHIBIT 1041**

**Copyright © 2017 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 are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

***\*\*\* This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP1739N-POD
ISBN (Print-On-Demand):	978-1-5090-3036-1
ISBN (Online):	978-1-5090-3035-4
ISSN:	2324-8149

**Additional Copies of This Publication Are Available From:**

Curran Associates, Inc  
57 Morehouse Lane  
Red Hook, NY 12571 USA  
Phone: (845) 758-0400  
Fax: (845) 758-2633  
E-mail: [curran@proceedings.com](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# TABLE OF CONTENTS

<b>IONTO - ONTOLOGY DRIVEN APPROACH FOR SELECTING APPROPRIATE ONTOLOGY MATCHING ALGORITHM</b> .....	1
<i>Sobhani Umanga Pilapitiya</i>	
<b>NEED FOR INFORMATION SECURITY POLICIES COMPLIANCE: A PERSPECTIVE IN HIGHER EDUCATION INSTITUTIONS</b> .....	7
<i>Sadaf Hina ; Dhanapal Durai Dominic</i>	
<b>DETECTION AND PREVENTION OF POSSIBLE UNAUTHORIZED LOGIN ATTEMPTS THROUGH STOLEN CREDENTIALS FROM A PHISHING ATTACK IN AN ONLINE BANKING SYSTEM</b> .....	13
<i>Shammi Ishara Hewamadduma</i>	
<b>THE RELATIONSHIP BETWEEN MANAGEMENT SUPPORT AND INDIVIDUAL MOTIVATION FOR KNOWLEDGE SHARING PRACTICE</b> .....	19
<i>Arif Abdelwhab Ali ; P. D. D. Dominic</i>	
<b>A SYSTEMATIC LITERATURE REVIEW: INFORMATION SECURITY CULTURE</b> .....	25
<i>Amjad Mahfuth ; Salman Yussof ; Asmidar Abu Baker ; Nor'Ashikin Ali</i>	
<b>A CONCEPT-LEVEL APPROACH IN ANALYZING REVIEW READERSHIP FOR E-COMMERCE PERSUASIVE RECOMMENDATION</b> .....	31
<i>Nur-Syadhila Bt Che Lah ; Ab Razak Bin Che Hussin ; Halina Mohamed Dahlan</i>	
<b>DEVELOPING A SUCCESS MODEL OF RESEARCH INFORMATION MANAGEMENT SYSTEM FOR RESEARCH AFFILIATED INSTITUTIONS</b> .....	36
<i>Mahmudul Hasan ; Harmi Izzuan Baharum ; Ganthan Narayana Samy ; Nurazeen Maarop ; Wardah Zainal Abidin ; Noor Hafizah Hassan</i>	
<b>THE ROLES OF PROJECT STAKEHOLDERS IN EPCM BIM-ENABLED PROJECTS</b> .....	42
<i>Cen Ying Lee ; Heap-Yih Chong ; Xiangyu Wang</i>	
<b>FILE AND TEAM MANAGEMENT ON REMOTELY-WORKED BUILDING INFORMATION MODELLING PROJECT</b> .....	48
<i>Gregorius A Gegana A ; Fauzan Alfi Agirachman</i>	
<b>TOUCH SENSATION AS PART OF MULTIMEDIA DESIGN ELEMENTS TO IMPROVE COMPUTER ACCESSIBILITY FOR THE BLIND USERS</b> .....	54
<i>Manoranjitham Muniandy ; Suziah Sulaiman</i>	
<b>NEARMESH: NETWORK ENVIRONMENT AWARE ROUTING IN A WIRELESS MESH NETWORK FOR EMERGENCY-RESPONSE</b> .....	60
<i>Tawfik Al-Hadhrami ; Faisal Saeed</i>	
<b>E-LEARNING SERVICE QUALITY</b> .....	66
<i>Nur Amirah Abd Rahman ; Nor Hayati Abdul Hamid</i>	
<b>INFORMATION SECURITY CULTURE IN HEALTH INFORMATICS ENVIRONMENT: A QUALITATIVE APPROACH</b> .....	72
<i>Noor Hafizah Hassan ; Norazeen Maarop ; Zuraini Ismail ; Wardah Zainal Abidin</i>	
<b>ROADCROWD: AN APPROACH TO ROAD TRAFFIC FORECASTING AT JUNCTIONS USING CROWD-SOURCING AND BAYESIAN MODEL</b> .....	78
<i>Sazid Zaman Khan ; W. M. Abdul Rahuman ; Shaon Dey ; Toni Anwar ; A. S. M. Kayes</i>	
<b>A MOBILE BASED ENVIRONMENTAL EDUCATION FOR PRIMARY SCHOOLCHILDREN IN MALAYSIA</b> .....	84
<i>K. S. Savita ; Manoranjitham Muniandy ; Z. Nur' Ain ; Mazlina Mehat</i>	
<b>RESOLVING DATA DUPLICATION, INACCURACY AND INCONSISTENCY ISSUES USING MASTER DATA MANAGEMENT</b> .....	90
<i>Faizura Haneem ; Rosmah Ali ; Nazri Kama ; Sufyan Basri</i>	
<b>THE DESIGN OF A SCHOOLCHILDREN IDENTIFICATION AND TRANSPORTATION TRACKING SYSTEM</b> .....	96
<i>Khairul Shafee Kalid ; Nabihah Rosli</i>	
<b>REVIEW ON THE ROLE OF SOCIAL SUPPORT IN HEALTH INFORMATION SYSTEMS</b> .....	102
<i>Archanaa Visvalingam ; Jaspaljeet Singh Dhillon ; Saraswathy Shamini Gunasekaran</i>	
<b>AN EFFICIENT FUZZY KEYWORD MATCHING TECHNIQUE FOR SEARCHING THROUGH ENCRYPTED CLOUD DATA</b> .....	108
<i>M A Manazir Ahsan ; Fahad Zaman Chowdhury ; Musarat Sabilah ; Ainuddin Wahid Bin Abdul Wahab ; Mohd Yamani Idna Bin Idris</i>	

<b>RTRAFFIC - A REALTIME WEB APPLICATION FOR TRAFFIC STATUS UPDATE IN THE STREETS OF BANGLADESH</b> .....	113
<i>Shuvashish Paul ; Pinku Deb Nath ; Naseef M. Abdus Sattar ; Hasan U. Zaman</i>	
<b>A NOVEL CONCEPTUAL FRAMEWORK OF HEALTH INFORMATION SYSTEMS (HIS) SUSTAINABILITY</b> .....	119
<i>Noor Azizah Mohamadali ; Nur Faizah Ab Aziz ; Nurul Aqilah Mohd Zahari</i>	
<b>INFORMATION MODEL TO SUPPORT SUSTAINABLE PROCUREMENT</b> .....	125
<i>Emelia Akashah P. Akhir ; Robert T. Hughes ; Karl Cox</i>	
<b>A PILOT STUDY: SHUTTLE BUS TRACKER APP FOR CAMPUS USERS</b> .....	131
<i>Su Mon Chit ; Lee Yen Chaw ; Chee Ling Thong ; Chiw Yi Lee</i>	
<b>REVIEW ON DASHBOARD APPLICATION FROM MANAGERIAL PERSPECTIVE</b> .....	137
<i>Azizah Abdul Rahman ; Yunusa Bena Adamu ; Pershella Harun</i>	
<b>LIFESTYLE DISEASE PREVENTION: HEALTH LITERACY, HEALTH ATTITUDE AND MHEALTH</b> .....	142
<i>Moi Wei Yun ; Nasuha Lee Abdullah ; Rosnah Idrus ; Pantea Keikhosrokiani</i>	
<b>A FRAMEWORK FOR DEVELOPING PREDIABETES SELF-CARE APPLICATION</b> .....	148
<i>Suthashini Subramaniam ; Jaspaljeet Singh Dhillon ; Mohd. Sharifuddin Ahmad ; Cameron Teoh ; Joyce W Leong</i>	
<b>FACTORS CONCERNING PROCUREMENT SELECTION IN BUILDING INFORMATION MODELLING (BIM) PROJECTS</b> .....	155
<i>Hamizah Liyana Tajul Ariffin ; Kerk Chia Cun ; Faraziera Mohd. Raslim ; Nur Emma Mustaffa</i>	
<b>KNOWLEDGE GRAPH CONSTRUCTION AND SEARCH FOR BIOLOGICAL DATABASES</b> .....	161
<i>Nazar Zaki ; Chandana Tennakoon ; Hany Al Ashwal</i>	
<b>MODELING INSTRUCTIONAL MATERIAL USING ONTOLOGY</b> .....	167
<i>Khairul Nurmazianna Ismail ; Fadilah Ezlina Shahbudin ; Fadzlin Ahmadon</i>	
<b>THE CHALLENGES OF EXTRACT, TRANSFORM AND LOADING (ETL) SYSTEM IMPLEMENTATION FOR NEAR REAL-TIME ENVIRONMENT</b> .....	172
<i>Adilah Sabtu ; Nurulhuda Firdaus Mohd Azmi ; Nilam Nur Amir Sjarif ; Saiful Adli Ismail ; Othman Mohd Yusop ; Haslina Sarkan ; Suriyati Chuprat</i>	
<b>A CONCEPTUAL FRAMEWORK FOR SOCIAL NETWORK ANALYSIS OF BUILDING INFORMATION MODELLING IN CONSTRUCTION PROJECTS</b> .....	177
<i>Fotios Gardounis ; Heap-Yih Chong ; Xiangyu Wang</i>	
<b>SERVICE SYSTEMS ENGINEERING FRAMEWORK BASED ON COMBINING SERVICE ENGINEERING AND SYSTEMS ENGINEERING METHODOLOGIES</b> .....	183
<i>Suhardi ; Novianto Budi Kurniawan ; Jaka Sembiring ; Purnomo Yustianto</i>	
<b>PUBLIC COMPLAINT SERVICE ENGINEERING BASED ON GOOD GOVERNANCE PRINCIPLES</b> .....	189
<i>Suhardi ; Novianto Budi Kurniawan ; Deni Prayitno ; Jaka Sembiring ; Purnomo Yustianto</i>	
<b>THE INFLUENCE OF INDIVIDUALS' TRAITS ON VIRTUAL COMMUNITY COHESION</b> .....	195
<i>Zulkhairi Md. Dahalin ; Nor Iadah Yusop ; Zahurin Mat Aji</i>	
<b>EXPLORING THE USABILITY, SECURITY AND PRIVACY TAXONOMY FOR MOBILE HEALTH APPLICATIONS</b> .....	201
<i>Norhidayah Asaddok ; Masitah Ghazali</i>	
<b>DESCRIPTIVE ANALYSIS AND TEXT ANALYSIS IN SYSTEMATIC LITERATURE REVIEW: A REVIEW OF MASTER DATA MANAGEMENT</b> .....	207
<i>Faizura Haneem ; Rosmah Ali ; Nazri Kama ; Sufyan Basri</i>	
<b>STRATEGIC INFORMATION SYSTEMS PLANNING FOR BUREAUCRATIC REFORM</b> .....	213
<i>Arfive Gandhi ; Yova Ruldeviyani ; Yudho Giri Sucahyo</i>	
<b>SENTIMENT ANALYSIS OF STUDENT FEEDBACK USING MACHINE LEARNING AND LEXICON BASED APPROACHES</b> .....	219
<i>Zarmeen Nasim ; Quratulain Rajput ; Sajjad Haider</i>	
<b>EXPLORING PUBLIC E-SERVICE SUSTAINABILITY: IN THE CASE OF MALAYSIA</b> .....	225
<i>Haslinda Sutan Ahmad Nawi ; Othman Ibrahim ; Azizah Abdul Rahman</i>	
<b>SUMMATIVE EVALUATION FOR DESIGN SCIENCE ARTIFACT USING STRUCTURED WALKTHROUGH</b> .....	231
<i>Nur Syufiza Ahmad Shukor ; Noorminshah A. Iahad ; Azizah Abdul Rahman</i>	
<b>MOBILE PAYMENT FRAMEWORK FOR THE UNBANKED FILIPINOS</b> .....	237
<i>Wardah Zainal Abidin ; Oliver Rivera ; Nurazeen Maarop ; Noor Hafizah Hassan</i>	
<b>FUZZY COGNITIVE MAPS BASED ON TEXT ANALYSIS FOR SUPPORTING STRATEGIC PLANNING</b> .....	243
<i>Petr Hajek ; Ondrej Prochazka ; Piotr Pachura</i>	

<b>BUILDING INFORMATION MODELLING TECHNOLOGICAL INNOVATIONS IN INDUSTRIALISED BUILDING SYSTEMS COST ESTIMATION .....</b>	<b>249</b>
<i>Mohamed Murteza Gulamhussein Moledina ; Goh Wei Pin ; Wallace Imoudu Enegbuma ; Kherun Nita Ali ; Kayode Adenuga</i>	
<b>SECURITY THREATS FOR BIG DATA .....</b>	<b>255</b>
<i>Tarannum Zaki ; Md. Sami Uddin ; Md. Mahedi Hasan ; Muhammad Nazrul Islam</i>	
<b>ANTECEDENTS OF EWOM IN SOCIAL COMMERCE.....</b>	<b>261</b>
<i>Sahabi Y. Ali ; Ab Razak Che Hussin ; Abdelsalam H. Busalim</i>	
<b>A FIRM AND INDIVIDUAL CHARACTERISTIC-BASED PREDICTION MODEL FOR E2.0 CONTINUANCE ADOPTION.....</b>	<b>267</b>
<i>Qiong Jia ; Fu Xin ; Yue Guo ; Stuart J. Barnes</i>	
<b>A MODEL OF INFORMATION SHARING PROCESS ON SOCIAL MEDIA .....</b>	<b>271</b>
<i>P. W. Handayani ; D. F. Alaika</i>	
<b>SOCIAL MEDIA ADOPTION FRAMEWORK FOR AGED CARE SERVICE PROVIDERS IN AUSTRALIA.....</b>	<b>277</b>
<i>Babak Abedin ; Shadi Erfani ; Yvette Blount</i>	
<b>A REVIEW ON BIM-BASED AUTOMATED CODE COMPLIANCE CHECKING SYSTEM .....</b>	<b>283</b>
<i>Aimi Sara Ismail ; Kherun Nita Ali ; Noorminshah A. Iahad</i>	
<b>UNDERSTANDING THE FORMATION OF KNOWLEDGE OUTCOMES IN VIRTUAL COMMUNITIES - A TRUST DEVELOPMENT PERSPECTIVE .....</b>	<b>289</b>
<i>Shu-Man Chen ; Chia-Shiang Hsu ; Shih-Wei Chou</i>	
<b>BIM-BASED SUSTAINABLE BUILDING DESIGN PROCESS AND DECISION-MAKING .....</b>	<b>295</b>
<i>Yaik-Wah Lim</i>	
<b>EXTENDED ERP FOR INVENTORY MANAGEMENT: THE CASE OF A MULTI-NATIONAL MANUFACTURING COMPANY .....</b>	<b>301</b>
<i>Ooi Chun Wei ; Rosnah Idrus ; Nasuha Lee Abdullah</i>	
<b>USE OF ICT IN INDIGENOUS PRIMARY SCHOOL CLASSROOM: A CASE STUDY OF TEACHERS' EXPECTATIONS AND EXPERIENCES .....</b>	<b>306</b>
<i>Norshakirah Aziz ; Norizzati Abdul Rahman</i>	
<b>ACADEMIC READINESS FOR BUILDING INFORMATION MODELLING (BIM) INTEGRATION TO HIGHER EDUCATION INSTITUTIONS (HEIS) IN MALAYSIA .....</b>	<b>310</b>
<i>Badiru Yunusa Yusuf ; Mohamed Rashid Embi ; Kherun Nita Ali</i>	
<b>UNDERSTANDING KNOWLEDGE MANAGEMENT BEHAVIOR FROM A SOCIAL EXCHANGE PERSPECTIVE .....</b>	<b>316</b>
<i>Chia-Shiang Hsu ; Hui-Tzu Min ; Shih-Wei Chou</i>	
<b>VALIDATING QUESTIONNAIRE DESIGN OF INFOSTRUCTURE MATURITY MODEL FOR DISASTER MANAGEMENT SELECTED PROCESSES .....</b>	<b>321</b>
<i>Aliza Abdul Latif ; Noor Habibah Arshad ; Norjansalika Janom ; Nor Shahniza Kamal Bashah ; Syaripah Ruzaini Syed Aris</i>	
<b>EXPLORING DEVELOPERS' UNDERSTANDING ON BUILDING INFORMATION MODELLING (BIM) AND ITS IMPACT ON RETURN ON INVESTMENT (ROI) .....</b>	<b>327</b>
<i>Aryani Ahmad Latiffi ; Ng Hua Tai</i>	
<b>WHAT REAL NAME DO YOU USE ONLINE? .....</b>	<b>332</b>
<i>Akiko Orita</i>	
<b>FRAMEWORK FOR EMBEDDING GAMIFICATION IN MASSIVE OPEN ONLINE COURSE (MOOC) .....</b>	<b>338</b>
<i>Nur Fatimah Abu Bakar ; Ahmad Fadhil Yusof ; Noorminshah A. Iahad ; Norasnita Ahmad</i>	
<b>INFLUENTIAL FACTORS FOR PATIENTS' ONLINE RATINGS OF GENERAL PRACTITIONERS.....</b>	<b>343</b>
<i>Dominic Denker ; Heiko Gewalt</i>	
<b>HEALTHCARE EMPLOYEES' PERCEPTION ON INFORMATION PRIVACY CONCERNS .....</b>	<b>349</b>
<i>Fiza Abdul Rahim ; Zuraini Ismail ; Ganthan Narayana Samy</i>	
<b>VERIFICATION CAPABILITIES FOR BUSINESS RULES MANAGEMENT IN THE DUTCH GOVERNMENTAL CONTEXT.....</b>	<b>355</b>
<i>Koen Smit ; Martijn Zoet ; Matthijs Berkhout</i>	
<b>CULTURAL DETERMINANTS OF RESEARCH COMMUNITY PARTICIPATION .....</b>	<b>361</b>
<i>Rabiah Eladwiah Abdul Rahim ; Nor'Ashikin Ali ; Juraifia Jais</i>	
<b>UNDERSTANDING THE FORMATION OF INTENTION KNOWLEDGE EXPLOITATION IN ELECTRONIC VIRTUAL COMMUNITY FROM ATTRACTION THEORY PERSPECTIVE .....</b>	<b>365</b>
<i>Ni-Wayan Masri ; Chia-Shiang Hsu ; Shih-Wei Chou</i>	

<b>AN AUTOMATED ADVISOR SYSTEM TO SUGGEST RESPONSE AFTER ANALYZING USER WRITINGS IN SOCIAL NETWORK.....</b>	<b>371</b>
<i>Deen Md. Abdullah ; Sara Binte Zinnat ; Rahnuma Tasmin ; Shibir Ahmed ; Mahamudul Hasan</i>	
<b>SUCCESS FACTORS MODEL FOR ICT SHARED SERVICES.....</b>	<b>377</b>
<i>Noreen Mhd Hashim ; Nazmona Mat Ali ; Norris Syed Abdullah ; Suraya Miskon ; Sharin Hazlin Huspi</i>	
<b>THE ROLE OF TECHNOLOGY IN BEHAVIOURAL CHANGE FOR DENGUE PREVENTION COMMUNITY ACTIVITY: A SYSTEMATIC REVIEW .....</b>	<b>383</b>
<i>Afzan Rosli ; Masitah Ghazali</i>	
<b>SCAFFOLDING PROGRESS MONITORING OF LNG PLANT MAINTENANCE PROJECT USING BIM AND IMAGE PROCESSING TECHNOLOGIES .....</b>	<b>389</b>
<i>Hung-Lin Chi ; Jian Chai ; Changzhi Wu ; Junxiang Zhu ; Xiangyu Wang ; Chongyi Liu</i>	
<b>LIMITATIONS AND FUTURE OF ELECTROCARDIOGRAPHY DEVICES: A REVIEW AND THE PERSPECTIVE FROM THE INTERNET OF THINGS .....</b>	<b>395</b>
<i>A. M. Khairuddin ; K. N. F Ku Azir ; P. Eh Kan</i>	
<b>IDENTIFYING PREDICTORS OF CONTINUANCE INTENTION ON SOCIAL MEDIA-BASED PHYSICAL ACTIVITY USING THE ANALYTIC HIERARCHY PROCESS METHOD .....</b>	<b>402</b>
<i>Nittee Wanichavorapong ; Ab Razak Che Hussin ; Ahmad Fadhil Bin Yusof</i>	
<b>EXPERIENCES OF BUILDING INFORMATION MODELLING (BIM) ADOPTION IN VARIOUS COUNTRIES .....</b>	<b>408</b>
<i>Nur Emma Mustaffa ; Rozana Mohamed Salleh ; Hamizah Liyana Binti Tajul Ariffin</i>	
<b>FACTORS AFFECTING PURCHASE INTENTION IN TOURISM E-MARKETPLACE .....</b>	<b>415</b>
<i>P. W. Handayani ; Z. Arifin</i>	
<b>A LATENT FACTOR MODEL BASED MOVIE RECOMMENDER USING SMARTPHONE BROWSING HISTORY .....</b>	<b>421</b>
<i>Dixon Prem Daniel R ; Rangaraja P Sundarraj</i>	
<b>WHAT DOES ‘LEADERSHIP’ ENTAIL IN PUBLIC SECTOR BPM INITIATIVES OF DEVELOPING NATIONS: INSIGHTS FROM AN INTERPRETATIVE CASE STUDY FROM SRI LANKA.....</b>	<b>427</b>
<i>Rehan Syed ; Erica French ; Wasana Bandara ; Glenn Stewart</i>	
<b>CIVIC NETWORKS, TECHNOLOGICAL AND INSTITUTIONAL SUPPORT TO BUILD EFFECTIVE DISASTER PREPAREDNESS MODEL .....</b>	<b>434</b>
<i>Dinesh Alawanthan ; Magiswary Dorasamy ; Murali Raman</i>	
<b>A PROPOSED FRAMEWORK: AN APPROPRIATION FOR PRINCIPLE AND PRACTICE IN INFORMATION TECHNOLOGY RISK MANAGEMENT .....</b>	<b>440</b>
<i>Urairat Maneerattanasak ; Nitaya Wongpinunwatana</i>	
<b>AN ONTOLOGY BASED FRAMEWORK TO SUPPORT MULTI-STANDARD COMPLIANCE FOR AN ENTERPRISE.....</b>	<b>446</b>
<i>Danny C. Cheng ; Nathalie Rose Lim-Cheng</i>	
<b>A METAMODEL FOR TOURIST INTENTIONS TO VISIT A DESTINATION USING SYSTEMATIC LITERATURE REVIEW .....</b>	<b>452</b>
<i>Hafiz Ishfaq Ahmad ; Alex Tze Hiang Sim ; Jee Mei Hee</i>	
<b>FACEBOOK AND YOUTUBE ADDICTION: THE USAGE PATTERN OF MALAYSIAN STUDENTS.....</b>	<b>458</b>
<i>Sedigheh Moghavvemi ; Ainin Binti Sulaiman ; Noor Ismawati Binti Jaafar ; Nafisa Kasem</i>	
<b>DISTRACTION OR NOT? INVESTIGATING THE RELATIONSHIP BETWEEN MOBILE SOCIAL NETWORK ENGAGEMENT AND TASK PERFORMANCE .....</b>	<b>464</b>
<i>Manli Wu ; Chuang Wang ; J. Leon Zhao ; Liang Liang</i>	
<b>THE IMPACT OF FACEBOOK USAGE ON ACADEMIC PERFORMANCE.....</b>	<b>469</b>
<i>Sedigheh Moghavvemi ; Ainin Sulaiman ; Azmin Azliza Aziz ; Phoong Seuk Wai</i>	
<b>NATIONAL CYBER SECURITY STRATEGIES FOR DIGITAL ECONOMY.....</b>	<b>474</b>
<i>Chooi Shi Teoh ; Ahmad Kamil Mahmood</i>	
<b>UNDERSTANDING RELATIONSHIPS BETWEEN LEARNERS AND GAME ENVIRONMENT OF EDUCATIONAL GAMES: HERMENEUTIC APPROACH .....</b>	<b>480</b>
<i>Mifrah Ahmad ; Lukman Ab. Rahim ; Noreen Izza Arshad</i>	
<b>CYBERBULLYING AMONG STUDENTS: AN APPLICATION OF THEORY OF PLANNED BEHAVIOR .....</b>	<b>486</b>
<i>Hosien Jafarkarimi ; Robab Saadatdoost ; Alex Tze Hiang Sim ; Jee Mei Hee</i>	
<b>FACTORS INFLUENCING SUCCESS OF INCREASING PARTICIPATION IN USING ELECTRONIC INFORMATION SHARING BETWEEN A YEMEN MINISTRY AND UNIVERSITY .....</b>	<b>491</b>
<i>Eman Maarof ; Huda Ibrahim</i>	

<b>A CONCEPTUAL MODEL FOR FLIPPED CLASSROOM: INFLUENCE ON CONTINUANCE USE INTENTION</b> .....	497
<i>Ireti Hope Ajayi ; Noorminshah A. Iahad ; Norasnita Ahmad ; Ahmad Fadhil Yusof</i>	
<b>PERCEPTION OF INTERNAL AUDITOR ON THE USE OF GENERALIZED AUDIT SOFTWARE</b> .....	503
<i>Rindang Widuri ; Nuraini Sari ; Aries Wicaksono ; Yen Sun ; Synthia Atas Sari</i>	
<b>DO PRIVATE AND SEXUAL PICTURES RECEIVE MORE LIKES ON INSTAGRAM?</b> .....	509
<i>Hyanghee Park ; Joonhwan Lee</i>	
<b>A CONCEPTUAL APPROACH FOR UNDERSTANDING COMPUTER PROGRAMMING SKILLS DEVELOPMENT</b> .....	515
<i>Asma Md Ali ; Afidalina Tumian ; Muhamad Sadry Abu Seman</i>	
<b>HOW DESIGN INVOLVEMENT IMPACTS DEAF CHILDREN</b> .....	520
<i>Jessica Korte ; Leigh Ellen Potter ; Sue Nielsen</i>	
<b>THE CRITICAL SUCCESS FACTORS (CSFS) OF SOCIAL CRM IMPLEMENTATION IN HIGHER EDUCATION</b> .....	526
<i>Meylana ; Bruno Sablan ; Achmad Nizar Hidayanto ; Eko K. Budiardjo</i>	
<b>ENTERPRISE SOCIAL MEDIA WITHIN MALAYSIAN COMPANY: USAGE IMPACTS AMONG EMPLOYEES</b> .....	532
<i>Nurul Syahira Binti Yasse ; Mohd Heikal Husin</i>	
<b>INFORMATION TECHNOLOGY DISASTER RECOVERY PROCESS IMPROVEMENT IN ORGANIZATION</b> .....	537
<i>Dinesh Alawanthan ; Magiswary Dorasamy ; Murali Raman</i>	
<b>SERVICE ORIENTED ARCHITECTURE ADOPTION MODEL FOR ICT OFFICE IN MALAYSIA</b> .....	543
<i>Wan Faezah Abbas ; Nur Hafizah Musa ; Kamalia Azma Kamaruddin ; Wan Nor Amalina Wan Hariri ; Haryani Haron</i>	
<b>FACTORS INFLUENCING KNOWLEDGE COMMUNICATION IN MALAYSIAN PUBLIC SECTOR</b> .....	549
<i>Rohaizan Daud ; Nor Zairah Ab Rahim ; Roslina Ibrahim</i>	
<b>FIRM PERFORMANCE THROUGH SOCIAL CUSTOMER RELATIONSHIP MANAGEMENT: EVIDENCE FROM SMALL AND MEDIUM ENTERPRISES</b> .....	555
<i>Ali Ahani ; Nor Zairah Ab. Rahim ; Mehrbakhsh Nilashi</i>	
<b>ENTREPRENEUR'S AMBIDEXTERITY, KNOWLEDGE BROKERAGE AND FIRM PERFORMANCE: PRELIMINARY FINDINGS</b> .....	561
<i>Nurul Afza Hashim ; Ching Seng Yap ; Rizal Ahmad ; Farah Waheeda Jalaludin</i>	
<b>USER ACCEPTANCE OF ON-DEMAND SERVICES</b> .....	566
<i>Jasmine A. L. Yeap ; Emily H. T. Yapp ; Chaaminy Balakrishna</i>	
<b>FACTORS INFLUENCING TO THE IMPLEMENTATION SUCCESS OF BIG DATA ANALYTICS: A SYSTEMATIC LITERATURE REVIEW</b> .....	572
<i>Cecilia Adrian ; Rusli Abdullah ; Rodziah Atan ; Yusmadi Yah Jusoh</i>	
<b>RESEARCHER'S PARTICIPATION IN E-COLLABORATION</b> .....	578
<i>Jamilah Mahmood ; Halina Mohamed Dahlan ; Ab Razak Che Hussin ; Muhammad Aliif Ahmad</i>	
<b>LITERATURE REVIEW ON TECHNOLOGY USAGE AND EMOTIONAL CONNECTION AMONG CHILDREN</b> .....	583
<i>Nur Fatini Ismail ; Mohd Hilmi Hasan ; Emy Elyanee Mustapha</i>	
<b>MOTIVATING CROWDWORKERS BY MANAGING EXPECTATIONS</b> .....	588
<i>Shakir Karim ; Umair Uddin Shaikh ; Zaheeruddin Asif</i>	
<b>PDEDUGAME: TOWARDS PARTICIPATORY DESIGN PROCESS FOR EDUCATIONAL GAME DESIGN IN PRIMARY SCHOOL</b> .....	592
<i>Rozana Ismail ; Roslina Ibrahim</i>	
<b>ORGANIZATION'S PERSPECTIVE OF MANAGING B2C E-COMMERCE IMPLEMENTATION: LESSONS FROM FASHION AND APPAREL BUSINESS IN MALAYSIA</b> .....	598
<i>Deborah Libu Paris ; Mahadi Bahari ; Noorminshah A. Iahad ; Haslina Hashim ; Waidah Ismail</i>	
<b>TOWARDS THE INVESTIGATION OF THE EFFECT OF CUSTOMER SATISFACTION AND CUSTOMER EXPERIENCE ON BEHAVIOURAL INTENTION IN MOBILE TELECOMMUNICATION SERVICES IN AUSTRALIA</b> .....	604
<i>Hassan Shakil Bhatti ; Ahmad Abareshi ; Siddhi Pittayachawan</i>	
<b>PROMOTING STUDENTS' ENGAGEMENT IN LEARNING PROGRAMMING THROUGH GAMIFICATION IN PEER-REVIEW DISCUSSION FORUM</b> .....	610
<i>Shahdatunnaim Azmi ; Norasnita Ahmad ; Noorminshah A Iahad ; Ahmad Fadhil Yusof</i>	

**FORECASTING MALAYSIAN EXCHANGE RATE USING MACHINE LEARNING  
TECHNIQUES BASED ON COMMODITIES PRICES ..... 616**  
*Suresh Ramakrishnan ; Shamaila Butt ; Muhammad Ali Chohan ; Humara Ahmad*  
**Author Index**

# *Detection and Prevention of Possible Unauthorized Login Attempts through Stolen Credentials from a Phishing Attack in an Online Banking System*

*Shammi Ishara Hewamadduma*

School of Computing, Asia Pacific Institute of Information Technology (APIIT),  
Colombo 2, Sri Lanka.  
shammishara@gmail.com

**Abstract**—With the current technological expansions customers wish to use online banking facilities due to its convenience and worldwide accessibility. The main challenge of going online for a bank is to provide sufficient security for the online customers and their accounts. The dramatic growth of the number of online banking customers has attracted cyber criminals and identity theft is a severe threat to online banking services. Phishing is a famous and easiest method to steal user credential of online customers where the sole intention is to obtain confidential information for the purpose of monetary gain. In such a situation the main purpose of this research paper is to analysis the usage of phishing attacks and the dangers it poses to customers and the bank, then to find out the available methods to detect and prevent unauthorized login attempts, the technologies and security weaknesses of those methods and finally to propose a solution to detect and prevent unauthorized login attempts using behavioral based analysis, IP and device identification technologies.

**Keywords** – *Phishing, Online banking systems, Anomaly based detection, Device Identification, IP Address Identification*

## I. INTRODUCTION

Providing security to a customer's financial information is vital and therefore banks and other financial institutes offer different security mechanisms to reduce the risk of unauthorized access to their online customer accounts. Most of the attacks on online banking systems are based on deceiving the user to reveal their login details and then the attacker will use those stolen credentials to gain unauthorized access to the customer accounts. Phishing attacks and social engineering methods are mostly used to deceive the online account users. As most of the phishing attacks are targeting the financial sector, protecting online banking systems from phishing attacks is a major concern. Failing to provide a proper security assurance will reduce the growth and damage the reputation of online banking services. Even though there are several researches already being carried out and commercial products are available to secure online banking systems, they have their own ups and downs. [7] Therefore proposing a method to prevent unauthorized login attempts in an online banking systems is a timely requirement and in this research a solution is proposed to detect and prevent possible unauthorized login attempts in an Online Banking System. In this research paper first it describes the literature review in the domain. Then the methodology, system implementation and test results will be presented.

## II. RELATED WORK

Initially some background survey has been carried out in order to study about the online banking facilities provided by banks. Then a study was carried out about different types of attacks that can be threats to the online banking services and has identified phishing attacks as the main threat to the online banking security. Therefore the study was mainly focused on phishing attacks. After that a study was carried out to find out different methods and solutions which are currently available to safeguard online banking customers from the fraudsters.

### A. Online Banking Facility

Internet banking provides users the facility to access their finance information and perform banking transactions regardless of normal banking hours. In order to access an online banking facility, usually a customer should first register with the online banking service provided by the bank and set up username and a password. Some of the banks use additional security steps for online banking, such as smart card readers which can generate codes, free security software and guidance to increase customer awareness.

### B. Phishing attacks on online banking systems

The concept of phishing is related to deceiving the customers to reveal their login credentials to attackers by masquerading as a trustworthy entity and the term first used by the hackers to describe stealing America Online (AOL) accounts by acquiring usernames and passwords.[9] But today it is becoming a huge threat to online banking security.

According to the Anti-Phishing Working Group (APWG), phishing attacks grew 20% in the third quarter of 2013. 31.45% of all phishing attacks in 2013 were targeted financial institutions. 22.2% of all attacks involved fake bank websites; the share of banking phishing doubled compared with 2012. 59.5% of banking phishing attacks exploited the names of 25 international banks. Estimated hard costs that result from phishing attacks range from \$300 to \$1,800 per compromised account record. There are also soft costs that cannot be easily quantified; such as the loss of customer trust and the erosion of brand value [1].

The above surveys clearly indicate that the most popular target of phishing attacks is happened to be banking industry.

### C. Currently available methods to safeguard online banking

Since it is very important to safeguard the online banking systems, there are different methods and mechanisms developed by organizations. The main action a financial institute is taking to protect their online customers is to educate the customer on online banking services security. This means the bank itself provide some advices and awareness to their online customers to make sure they will not be a victim of an online banking account compromise. The major advices are setting up a secured password, not to reveal their confidential credentials/information to anyone not even from the bank, information about phishing and scamming emails etc. [8]

Even though the banks try to educate their customers, some customers are deceived by the fraudsters to make them reveal their sensitive information. A method that the phishing attackers try to make it urgent to confirm customer credential is, send the phishing mails during bank holidays so that the customer will not have time to call the bank and verify the authenticity of the mail from the bank. Therefore financial institutes always attempt to identify the fraudulent activities before it harms their customers. [11]

Banks sometimes ask the customers to use card readers to reassure the user identity. This method enables the two factor authentication where user has to submit a code generated by the card reader other than the username and the password. In order to confirm a transaction the user should have the card reader, his Visa debit/credit card, and his PIN. This is the same PIN the user would use in an ATM or shop. If the user enters the PIN incorrectly more than three times in a row the card will be blocked. But it might be a burden to the customer as the customer cannot proceed with transactions without using the card readers. [10]

The banks sometimes use some commercial products like Guardian Analytics, ThreatMetrix, Actimize, and The Versafe TotALL to protect their customers from attackers.

### D. Anomaly based detection of frauds

Anomaly based detection is the process of detecting an unusual or suspected behaviour of a user or a system relative to its expected or normal behaviour [2].

According to an electronic document published by Aleksandar Lazarević, anomaly detection techniques based on employed techniques can be classified into the following five groups. [3]

Statistical Methods - Detects the abnormalities of users or systems by monitoring the behaviour over a time period by measuring certain variables (e.g. login and logout time of each session), Distance based Methods – More advanced than statistical method and uses algorithms to detect outliers by computing distances among points, Rule based systems – Abnormal behaviours are detected based on pre-defined set of rules, Profiling Methods – A profile is created based on the normal behaviour and deviations from that profile are considered as intrusions, Model based approaches – Models are defined based on the normal behaviour and anomalies are detected as deviations from the model that represents the normal behaviour [3].

Amavised-new is a spam filter which is integrated with SpamAssassin. SpamAssassin. It provides spam filtering, including feature recognition, and Bayesian learning mechanisms. Feature recognizers check for the previously identified spam patterns or spam symptoms in the headers or the body of the e-mail. The example spam symptoms can be a header date contains a twelve hours in the future or the mail contains an image without text. A mail having more than a thousand of words is more possible to be a ham. SpamAssassin also checks the mail server's or clients IP address against a number of DNS-based block lists (DNSBLs) to make sure it is not a known spam source. SpamAssassin also provides a Bayesian learning mechanism, which is an automated, feature recognizer. Bayesian approach attempts to pick out email features automatically, and identify spams based on an analysis of the spam and ham the user has received previously. [4]

### E. Other methods to safeguard online banking systems

Other than the commercially available products the banking websites and also some commercial websites use different methods to safeguard their users and confirm the identity of them.

Facebook performs access control through two security tools, Login approvals and Login Notifications. If the user tries to login to the account using a different device, a security code will be sent to a pre-registered phone number. In order to get the access user should enter the received security code with the username and the password. Also that action will be informed to the user via Login Notifications. In order to identify the devices Facebook uses Cookies [5].

In some of the online sites the Two-factor authentication is enabled as a second level of authentication. Twitter, Apple, Google, Microsoft, Facebook, and Amazon support Two-factor authentication for a while.

### F. Current situation of online banking systems

When it comes to Sri Lanka, the security measures provided by some of the Sri Lankan banks are listed below.

HSBC – Uses a security device to enable two factor authentication and one time password of protection. Commercial Bank – Has enabled 128-bit encryption, two-factor authentication, password protection and multiple levels of authorization. National Development Bank (NDB) - Offers 128-bit encryption, and multi-layered security architecture with firewalls, filtering routers, and digital certification from the VeriSign Inc.

Although all those encryptions are used for secure communications but once a user name and password is stolen, those encryptions will not be helpful. All the online banking sites provide security messages to advice/inform their customers about phishing attacks and other security related matters that the customers should be aware of. A special unit is also set up in the Criminal Investigation Department as Counterfeit Currency Bureau (CIB) to look into these financial frauds and especially to investigate into credit and debit card frauds [6].

According to the carried out investigations, the Sri Lankan banks do not have methods to detect the unauthorized login

attempts. Once a security breach is disclosed most of the time banks reimburse the loss to the account holder to keep the customer satisfaction. And some of the banks seek to recover the damage via insurance companies. But if the contract between the user and the bank at the account opening does not mention that it covers the loss due to cyber-attacks, the bank is not legally obliged to compensate the customer's losses. Especially if a phishing attack is carried out against a bank they do not have any method to identify that attack until they get a complaint from their customers.

### III. METHODOLOGY

In this study an effort is provided for a reliable and a trustworthy solution to safeguard the genuine customer accounts from fraudsters and to mitigate unauthorized login attempts. In the proposed solution the researcher's effort is to implement layered security architecture. From here onwards the suggested mechanism of the researcher will be discussed.

#### A. How the system works

The system mainly depends on identifying the abnormalities of user behaviour.

##### Step 1

In the proposed solution, at the time a customer sends a login request, the IP address, device, cookie, time of the day, location, the operating system and the browser are considered in order to detect anomalies. Those factors are used to identify the customers at the initial step. Based on initial identification a personal profile is created and stored in the database.

##### Step 2

Based on the mentioned factors the users are compared with the personal profile which is in the system database, from the next login attempt onwards. If there are no anomalies detected and all the factors are compatible with the profile, access will be allowed. But if there are some anomalies, based on the weight level security mechanism will be carried out. This security mechanism includes an automated email notification system, security question and a security code. Based on the security mechanism access will be allowed or denied.

##### Step 3

Even all the security steps are completed the customer behaviour will be further monitored in order to detect anomalies.

The available products are mostly based on a single solution only. But the main strengths of the proposed solution are, it combines the anomaly based detection, Device identification and IP address identification methods to differentiate genuine users from the fraudsters. Through this the unauthorized login attempts can be identified even though the attacker provides the correct login credentials.

### IV. IMPLEMENTATION

Since anomaly based detection, Device identification and IP address identification technologies are the most important concepts that are used to develop the solution, those will be discussed in detail in the next sections.

#### A. Anomaly Based Detection

In anomaly based detection the normal behaviour of a particular customer will be detected and logged for a particular period of time. When a user initially starts to use the online banking facility, the person will be asked to provide some details at the registration process. From the details they have provided, the user's temporary profile can be created. But the most suitable way to identify a particular user is by analysing his behaviour for a predefined time period. For behavioural identification several facts will be considered.

The login country, login times, browser used to login, usual amount of transactions can be identified for each and every user individually. Then these details will be maintained inside the local database. Using those details a profile will be generated for every user. If abnormal action which is different to the profile behaviour is detected by the bank then it might be a possible unauthorized login attempt. If a particular user's login attempts are recorded from different countries within a very short period of time where the person will not have enough time to travel can be a possible unauthorized login attempt. Also if the user needs to use his online banking system abroad he should inform this to the bank. If not the bank will not allow that user to login online banking system from different countries.

The password which is selected at the registration process will be hashed for security purposes before saved in the database. There is a security question that the user should select and answer at the registration. This will be stored in the database and will be used to secure the account. Once the registration is completed a confirmation email will be sent to the email address which is given at the registration.

In order to create a behaviour based profile, the normal behaviour of that particular user will be detected and logged for a particular period of time. The period depends on the requirement of the bank, customer's usage pattern and how often customer uses the system. Then the system can use a data clustering method to categorize the users based on their activities. Some data categorization method such as K-means algorithm can be implemented and used to create the ultimate more specific user profile.

Once the user profile is generated for a specific user it will be kept saved in the database as authorized users. Then when a specific customer is trying to log in to the system the login details such as login country, times, browser, amount of transaction will be obtained and the obtained information will be compared with the user profile which is stored in the database. At the validation if the system does not detect any deviations, then the user will be identified as an authorized user. If an anomaly is detected then the security question will be asked for the verification and if the customer's answer is correct then login will be allowed. But the login attempt is suspicious, transactions will be monitored further. Anyway since the behaviour is detected as abnormal, a notification will be sent to the authorized user about the login attempt. Also all the successful and failed login attempts will be logged in the database for future references.

#### B. Device Identification

When a customer is registering with the online banking facility the device he used will be identified and tracked using

a cookie. That means using the installed cookie the device can be identified every time the user try to log-in. But if the user uses a different device which cannot be identified as the authorized device then a notification will be sent to the genuine customer. Also at the same time user has to answer the security question in order to proceed with the login attempt. Then if the user answers the security question successfully then the access will be permitted. If the customer wishes to save the new device as an authorized device he can install the cookie in the new device and make it as an authorized device as well.

### C. IP Address Identification

Once the user tries to login in to his online bank account users' IP address will be identified. Then the IP address will be validated. For an example if a particular user always login to his account from a local IP Address range and suddenly he tried to log in from a foreign IP Address that might be a possible unauthorized login attempt. So the IP Address will be checked and if it is a suspicious IP, access will be blocked and transactions will be stopped. There are known malicious IP Address ranges. These known malicious IPs are predefined in the system itself. If the system detects a login attempt from such IP Address then that attempt will be blocked immediately and the genuine user will be notified via an email.

Once a login attempt is suspicious according to the defined rules based on the situation the user will be asked to answer the security question. If the user answers the question successfully then he will be able to proceed with the login. But if the user is unable to answer the security question or the attempt is identified as an unauthorized attempt the login will be blocked and the genuine user will be notified immediately via an email or a text message via a pre-defined mobile number and an email address.

### D. System Functionality

- Verifying Valid and Invalid Login Attempts

At the time a user tries to log in, the username will be checked with the password. If the username does not match with the password then the login will not be allowed.

- Storing User Passwords

Ensuring the secrecy of user passwords is one of the most critical aspects in online banking; every user password found in the online Banking system is stored in the system using encrypted MD5 hash.

	FirstName	LastName	Email	UserName	Password	Co
1	Ruwan	Ananda	ruwan.a@sbsl.lk	ruwan.a	03941b924d12454219648d61a7b025e1	NU
2	Shama	Dilani	shama.s@sbsl.lk	shama.s	cbf6d70c20a02e58e25a5b52fde6bdad	NU

Fig. 1. Hashed passwords stored in backend database

Even if the username matches with the password then as a background process the login process will be checked for the anomalies. Firstly the device will be verified. For that the device identification will be performed using the cookie. If the device is identified as an authorized device then it will proceed

to the next level. If the system cannot identify the device then the user will be asked to answer the security question. If he is able to answer the question then the system will proceed again to the next level. If the user cannot answer the security question then a notification will be sent to the authorized user's predefined email address or a phone number.

If the device is identified as an authorized device then the backend user profile will be compared with the current user credentials. IP address identification and anomaly based detection is performed in this step. If there is no suspicious action is detected, user will be allowed to progress with transactions or if some suspicions rise up then the user will be blocked and notifications will be sent to predefined email address or a phone number.

- Detection of abnormality of a Login in user

After the detection of an abnormality of certain factor of a login in user, security actions can be performed accordingly. For each and every factor the weights can be assigned according to the importance. For the proposed sample system following actions is taken according to the abnormality of factors. Here the IP address and the cookie are considered as major factors.

TABLE 1

SECURITY ACTIONS FOR LOGIN IN USER ANOMALIES

IP	Device	Cookie	Time	OS	Browser	Action
√	√	√	√	√	√	Allow
√	√	√	√	x	x	Security Question
x	√	√	√	√	√	Security Question
x	x	x	√	√	√	Security Question + Code
x	x	x	x	x	x	Block + Email notification

As mentioned in the Table 1 security actions can be taken according to the deviations of the factors. Here for the cookie and the IP address more weightage is assigned as those factors can be considered as more important according to the literature study.

## V. RESULTS

As the test case, sample of 25 users is selected.

### A. Registering of a new user

First of all a new user should be registered with the online banking system. For that purpose user should visit the registration page and enter the required details. Once the user click on the submit button, user details will be sent to the database and user will be saved as an authenticated user. Figure 2 shows the database entry for the registered user. At the same time an email will be sent to the provided email address in the registration form confirming the registration.

For registration users are asked to use their own devices and secure internet connection. Out of the 25 all the 25 users were successfully got registered with the system and 25 out of 25 users received the confirmation email. The database entries for the new users are shown in Figure 2.

FirstName	LastName	Email	Contact	UserName	Password
Nirupama	Bandara	shammishara@gmail.com	0771234567	nirupama.b	29c42773cb16bffe8cc141d8c
Priyankara	Perera	wsvperera@gmail.com	0711223456	priyankara.p	1adbb3178591fd5bb0c24851
Kamal	Perera	shammishara@gmail.com	0713456734	kamal.p	2b2af08c09f1de8e69377c03c
Shanika	Bandara	shammishara@gmail.com	0711213432	Shanika.b	2b2af08c09f1de8e69377c03c
Ruwantha	Perera	ruwantha1993@gmail.com	0771523345	ruwantha.p	6572bdaff799084b973320f4

Fig. 2. Database entry of the new user

Once the registration is completed the user can use the selected username and the password to login into the online banking system. Once the user tries to login to the system for the first time the system will ask the security question in order to identify the user. Figure 3 shows the security question that is asked by the user at the first login attempt.

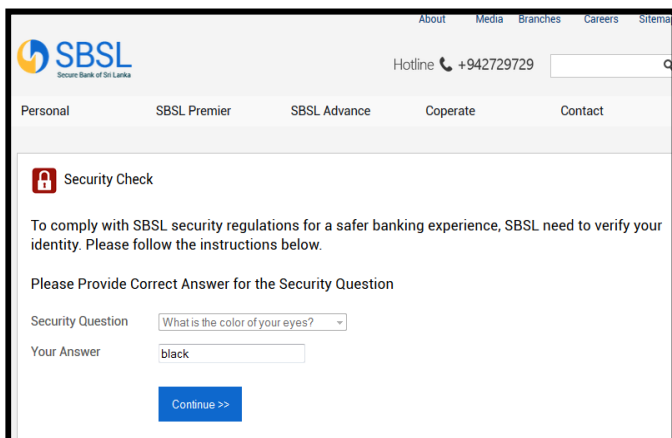


Fig. 3. Security question

If the user is able to answer the question he will be allowed and an entry will be made in the database as a successful attempt. If he could not provide the details properly he will not be allowed to login in and an entry will be made in the database as a failed login attempt.

Out of 25 sample test cases 5 users' security questions were answered wrong. Therefore in the database, 5 login attempt entries were logged as failed attempts and other 20 login attempt entries were logged as successful attempts.

### B. System Logs

When a client PC is connected to the banking website, logs will be made on the backend web server. The format of a single log record is as follows.

“Username <tab> Date <tab> Time <tab> IP address <tab> Operating System”

Figure 4 shows the log results for the selected sample users which have already in the system, and which will be using to validate users at the time they try to login in to the system.

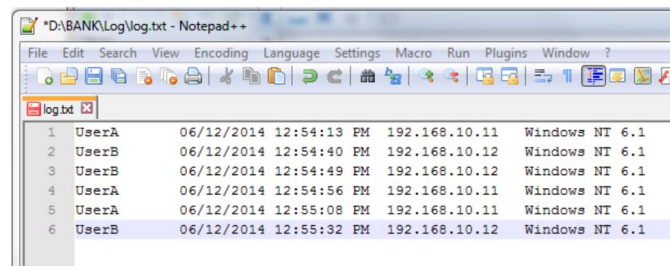


Fig. 4. Sample log results of users

### C. Detection of anomalies

If user tries to log in to online banking web interface with an IP address which is not listed in current logs or with an Operating System which is not listed, it can be detected by log analysis. The researcher has automated this task in backend logic web server. Once this type of anomaly is detected by the system will automatically prompt the security question. If the customer is able to answer the question successfully access will be allowed. But still logs will be made in the database as with the login details.

In order to test this function 10 user accounts were used out of the 25 sample user accounts. The 10 user accounts were tested with different anomalies. 4 accounts were logged in with different IP addresses which is not listed in the user's personal profile. Another 4 accounts were logged in with different operating systems which is not listed in the user's personal profile. Then the other 2 accounts were logged in with different browsers which is not listed in the user's personal profile.

In all the above login attempts the system was able to detect the anomalies and prompted the security question to the user. Only if the correct answer is given, the system allowed the login. As the testing in the above mentioned 10 accounts for 5 test cases correct answers were given and for the rest of the 5 accounts wrong answers were given. Whenever the correct answer is given, the system allowed the user login and whenever the wrong answer is given it denied and block the login attempt.

### D. Device identification

Once the registration is over a cookie will be saved in the customer's device at the first login attempt. The saved cookie will be expired after 10 days because of the security purposes. If the system can find the cookie in the device, the device can be identified as an authorized device. If the system could not find the cookie in the device the user has to answer the security question and/or has to provide the security code that is sent to the user's phone number based on the situation and install the cookie before proceed.

For testing purposes out of the 25 sample accounts 5 account were logged in without the cookie and another 5 accounts were logged in with expired cookies. In all the 10 cases security codes were sent to pre-define mobile phone numbers and in

order to proceed the user had to provide the correct security code to the system.

### E. Discussion of Results

When the system detects any abnormal login attempts on a given user account, the original user got notified via automated e-mail notification as soon as possible. This e-mail instructs the original user to change his/her login password as soon as possible. This situation was tested for the abnormalities in IP address, operating system, web browser and cookie file. Even though the provided username and password is matched the system was able to detect the introduced anomalies. Also in the cases where user was failed to answer the security question, login was blocked and a verification code was sent to the registered phone number. To enter the code user was given only one attempt. In the cases where the user was able to provide the code then the system allowed the login attempt. But these attempts were all notified to the user and the bank via emails.

Figure 5 shows the security code verification process carried out by the system in order to identify the user.

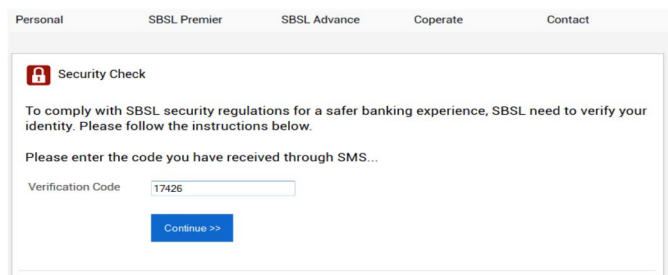


Fig 5. Security code verification

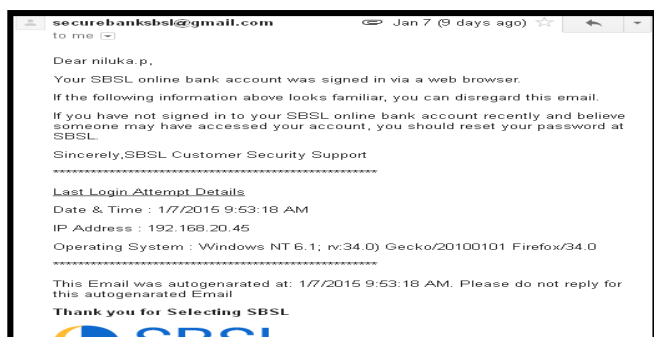


Fig 6. E mail notification

Figure 6 shows the email notification which is sent to the authorized customer informing the suspicious activity.

## VI. CONCLUSION

As discussed so far by the final solution the researcher was able to tackle the research problem properly. The research question “How to detect and prevent possible unauthorized login attempts through stolen details from a phishing attack in an online banking system?” “ was finally answered by the suggested solution using three mechanisms successfully. The

three mechanisms can be classified an anomaly based detection, IP address identification and device identification.

The overall system will not only detect the unauthorized login attempts but also prevent it, notified to authorized users and safeguard online banking customers from fraudsters.

This solution will safeguard online customers as well as financial institutes. Sometimes if a fraud is carried out against a bank especially via a phishing attack the customers will be reimbursed the loss to maintain bank’s reputation which is again a burden and a loss for the bank. Therefore this solution can be considered as a great improvement of online banking security. Also according to the researcher’s findings Sri Lankan banks do not use any methods to detect and prevent unauthorized login attempts. If a fraudster finds out a username and a password he will be able to login to the account posing as a legitimate customer. By this solution that type of incidents can be mitigated.

## ACKNOWLEDGMENT

I would like to express my sincere gratitude to Eng. Roshan Chandraguptha for his continuous support and insightful comments. I wish to mention Mr. Priyankara Perera for helping me throughout this project. I am truly grateful to my family for their encouragement, motivation and love.

## REFERENCES

- [1] PHISHLABS, “How to Fight Back against Phishing - A guide to mitigating and deterring attacks targeting your customers,” Ecrime Management Strategies, Inc, 2013. [Online] Available from: <http://f6ce14d4647f05e937f4d6abce208e5e17c2085b466b98c2083.r3.cfl.rac.kcdn.com/how-to-fight-back-against-phishing-pdf-3-w-935.pdf> [Accessed: 20 Sep 2014]
- [2] Guardian Analytics. “A Practical Guide to Anomaly Detection Implications of meeting new FFIEC minimum expectations for layered security” [Online] Available from: <https://www.aba.com/Tools/Others/Documents/Guardian-PracticalGuidetoAnomalyDetection.pdf> [Accessed: 08 Jan 2015]
- [3] Aleksandar Lazarevic, “Anomaly Detection / Outlier Detection in Security Applications” [Online] Available from: [http://www-users.cs.umn.edu/~aleks/anomaly\\_detection.htm](http://www-users.cs.umn.edu/~aleks/anomaly_detection.htm) [Accessed: 25 Nov 2014]
- [4] Robert LeBlanc, “Beating Spam and Viruses with amavisd-new and Maia Mailguard” [Online] Available from: <http://www.linuxjournal.com/article/7427?page=0,0>
- [5] ikawnoelastic thoughts, “Facebook Security: Use Login Notifications to Watch for Unauthorized Access,” [Online] Available from: <http://ikawnoelastic.com/social-media/facebook-security-use-login-notifications-to-watch-for-unauthorized-access/> [Accessed: 24 Nov 2014].
- [6] Wikipedia. “Actimize”, 21 May 2014. [Online] Available from: <http://en.wikipedia.org/wiki/Actimize> [Accessed: 6 Nov 2014].
- [7] LongfeiWu et al., “Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms,” in *IEEE Transactions On Vehicular Technology*, 2016, pp. 6678-6691.
- [8] Ibrahim Waziri Jr., “Website Forgery: Understanding Phishing Attacks & Nontechnical Countermeasures,” in *IEEE 2nd International Conference on Cyber Security and Cloud Computing*, 2015, pp. 445-450.
- [9] Surbhi Gupta et al., “A Literature Survey on Social Engineering Attacks: Phishing Attack,” in *International Conference on Computing, Communication and Automation (ICCCA2016)*, 2016, pp. 537-540.
- [10] A.A. Ghorbani et al., “Detection Approaches” in *Network Intrusion Detection and Prevention: Concepts and Techniques*, 2010.ch.2, pp. 27-53
- [11] SANS Institute, “Phishing: An Analysis of a Growing Problem”, 2007. [online] Available from: <https://www.sans.org/reading-room/whitepapers/threats/phishing-analysis-growing-problem-1417> [Accessed: 23 May 2017].