New Axioms in Topological Spaces

Vivekananda Dembre
Assistant Professor
Department of Mathematics,
Sanjay Ghodawat University,
Kolhapur,India

Abstract: In this paper, we study some separation axioms namely, w-To-space, w-T1 -space and w-T2-space and their properties. We also obtain some of their characterizations.

Keywords: W-TO-Space, W-T1 –Space, W-T2-Space.

1. INTRODUCTION

In the year 2000,Sheik John introduced and studied w-closed and w-open sets respectively. In this paper we define and study the properties of a new topological axioms called w-To-space, w-T1 –space, w-T2-space.

II.PRELIMINARIES

Throughout this paper space (X,τ) and (Y,σ) (or simply X and Y) always denote topological space on which no separation axioms are assumed unless explicitly stated. For a subset A of a space X, Cl(A), Int(A), A^c, P-Cl(A) and P-int(A) denote the Closure of A, Interior of A , Compliment of A, pre-closure of A and pre-interior of (A) in X respectively.

Definition 2.1: A subset A of a topological space (X, τ) is called

Definition 2.1: A subset A of a topological space (X, τ) is called

(i)A ωeakly closed set (briefly, ω-closed set) if $Cl(A)\subseteq U$ whenever $A\subseteq U$ and U is open in (X, τ).

(ii)A subset A of a topological space (X,τ) is called ωeakly open(briefly ω-open) set in X if A^c is ω-closed in X.

(iii)A topological space X is called a τ_w space if every w -closed set in it is closed.

Defintion 3: A map $f:(X, \tau)$ -» (Y, σ) is called

(i) W-continuous map [1] if $f^{-1}(v)$ is w closed in (X,τ) for every closed V in (Y,σ).

(ii)W-irresolute map[1]if $f^{-1}(v)$ is w closed in $(X,\tau)$for every w-closed V in (Y,σ).

(iii)W-closed map[1] if $f^{-1}(v)$ is w closed in (X,τ) for every closed V in (Y,σ).

(iv)W-open map[1] if $f^{-1}(v)$ is w closed in (X,τ) for every closed V in (Y,σ).

4. W-TO-SPACE:

Definition 4.4.1: A topological space (X, τ) is called w-T_o-space if for any pair of distinct points x,y of (X,τ) there exists an w-open set G such that $x\in G$, $y\notin G$ or $x\notin G$, $y\in G$.

Example 4.4.2: Let $X = \{a, b\}$, $\tau =\{\varphi,\{b\}, X\}$. Then (X, τ) is w-T_o-space, since for any pair of distinct points a, b of (X,τ) there exists an w-T_o open set {b} such that a $\notin\{b\}$,$b\in\{b\}$.

Remark 4.4.3: Every w-space is w-T_o-space.

Theorem 4.4.4: Every subspace of a w-T_o-space is w-T_o-space.

Proof: Let (X,τ) be a w-T_o-space and (Y,τ_y) be a subspace of (X,τ). Let $Y_1$and Y_2 be two distinct points of (Y,τ_y). Since (Y,τ_y) is subspace of (X,τ),Y_1 and Y_2 are also distinct points of (X,τ). As (X,τ) is w-T_o-space , there exists an w-open set G such that $Y_1\in G$, $Y_2 \notin G$. Then $Y\cap G$ is w-open in (Y,τ_y) containing but Y_1 not Y_2. Hence (Y,τ_y) is w-T_o-space.

Theorem 4.4.5: Let f: (X,τ) -» (Y, μ) be an injection, w-irresolute map. If (Y,μ) is w-T_o-space, then (X,τ) is w-T_o-space.

Proof: Suppose (Y, μ) is w-T_o-space. Let a and b be two distinct points in (X,τ).

As f is an injection f(a) and f(b) are distinct points in (Y,μ). Since(Y,μ) is w-T_o-space, there exists an w-open set G in (Y,μ) such that $f(a)\in G$ and $f(b)\notin G$. As f is w-irresolute, $f^{-1}(G)$ is w-open set in (X,τ) such that $a\in f^{-1}(G)$ and $b\notin f^{-1}(G)$. Hence (X,τ) is w-T_o-space.

Theorem 4.4.6: If (X,τ) is w-T_o-space, Tw-space and (Y,τ_y) is w-closed subspace of (X,τ), then (Y,τ_y) is w-T_o -Space.

Proof: Let (X,τ) be w-T_o-space, Tw-space and (Y,τ_y) is w-closed subspace of (X,τ). Let a and b be two distinct points of Y. Since Y is subspace of (X,τ), a and b are distinct points of (X,τ). As $(X,\tau)$is w-T_o -space, there exists an w-open set G such that $a\in G$ and $b\notin G$. Again since (X,τ) is Tw-space, G is open in (X,τ).Then $Y\cap G$ is open. So $Y\cap G$ is w-open such that $a\in Y\cap G$ and $b\notin Y\cap G$. Hence (Y,τ_y) is W-T_o –space.

Theorem 4.4.7: Let f: (X,τ) -» (Y, μ) be bijective w-open map from a w-T_0 Space (X,τ) onto a topological space (Y,τ_y). If (X,τ) is T_w-space, then (Y, μ) is w-T_0 Space.

Proof: Let a and b be two distinct points of (Y,τ_y). Since f is bijective, there exist two distinct points e and d of (X,τ) such that f(c) = a and f(d) = b. As (X,τ) is w-T_0 Space,there exists a w-open set G such that $c\in G$ and $d\notin G$. Since (X,τ) is T_w-space, G is open in (X,τ). Then f(G) is w-open in (Y, μ), since f is w-open, such that $a\in f(G)$ and $b\notin f(G)$. Hence (Y,τ_y) is w-T_0-space.

Definition 4.4.8: A topological space (X,τ) is said to be w-T_1-space if for any pair of distinct points a and b of (X,τ) there exist w-open sets G and H such that $a\in G$, $b\notin G$ and $a\notin H$, $b\in H$.

Example 4.4.9: Let X = {a,b} and τ = {$\emptyset$,{a},X}. Then (X,τ) is a topological space. Here a and b are two distinct points of (X,τ), then there exist w-open sets {a},{b} such that $a\in\{a\}$, $b\notin\{a\}$ and $a\notin\{b\}$, $b\in\{b\}$. Therefore (X,τ) is w-T_0 space.

Theorem 4.4.10: If (X,τ) is w-T_1-space,then (X,τ) is w-T_o-space.

Proof: Let (X,τ) be a w-T_1-space. Let a and b be two distinct points of (X,τ). Since (X,τ) is w-T_1-space, there exist w-open sets G and H such that $a\in G$, $b\notin G$ and $a\notin H$, $b\in H$. Hence we have $a\in G$, $b\notin G$. Therefore (X,τ) is w-T_o-space.

The converse of the above theorem need not be true as seen from the following example.

Example 4.4.11: Let X = {a,b} and τ ={φ,{b},X}. Then (X,τ) is w-T_o-space but not w-T_1-space. For any two distinct points a, b of X and an w-open set {b} such that $a\notin\{b\}$, $b\in\{b\}$ but then there is no w-open set G with $a\in G$, $b\notin G$ for $a\neq b$.

Theorem 4.4.12: If f: (X,τ) -» (Y,τ_y) is a bijective w-open map from a w-T_1-space and T_w-space (X,τ) on to a topological space (Y,τ_y), then$(Y,\tau_y)$is w-T_1-space.

Proof: Let (X,τ) be a w-T_1-space and T_w-space. Let a and b be two distinct points of (Y,τ_y). Since f is bijective there exist distinct points c and d of (X,τ) such that f(c) = a and f(d) = b. Since (X,τ) is w-T_1-space there exist w-open sets G and H such that $c\in G$, $d\notin G$ and $c\notin H$, $d\in H$.

Since (X,τ) is T_w-space, G and H are open sets in (X,τ) also f is w-open f(G) and f(H) are w-open sets such that a = f $(c)\in f(G)$, b = $f(d)\notin f(G)$ and a= $f(c)\notin$ f(H), b= $f(d)\in f(H)$. Hence (Y,τ_y) is w-T_1-space.

Theorem 4.4.13: If (X,τ) is wT_1 space and T_w-space, Y is a subspace of (X,τ), then Y is w-T_1 space.

Proof: Let (X,τ) be a w T_1 space and T_w-space. Let Y be a subspace of (X,τ). Let a and b be two distract points of Y. Since $Y\subseteq X$, a and b are also distinct points of X. Since (X,τ) is w-T_1-space, there exist w-open sets G and H such that $a\in G$, $b\notin G$ and $a\notin H$, $b\in H$. Again since (X,τ) is T_w-space,G and H are open sets in (X,τ), then $Y\cap G$ and $Y\cap H$ are open sets so w-open sets of Y such that $a\in Y\cap G$, $b\notin Y\cap G$ and $a\notin Y\cap H$, $b\in Y\cap H$. Hence Y is w T_1 space.

Theorem 4.4.14: Iff: (X,τ) -» (Y,τ_y) is injective w-irresolute map from a topological space (X,τ) into w-T_1-space(Y,τ_y), then $(X,\tau)$is w-T_1 - space.

Proof: Let a and b be two distinct points of (X,τ). Since f is injective, f(a) and f(b) are distinct points of (Y,τ_y). Since(Y,τ_y) is w-T_1 space there exist w-open sets G and H such that $f(a)\in G$, $f(b) \notin G$ and $f(a) \notin H$, $f(b)\in H$.Since f is w-irresolute, $f^{-1}(G)$ and $f^{-1}(H)$ are w-open sets in (X,τ) such that $a\in f^{-1}(G)$, $b \notin f^{-1}(G)$ and $a\notin f^{1}(H)$, $b\in f^{-1}(H)$. Hence (X,τ) is w-T_1 space.

Definition 4.4.15: A topological space (X,τ). is said to be w-T_2- space (or T_w-Hausdorff space) if for every pair of distinct points x, y of X there exist T_w-open sets M and N such that $x\in N$, $y\in M$ and $N\cap M = \emptyset$.

Example 4.4.16: Let X = {a,b}, τ = {$\emptyset$,{a},{b}, X}. Then (X,τ) is topological space. Then (X,τ) is w-T_2-space. T_w-open sets are $\emptyset$, {a}, {b},and X. Let a and b be a pair of distinct points of X, then there exist T_w - open sets {a} and {b} such that $a\in\{a\}$, $b\in\{b\}$ and $\{a\}\cap\{b\} = \emptyset$. Hence (X,τ) is w-T_2-space.

Theorem 4.4.17: Every w-T_2- space is w T_1space.

Proof: Let (X,τ) be a w-T_2- space. Let x and y be two distinct points in X. Since (X,τ) is w-T_2- space, there exist disjoint T_w-open sets U and V such that $x\in U$, and $y\in V$. This implies, $x\in U$, $y\notin U$ and $x\in V$, $y\notin V$. Hence (X,τ) is w-T_2-space.

Theorem 4.4.18: If (X,τ) is w-T_2-space, T_w- space and (Y,τ_y) is subspace of (X,τ), then (Y,τ_y) is also w-T_2-space.

Proof: Let (X,τ), be a w-T_2 - space and let Y be a subset of X. Let x and y be any two distinct points in Y. Since $Y\subseteq X$, x and y are also distinct points of X. Since $(X,\tau)$is w-T_2 - space, there exist disjoint T_w-open sets G and H which are also disjoint open sets, since (X,τ) is T_w - space. So $G\cap Y$ and $H\cap Y$ are open sets and so T_w- open sets in (Y,τ_y). Also $x\in G$, $x \in Y$ implies $x\in G\cap V$ and $y\in H$ and $y\in Y$ this implies $y \in Y\cap H$, since $G\cap H = \emptyset$, we have $(Y\cap G)\cap(Y\cap H) = \emptyset$. Thus $G\cap Y$ and $H\cap Y$ are disjoint T_w-open sets in Y such that $x\in G\cap Y$, $y\in H\cap Y$ and $(Y\cap G)\cap(Y\cap H)= \emptyset$. Hence (Y,τ_y) is w-T_2 - space.

Theorem 4.4.19: Let (X,τ), be a topological space. Then (X,τ),is w-T_2-space if and only if the intersection of all T_w-closed neighbourhood of each point of X is singleton.

Proof: Suppose (X,τ), is w-T_2-space. Let x and y be any two distinct points of X. Since X is w-T_2-space, there exist open sets G and H such that $x\in G$, $y\in H$ and $G\cap H = \emptyset$.Since $G\cap H = \emptyset$ implies $x\in G\subseteq X-H$. SoX-H is T_w-closed neighbourhood of x, which does not contain y. Thus y does not belong to the intersection of all T_w-closed neighbourhood of x. Since y is arbitrary, the intersection of all T_w-closed neighbourhoods of x is the singleton {x}.

Conversely, let (x) be the intersection of all T_w-closed neighbourhoods of an arbitrary point $x\in X$. Let y be any point of X different from x. Since y does not belong to the intersection, there exists a T_w-closed neighbourhood N of x such that $y\notin N$. Since N is T_w-neighbourhood of x, there exists an T_w-open set G such $x \in G\subseteq X$. Thus G and X - N are T_w-open sets such that $x\subseteq G$, $y\in X-N$ and $G\cap(X - N) = \emptyset$. Hence (X,τ) is w-T_2-space.

Theorem 4.4.20: Let f: (X,τ) -» (Y,τ_y) be a bijective w-open map. If (X,τ) is w-T_2- space and T_w space, then $(Y,\tau_y)$is also w-T_2- space.

Proof: Let (X,τ), is w-T_2- space and T_w- space. Let y_1 and y_2 be two distinct points of Y. Since f is bijective map, there exist distinct points x_1 and x_2 of X such that $f(x_i) = y_j$ and $f(x_2) = y_2$. Since (X,τ) is w-T_2- space,there exist w-open sets G and H such that $X_1 \in G$, $X_2 \in H$ and $G \cap H = \emptyset$. Since (X,τ) is T_w-space, G and H are open sets, then f(G) and f(H) are w- open sets of (Y,τ_y) , since f is ppw-open, such that $y_1 = f(x_1) \in f(G)$, $y_2 = f(x_2) \in f(H)$ and $f(G) \cap f(H) = \emptyset$. Therefore we have $f(G) \cap f(H) = f(G \cap H) = \emptyset$. Hence (Y,τ_y) is wT_2-space.

Theorem 4.4.21: Let (X,τ) be a topological space and let (Y,τ_y) be a W-T_2-space. Let f: $(X,\tau) \longrightarrow (Y,\tau_y)$ be an injective w-irresolute map. Then (X,τ) is w-T_2-space.

Proof: Let x_1 and x_2 be any two distinct points of X. Since f is injective, $x_1 \neq x_2$ implies $f(x_1) \neq f(x_2)$. Let $y_1 = f(x_1)$, $y_2 = f(x_2)$ so that $x_1 = f^{-1}(y_1)$, $x_2 = f^{-1}(y_2)$.Then $y_1, y_2 \in Y$ such that $y_1 \neq y_2$. Since (Y,τ_y) is W-T_2-space there exist T_w-open sets G and H such that $y_1 \in G$, $y_2 \in G$ and $G \cap H = \emptyset$. As f is T_w-irresolute $f^{-1}(G)$ and $f^{-1}(H)$ are T_w-open sets of (X,τ).

Now $f^{-1}(G) \cap f^{-1}(H) = f^{-1}(G \cap H) = f^{-1}(\emptyset) = \emptyset$ and $y_1 \in G$ implies $f^{-1}(y_1) \in f^{-1}(G)$ implies $x_1 \in f^{-1}(G)$, $y_2 \in H$ implies $f^{-1}(y_2) \in f^{-1}(H)$ implies $x_2 \in f^{-1}(H)$.Thus for every pair of distinct points x_1, x_2 of X there exist disjoint T_w-open sets $f^{-1}(G)$ and $f^{-1}(H)$ such that $x_1 \in f^{-1}(G)$, $x_2 \in f'^{-1}(H)$. Hence (X,τ) is w-T_2-space.

REFERENCES:

[1] M.Sheik john, a study on g-closed sets on continuous maps in topological and bitopological spaces ph.d Thesis Bharathiar University Coimbatote (2002).

[2]R.S.Wali and Vivekananda Dembre, “ Minimal weakly open sets and maximal weakly closed sets in topological spaces”; International Journal of Mathematical Archieve; Vol-4(9)-Sept-2014.

[3] R.S.Wali and Vivekananda Dembre, “Minimal weakly closed sets and Maximal weakly open sets in topological spaces” ; International Research Journal of Pure Algebra; Vol-4(9)-Sept-2014.

[4] R.S.Wali and Vivekananda Dembre, “ on semi-minimal open and semi-maximal closed sets in topological spaces ”; Journal of Computer and Mathematical Science;Vol-5(9)-0ct-2014 (International Journal).

[5] R.S.Wali and Vivekananda Dembre, “on pre generalized pre regular weakly closed sets in topological spaces ”; Journal of Computer and Mathematical Science;Vol-6(2)-Feb-2015 (International Journal)

[6]R.S.Wali and Vivekananda Dembre, “ on pre genearalized pre regular open sets and pre regular weakly neighbourhoods in topological spaces”; Annals of Pure and Applied Mathematics” ; Vol-10- 12 2015.

[7]R.S.Wali and Vivekananda Dembre, “on pre generalized pre regular weakly interior and pre generalized pre regular weakly closure in topological spaces”, International Journal of Pure Algebra- 6(2),2016,255-259.

[8]R.S.Wali and Vivekananda Dembre , “on pre generalized pre regular weakly continuous maps in topological spaces”, Bulletin of Mathematics and Statistics Research Vol.4.Issue.1.2016 (January-March).

[9]R.S.Wali andVivekananda Dembre,on Pre-generalized pre regular weakly irresolute and strongly pgprw-continuous maps in topological spaces, Asian Journal of current Engineering and Maths 5;2 March-April (2016)44-46.

[10]R.S.Wali and Vivekananda Dembre,On Pgprw-locally closed sets in topological spaces,
International Jounal of Mathematical Archive-7(3),2016,119-123.

[11]R.S.Wali and Vivekananda Dembre,(τ_1,τ_2) pgprw-closed sets and open sets in Bitopological spaces,International Journal of Applied Research 2016;2(5);636-642.

[12]R.S.Wali and Vivekananda Dembre,Fuzzy pgprw-continuous maps and fuzzy pgprw-irresolute in fuzzy topological spaces; International Journal of Statistics and Applied Mathematics 2016;1(1):01-04.

[13]R.S.Wali and Vivekananda Dembre,On pgprw-closed maps and pgprw-open maps in Topological spaces;International Journal of Statistics and Applied Mathematics 2016;1(1);01-04.

[14]Vivekananda Dembre, Minimal weakly homeomorphism and Maximal weakly homeomorphism in topological spaces, Bulletin of the Marathons Mathematical Society,Vol. 16, No. 2, December 2015, Pages 1-7.

[15]Vivekananda Dembre and Jeetendra Gurjar, On semi-maximal weakly open and semi-minimal weakly closed sets in topological spaces, International Research Journal of Pure Algebra-Vol-4(10), Oct – 2014.

[16]Vivekananda Dembre and Jeetendra Gurjar, minimal weakly open map and maximal weakly open maps in topological spaces, International Research Journal of Pure Algebra-Vol.-4(10), Oct – 2014; 603-606.

[17]Vivekananda Dembre ,Manjunath Gowda and Jeetendra Gurjar, minimal weakly and maximal weakly continuous functions in topological spaces, International Research Journal of Pure Algebra-vol.-4(11), Nov– 2014.

[18]Arun kumar Gali and Vivekananda Dembre, mınımal weakly generalızed closed sets and maxımal weakly generalızed open sets in topologıcal spaces, Journal of Computer and Mathematical sciences,Vol.6(6),328-335, June 2015.

[19]R.S.Wali and Vivekananda Dembre; Fuzzy Pgprw-Closed Sets and Fuzzy Pgprw-Open Sets in Fuzzy Topological SpacesVolume 3, No. 3, March 2016; Journal of Global Research in Mathematical Archives.

[20]Vivekananda Dembre and Sandeep.N.Patil; On Contra Pre Generalized Pre Regular Weakly
Continuous Functions in Topological Spaces; IJSART - Volume 3 Issue 12 – DECEMBER 2017

[21]Vivekananda Dembre and Sandeep.N.Patil ; On Pre Generalized Pre Regular Weakly Homeomorphism in Topological Spaces; Journal of Computer and Mathematical Sciences, Vol.9(1), 1-5 January 2018.

[22]Vivekananda Dembre and Sandeep.N.Patil ;on pre generalized pre regular weakly topological spaces; Journal of Global Research in Mathematical Archives volume 5, No.1**,** January 2018.

[23]Vivekananda Dembre and Sandeep.N.Patil ; Fuzzy Pre Generalized Pre Regular Weakly Homeomorphism in Fuzzy Topological Spaces ;International Journal of Computer Applications Technology and Research Volume 7–Issue 02, 28-34, 2018, ISSN:-2319–8656.

[24]Vivekananda Dembre and Sandeep.N.Patil; PGPRW-Locally Closed Continuous Maps in Topological Spaces; International Journal of Trend in Research and Development, Volume 5(1), January 2018.

[25]Vivekananda Dembre and Sandeep.N.Patil ; Rw-Separation Axioms in Topological Spaces; International Journal of Engineering Sciences & Research Technology; Volume 7(1): January, 2018.

[26]Vivekananda Dembre and Sandeep.N.Patil ; Fuzzy pgprw-open maps and fuzzy pgprw-closed maps in fuzzy topological spaces; International Research Journal of Pure Algebra-8(1), 2018, 7-12.

[27]Vivekananda Dembre and Sandeep.N.Patil ; Pgprw-Submaximal spaces in topological spaces ; International Journal of applied research 2018; Volume 4(2): 01-02.

Survey of Research on IP-DECT and VOIP Systems Safety and a Novel Counter-Measure Approach

Ferdi Sönmez
Department of Computer Engineering,
Istanbul Arel University, Turkey

Beytullah EROL
Department of Computer Engineering,
Istanbul Aydin University, Turkey

Abstract: One of the most preferred communication tools in the telecommunication world is telephony. Telephone exchanges that do not use the functioning Internet Protocol (IP) technology are beginning to lose importance. Instead, exchange systems that provide communication over IP have begun to be used. Although, Voice over IP (VoIP) technology provides great advantages over traditional telephone exchanges as enabling voice transmission over IP, security and safety concerns are seen as critical issues for VoIP technology and devices or software applications using this technology. VoIP security and safety is directly related with Internet security, since VoIP technology uses Internet infrastructure during communication and the data is transmitted between devices as IP packets. In this study, old-fashioned telephone exchange systems and systems using IP technology are compared at first glance. Secondly, threats, security and safety issues related to VoIP are addressed and studies consisting of identification of threats, identification of security measures, testing of these security measures, situations threaten VoIP security and vulnerabilities of VoIP technology are examined. Threat categorizations of Voice Over IP Security Alliance (VoIPSA) and the Internet Engineering Task Force (IETF) are examined. Papers on VoIP security and safety are classified according to VoIPSA and IETF threat taxonomy. Lastly, possible and novel counter-measures to those security and safety threats are proposed.

Keywords: Switchboard, IP PBX, IP Deck, VoIP Security and Safety, IP Deck Security and Safety

1. INTRODUCTION

By means of the telephone, the voice has been transmitted from one point to another using public switched telephone networks (PSTN) [1]. With the rapid progress and development of Internet Protocol (IP) technology, widespread use has led to the idea of voice transmission over packet-switched networks [2]. PBX means private branch exchange and IP PBX is the exchange system that makes data communication over IP (Internet protocol). On the other hand, while PBX is a conventional PBX system, IP PBX refers to PBX systems that communicate over IP. These IP PBX systems have many advantages over conventional PBX systems [3][4].

Voice over Internet protocol (VoIP) is a collection of technologies based on the IP protocol that enables today's circuit-switched communication services to operate on packed data networks [1]. In other words, instead of traditional telephone networks, the transmission of voice over IP-based networks by converting them into IP packets is called 'IP Telephony' [2]. In other respects, The IP-DECT (digitally enhanced cordless telephone) system can be thought of as a link (bridge) between VoIP and DECT. IP-DECT systems can be used in a number of situations where wireless connectivity is needed in IP converters or integrated communications systems [3]. Especially; IP-DECT systems provide effective advantages for users where wireless connection is required [5][6]. But even for any person, it is a practical and very advantageous solution for users to take their phone and go to another place, and respond to all their calls without being tied to the desk. Flexibility and ease of use are combined with IP-DECT technology [6]. The disadvantages of fixed phone are eliminated by IP-DECT technology and a more advantageous solution is offered [6][7].

When looked at by the IP PBX, each DECT phone sends an IP call in the context of the phone feature. Many services are provided, such as the features that the IP PBX is subscribed to, and the numbering plan [8]. All configuration and maintenance procedures are performed via the IP-DECT Base Stations, the IP-DECT Gateway and the web interface on the VoIP gateway. On account of the web interface, all the configuration and maintenance operations can be adjusted easily. Moreover, the web interface on IP-DECT base stations, IP-DECT gateways and VoIP gateways, many operations can be performed easily by manual operation in classical telephone exchange systems [8]. Another important feature is that new base stations with VoIP support can be used together with traditional base stations in the same system [9]. As an example of this advantageous situation, when a person wants to convert the traditional PBX system to the system of the new technology IP telephone server structure, the VoIP system can be seamlessly switched without losing the wireless communication system infrastructure used. Benefits of the IP-DECT system compared to traditional DECT systems [8][9]:

- Less cabling and maintenance requirements with a single main network
- Integrated telephony and data-based technologies
- Mobile freedom without being connected to a fixed location
- In other locations, there is no telephone exchange system requirement.
- One number for roaming (mobile) users
- Flexibility and usability
- Classic and new IP PBX systems can work together

Despite the advantages, VoIP carries some security problems, since the transmission is influenced by the problems that occur on the Internet. VoIP traffic consists of data stream between network devices that the interventions to the network devices mean that the system is open to intervention from the outside. The threats to the system are a combination of protocols used, VoIP devices and software. There are different methods of attack on such systems. VoIP traffic can be intercepted, copied, blocked, slowed, or altered by malicious intent [10]. The study was organized as follows. In section two, VOIP is examined. Section 3 involves the VOIP security and safety issues and a classification of research papers. Then, in section 4, counter-measures againsts threats is summarized. Section 5 includes concluding remarks.

2. VOICE COMMUNICATION over the INTERNET PROTOCOL

VoIP is the name given to technology that enables voice transmission over a packet-switched Internet network instead of a public switched telephone network.

2.1. VoIP and Historical Development

In VoIP, voice data is converted into IP packets and transmitted over the Internet. When the voice is converted into a packet, it is added to the voice data in the titles including the route information to be monitored by the package. Small segmented audio signals are sent over the network to a single destination [10]. In summary, audio signals are compressed while being packed, transferred over the network, and then decompressed again [11].

One of the biggest advantages of VoIP technology is that it can be negotiated at very long distances without paying a fee other than the Internet fee, or paying much below the standard telephone tariff. The development of VoIP solutions has enabled large business operators to have voice calls over existing Internet lines within their organization. VoIP can carry 5 to 10 times more voice calls over the same bandwidth compared to conventional circuit switched services [11]. In the case of voice transmission scenarios such as computer to computer, computer to telephone, computer to telephone and telephone to telephone, devices must make calls to each other, call terminations etc. There are protocols that they use when they perform business and operations. The need for different protocols to be developed by different VoIP application developers or device manufacturers needing to use a common set of protocols so that users can interact with each other [12].

2.2. VoIP Scenario

VoIP scenario takes place in five ways.

- Computer voice transmission from computer to computer.
- Computer to phone (PSTN) or telephone (PSTN) to computer
- From the phone (PSTN) to the phone (PSTN)
- Mobile VoIP
- Wireless VoIP

The conventional telephone system (PSTN) is numbered according to ITU-T E.164 recommendation. According to this numbering system, the phone numbers consist of country code, area code / national destination code (long distance code) and subscriber number [13]. In order for a phone on the PSTN network to communicate with a computer with Internet access, the computer to be dialed must have a number according to ITU-T E.164 recommendation. For instance, in the VoIP service named Wirofon offered by Turk Telekom Company, the subscriptions were given a number starting with an area code of 850.

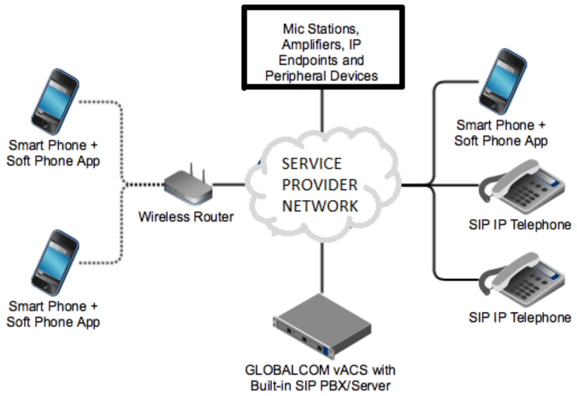

Mic Stations, Amplifiers, IP Endpoints and Peripheral Devices
Smart Phone + Soft Phone App
Smart Phone + Soft Phone App
Wireless Router
SERVICE PROVIDER NETWORK
Smart Phone + Soft Phone App
SIP IP Telephone
SIP IP Telephone
Smart Phone + Soft Phone App
GLOBALCOM vACS with Built-in SIP PBX/Server

Figure 1. A Generic VoIP Scenario

Switching between the traditional telephone system (PSTN) and the VoIP system is provided by means of a gateway. The gateway is responsible for converting voice and other signaling information between the traditional telephone system (PSTN) and VoIP systems [14].

2.3. Computer to computer voice transmission

Communication from computer to computer is usually done by entering the IP address of the opposite party. Other methods such as domain name, e-mail address, member name and password can be preferred.

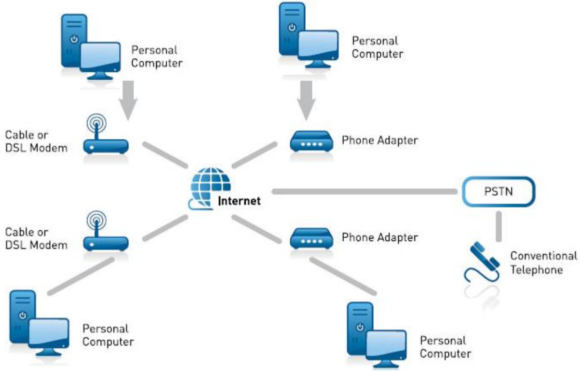


Figure 2. Computer voice transmission from computer to computer

VoIP calls can be made from mobile phone to mobile phone, as well as fixed phones and computers in PSTN network from mobile phone [14].

2.4. Mobile VoIP

Mobile VoIP has become a new VoIP scenario with the transition of mobile networks to 3G systems. While mobile networks operating with the 2G system operate with the circuit switching logic, packet switching data communication in addition to 2G has been possible with the transition to 3G [14]. Thanks to packet switching in the 3G system, bandwidth is only used during data exchange and much higher data transmission speeds are supported. With the innovations introduced by 3G technology, it supports users to make VoIP calls over the mobile network or using wireless networks [15].

2.5. Wireless VoIP

Wireless VOIP is implemented with phones designed to be compatible with the 802.11x standard family and capable of connecting to the Internet without cables and communicating voice over VoIP protocols over wireless networks [14][15]. Although WLAN is designed to expand IP networks, it has also created an alternative for voice communication.

Although wireless VoIP systems have evolved in recent years, Wi-Fi VoIP phones need to be improved in terms of battery life, security support, Internet browser support [16]. Because Wi-Fi technology is not designed to consume less energy, the small batteries of Wireless VoIP phones are inadequate. Some wireless network providers (Hotspot providers) use a website to login to the wireless network for security checks [17]. If the Wi-Fi VoIP phone does not have Internet browser support, the hotspot will not be able to use the wireless network because it can not open the Internet site required for access [16][17]. Supporting up-to-date wireless encryption methods in the 802.11x standard Wi-Fi VoIP phone will enable secure voice communication [18]. As a result, the widespread deployment of the Wireless VoIP scenario needs to increase the number of devices that are capable of the above mentioned features.

2.6. Session Initiation Protocol

Session Initiation Protocol (SIP) was proposed by The Internet Engineering Task Force (IETF) as a standard for IP multimedia calls and derived from Hyper-Text Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) [19]. It is flexible with the text based creation of SIP and can be expanded and scaled by code changes. In addition, the ability to work with the web also allows to use with other IP applications [20]. Multimedia presentations, instant messaging applications, distributed computer applications, signaling and most important VoIP calls are the main usage areas of SIP.

One of the advantages of SIP is that it can use Internet-based protocols to complete its own signaling protocols [21]. SIP only deals with how sessions are created, edited and terminated [20]. Other features are provided through protocols such as HTTP 2.0, Session Definition Protocol (SDP), Domain Name Server (DNS), Dynamic Host Configuration Protocol (DHCP), Real-time Transport Protocol RTP, Real-time Control Transport Protocol (RTCP) [21]. The SIP protocol can detect the condition of the destination of the voice packet. If the destination does not exist at that time or is not available, the SIP protocol can detect this situation . So, it tries other ways of reaching the target. It can do address resolution, address mapping, call routing [22].

3.VOIP SECURITY and SAFETY

In IP communication technology, every application used is the target or tool to be attacked [23]. With the increasing popularity of VoIP technology in recent years, it has become inevitable to target against the attackers. Especially VoIP attacks exploiting information security attacks are increasing day by day, and weaknesses and weak points of VoIP networks are being affected too much by this [24].

VoIP technology has several differences compared to traditional PSTN technology. Especially when the configuration of the software and services can be done by both the manufacturer and the end user, it makes the system vulnerable to attack. Today, VoIP applications and users are increasing rapidly [23]. It is also a possible that hundreds of million mobile VoIP users are thought to be faced with such threads. Because of SIP's text-based structure and its architecture similar to HTTP architecture, it is possible to attack not only known attack types but also SIP-specific attacks [23]. Packet exchanges during the use of TCP and UDP during communication make it very easy to exchange messages and information. Since SIP is not its own security mechanism, it is possible to be affected by the attacks as long as no measures are taken [25]. In addition to being vulnerable to known threats and known weaknesses, complex security architectures are needed depending on VoIP specific weaknesses. Currently used security devices are insufficient in VoIP and SIP security [24]. Attacks such DoS attacks, session dropping, wiretapping, fake recording, etc. can cause VoIP network to become ineffective or leak information [26]. The Voice Over IP Security Alliance (VOIPSA) has published security weaknesses against VoIP systems in its notice posted on its web site and categorized it as follows [25].

- Social threats
- Eavesdropping threats
- Denial of service threats
- Service abuse threats
- Physical access threats
- Interruption of services threats

IETF has categorized the threats coming with a similar grouping:

- Service disruption and annoyance
- Eavesdropping and traffic analysis
- Masquerading and impersonation
- Unauthorized access
- Fraud

3.1. Denial of Service

Denial of Service (DoS) attacks target IP networks that can have little effect on system operation or contrarily make the system completely unusable [27]. These attacks can not be prevented by security measures, such as encryption or authentication, because the voice packets are sent to the intended user [28]. It is difficult to take action against DoS and DDoS attacks because it usually comes in the form of Syncronize (SYN) and Internet Control Message Protocol (ICMP) packets [29]. Servers and UAs will accept these packages because it is not known which package is real, and which package is destined for attack. The percentage of DoS / DDoS attacks on networks such as VoIP, which perform real-time data communication, is very high [30]. A momentary interruption can cause major distress in these systems. If the attacker performs these attacks against high-priority network devices such as media gateways, interactive voice response (IVR), virtual machine, and so on, then ultimate harm may also occur [29][30]. The management of UDP ports is crucial to this attack, which can also be faced in the way that all calls are routed to another system or firewall [31]. Another and most faced DoS attack is replay attack which is a type of attack based on re-sending data packets. The re-transmitted data packets affect the data ordering on the receiver side. As a result, the stage becomes delayed and the call quality drops [29]. A person interfering with a call between two people records some or all of the talk, then transmits the packets it receives to the recipient. The most risky part of such an attack may be that the speaker shares his personal information or approves a major operation [28]. The attacker causes the voice packets containing the acknowledgment voice of the talkers to be repeatedly transmitted to the receiver in order to confirm the undesired operations. Below are other types of DoS attacks [30][31][32]. Some of these attacks may be partially inadequate, while others may completely disable the system. There are also DoS attacks that prevent calls from being made and that prevent voice messages from being received, and that do not even allow emergency calls.

- TLS Connection Reset
- VoIP Packet Replay Attack
- Quality of Service (QoS) Modification Attack
- VoIP Packet Injection
- DoS against Supplementary Services

- Control Packet Flood
- Bogus Message DoS
- Immature Software DoS
- Packet of Death DoS

3.2. Eavesdropping

Eavesdropping takes the form of listening or recording phone calls. It is necessary to access the network in order to carry out this attack [33]. Some protocol analysis programs can be used to listen to and record SIP and RTP traffic. Details of multiple conversations can be reached with this attack [34]. This means that unprotected signaling and data packets between users are displayed. It is possible to access and store data packets on the purpose of analyzing the network traffic [35]. Another intent of the attack is to obtain verbal or written information by techniques such as social engineering [36][37].

3.3. Spoofing

Spoofing is dangerous for service providers, since accomplished by changing the settings of the signaling messages or VoIP devices [29]. Here, attackers aim to make personal or financial gain by abusing VoIP services [30]. Fraud scenarios can be implemented in VoIP applications by influencing the call flow [27]. To prevent spoofing robust and difficult to interlace intrusion detection systems shold be preffered and more complex defense mechanisms should be followed.

3.4. Man in the Middle Attack and Call Hijack

This attack covers or combination of many other attacks. It can be described as the attacker entering between two or more users in the transmission and reading or changing messages without informing them [38]. If there is no security precautions for wireless connections and if there is a SIP communication over this network, vulnerability may occur [39]. The attacker intercepts the interim messages and changes the direction as it passes over its own server. Afterwards, DoS, hijacking and many other attacks can take place in the position [37]. This attack allows an attacker to intervene between the SIP server and the SIP user agent. Any valid username or password can be registered with the SIP server without knowing it [36]. Along with recording, it opens up many attacks.

3.5. Masquerade

Attackers behave and being treated as a user or system component and gain authorization on the system entities [40][41]. This attack is intended to access another user, service, or component [42]. This creates a significant layer of attack because fraud, unauthorized access, and service disruption attacks can be performed using this method. The characteristic of this attack is that system components can mimic the identity of entity. The target of the attack may be a user, device, or network component [43]. VoIP components can be signaled by unauthorized access or remote connection, or data packets can be used at their own discretion. Masquerade attacks particularly are directed to the application layer protocols [42][44].

3.6. Classification of Studies on VoIP Threats

Now, we discuss the studies contained in the VoIPSA and IETF classification that makes up the remaining of the study. All studies are classified in Table 1.

Table 1. Research Grouping by VoIPSA and IETF Threats Classification

S/N	VoIPSA classification	References by research	IETF classification	References by research	S/N
1	*Eavesdropping threats*	[33][34][35][36][37][38]	*Service disruption and annoyance*	[25][27][28][29][30][31][32]	1
2	*Denial of Service threats*	[23][25][27][28][29][30][31][32]	*Eavesdropping and traffic analysis*	[33][34][35][36][37][38]	2
3	*Service Abuse threats*	[45][46][47][48][49][50]	*Masquerading and impersonation*	[61][62][63][64][65][66]	3
4	*Physical access threats*	[51][52][53][54][55][56]	*Unauthorized access*	[51][52][53][54][55][56]	4
5	*Interruption of services threats*	[38][39][57][58][59][60]	*Fraud*	[45][46][47][48][49][50]	5
6	*Social threats*	[61][62][63][64][65][66]			

There are many academic studies on VoIP security. These studies mostly consist of identification of threats, identification of security measures, and testing of these security measures [24][67]. Since VoIP technology is a widely used, ever-evolving and growing technology, many service providers that offer VoIP services are also working on this issue. VoIP security has been the subject of thesis studies, too. Situations that threaten VoIP security are at the top of the most researched topics [67]. In order to take measures against security attacks, it is first necessary to identify these threats [59]. Vulnerabilities arise from VoIP architecture, protocols used, signaling weaknesses, routing and termination problems of components are the basis of their work. Classification of detected security threats is another important issue. Correct detection of security threats and good classification are an important step in taking effective measures against security threats [59]. After the identification of security threats, the proposed solution to these is another research topic.

4. COUNTER-MEASURES

VoIP security is directly related with Internet security, since VoIP technology uses Internet infrastructure during communication and the data is transmitted between devices as IP packets. There are many security mechanisms and methods developed against the attacks as counter-measures. In this section, we examined the security measures used in VoIP security, briefly. These security measures aim to provide effective and efficient security at each layer.

In order for a system to be secure, it must have at least three qualities or obey CIA triad [25] rules and domain specific ones [24][26]. These are;

- Confidentiality: The transmitted data means that only authorized users can access it. Ensuring that SIP signaling is done in a secure environment and that it is not affected by attacks such as wiretaps is essential. An attacker who can view SIP messages can easily listen to each unencrypted conversation [40]. To avoid this unwanted situation, messages must be encrypted. IPsec (Internet Protocol Security), developed to meet the security needs of the IP protocol, must be used to prove the authenticity of the communication, to ensure its privacy.
- Integrity: Protecting the data transmitted of stored against external factors, ensuring data integrity, means that only authorized users or malicious software change the data. Integrity principle, which provides user authentication, is used to protect the trusted sources. An attacker who is involved in an untrusted system without any situation of being caught or noticed can change different contents. It is desired to avoid this situation with integrity. SIP authentication prevents this from being altered by an unauthorized attacker. IPsec must be used to prove the authenticity of the communication, to ensure its integrity.
- Availability: It is defined as the time when the users defined in the system are at the request of the service and the service availability. Delays over acceptable level are undesirable for SIP networks. Any delay in real-time VoIP infrastructure can cause troubles. For example, a user who makes an invite request will cancel the request if the request does not take a certain period of time. However, the other user message will be delayed and the request message will be sent to the requesting user after the request is canceled. Another example is service disruption attacks which are intended to affect network components [40]. Spam Through Internet Telephony (SPIT) is examined as a service disruption attack which aims to prevent availability phones [41].
- Authentication: the user and the server must trust the credentials passed. In the request message, the called party must trust the requested information in the response message to the caller information sought.
- Rejection: The user who sent the message should not deny that it sent this message. This feature, which is used as an attack countermeasure, avoids the complexity and allows the attacker to distinguish between the attacker and the attacker.

5. CONCLUSION and RECOMMENDATIONS

IP telephone exchange systems are better than conventional telephone exchange systems in many respects, such as usability and security. As in all systems, there are security problems in IP based systems as well. Here, the security issues that IP-based systems may encounter, are addressed. Activating the https protocol will be of great benefit to users. This protocol, which means secure hyper text transfer communication, can be used to prevent the attacker from being infiltrated into the network and seizing the data, while being more protected than the classic http protocol against attack. Activating IP-based filtering is also an important factor. For example, accepting connections that only have a certain IP will not accept other connections. Another method is to restrict the number of users connected to the devices. Lastly, in order to make a system more secure, it must have at least three qualities or obey CIA triad rules and domain specific ones. In this study, 45 publications on IP DECK and VoIP security have been examined and classified by VoIPSA and IETF threat taxonomy. Vulnerabilities arise from VoIP architecture, protocols used, signaling weaknesses, routing and termination problems of components are the basis of their work. As a future hope and work, this study will help to conduct other VoIP security and counter-measures research and we will pay much attention on counter-measure research that after a comprehensive analysis of them we plan to develop a novel counter-measure or defense approach for recent threats or threats which have big and resident effects.

6. REFERENCES

[1] Bestak, R., Vranova, Z., & Ondryhal, V. (2011). Testing of Transmission Channels Quality for Different Types of Communication Technologies. Digital Information and Communication Technology and Its Applications, pp.13-23.

[2] Frieden, R. (2013). The mixed blessing of a deregulatory endpoint for the public switched telephone network. *Telecommunications Policy*, *37*(4), pp.400-412.

[3] Abid, F., Izeboudjen, N., Bakiri, M., Titri, S., Louiz, F., & Lazib, D. (2012). Embedded implementation of an IP-PBX/VoIP gateway. In Microelectronics (ICM), 2012 24th International Conference on, pp. 1-4.

[4] Kulin, M., Kazaz, T., & Mrdovic, S. (2012). SIP server security with TLS: Relative performance evaluation. In Telecommunications (BIHTEL), 2012 IX International Symposium on, pp. 1-6.

[5] Plosz, S., Moldovan, I., Trinh, T. A., Foglar, A. (2010). Design and Implementation of a Practical Smart Home System Based on DECT Technology. In International Conference on Energy-Efficient Computing and Networking, pp. 104-113, Springer, Berlin, Heidelberg.

[6] Coisel, I., & Sanchez, I. (2014). Practical interception of DECT encrypted voice communication in unified communications environments. In Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint, pp. 115-122.

[7] Vergados, D. D. (2010). Service personalization for assistive living in a mobile ambient healthcare-networked environment. Personal and Ubiquitous Computing, 14(6), 575-590.

[8] Soloducha, M., Raake, A., Kettler, F., Rohrer, N., Parotat, E., Waeltermann, M., & Voigt, P. (2016). Towards VoIP quality testing with real-life devices and degradations. In *Speech Communication; 12. ITG Symposium; Proceedings of*, pp. 1-5.

[9] Bestak, R., Vranova, Z., & Ondryhal, V. (2011). Testing of Transmission Channels Quality for Different Types of Communication Technologies. *Digital Information and Communication Technology and Its Applications*, pp.13-23.

[10] Bhalla, M. R., & Bhalla, A. V. (2010). Generations of Mobile Wireless Technology: A Survey. *International Journal of Computer Applications*, *5*(4), pp.26-32.

[11] Al-Saadawi, H., & Varol, A. (2017). Voice over IP forensic approaches: A review. In Digital Forensic and Security (ISDFS), 2017 5th International Symposium on, pp. 1-6.

[12] Facchinetti, T., Ghibaudi, M., Goldoni, E., & Savioli, A. (2010). Real-time voice streaming over IEEE 802.15. 4. In Computers and Communications (ISCC), 2010 IEEE Symposium on, pp. 985-990.

[13] Mealling, M., & Faltstrom, P. (2004). The E. 164 to uniform resource identifiers (URI) dynamic delegation discovery system (DDDS) application (ENUM).

[14] Wang, X., Patil, A., & Wang, W. (2006). VoIP over wireless mesh networks: challenges and approaches. In *Proceedings of the 2nd annual international workshop on Wireless Internet* (p. 6)..

[15] Boucadair, M., Borges, I., Neves, P. M., & Einarsson, O. P. (2011). *IP Telephony Interconnection Reference: Challenges, Models, and Engineering*. CRC Pres.

[16] Murty, R., Padhye, J., Chandra, R., Wolman, A., & Zill, B. (2008, April). Designing High Performance Enterprise Wi-Fi Networks. In NSDI, 8, pp. 73-88.

[17] Gibson, J. D., & Wei, B. (2004). Tandem voice communications: digital cellular, VoIP, and voice over Wi-Fi. In *Global Telecommunications Conference, 2004. GLOBECOM'04 IEEE* , 2, pp. 617-621.

[18] Ganguly, S., & Bhatnagar, S. (2008). *VoIP: wireless, P2P and new enterprise voice over IP*. John Wiley & Sons.

[19] Tzerefos, P., Smythe, C., Stergiou, I., & Cvetkovic, S. (1997, November). A comparative study of simple mail transfer protocol (SMTP), post office protocol (POP) and X. 400 electronic mail protocols. In *Local Computer Networks, 1997. Proceedings., 22nd Annual Conference on*, pp. 545-554.

[20] Gardner M. T., Frost V.S., Petr D.W. (2003). Using optimization to achieve efficient quality of service in voice over IP networks. In *Performance, Computing, and Communications Conference, 2003. Conference Proceedings of the 2003 IEEE International*, pp. 475-480.

[21] Ormazabal, G., Nagpal, S., Yardeni, E., & Schulzrinne, H. (2008). Secure sip: A scalable prevention mechanism for dos attacks on sip based voip systems. *Principles, systems and applications of IP telecommunications. Services and security for next generation networks*, pp. 107-132.

[22] Durkin, J. F. (2003). *Voice Enabling the Data Network: H. 323, MGCP, SIP, QoS, SLAs, and Security*. Cisco Press.

[23] Yüksel, M , Öztürk, N. (2017). SIP Attacks and Security Methods. International Journal of Informatics Technologies, 10 (3), pp. 301-310.

[24] Keromytis, A. D. (2012). A comprehensive survey of voice over IP security research. *IEEE Communications Surveys & Tutorials*, 14(2), pp. 514-537.

[25] Hanifan, Y., & Bandung, Y. (2013). Designing VoIP security system for organizational network. In *ICT for Smart Society (ICISS), 2013 International Conference on*, pp. 1-5.

[26] Lazzez A., Slimani T. (2013).“Deployment of VoIP Technology:QoS Concerns”, International Journal of Advanced Research in Computer and Communication Engineering, 2(9),pp. 65-74.

[27] Farley, R., & Wang, X. (2012). VoIP Shield: A transparent protection of deployed VoIP systems from SIP-based exploits. In *Network Operations and Management Symposium (NOMS), 2012 IEEE*, pp. 486-489.

[28] Akbar M. A. and M. Farooq, “Application of Evolutionary Algorithms in Detection of SIP based Flooding Attacks,” in Proc. Genetic and Evolutionary Computation Conference (GECCO), 2009.

[29] Ouchani, S., Jarraya, Y., & Mohamed, O. A. (2011). Model-based systems security quantification. In *Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference on*, pp. 142-149.

[30] Sengar, H., H. Wang, D. Wijesekera, and S. Jajodia, “Fast Detection of Denial-of-Service Attacks on IP Telephony,” in Proc. 14th IEEE International Workshop on Quality of Service (IWQoS), pp. 199–208, 2006.

[31] Hentehzadeh, N., Mehta, A., Gurbani, V. K., Gupta, L., Ho, T. K., & Wilathgamuwa, G. (2011). Statistical analysis of self-similar Session Initiation Protocol (SIP) messages for anomaly detection. In *New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on* (pp. 1-5).

[32] D. Geneiatakis and C. Lambrinoudakis, “A Lightweight Protection Mechanism against Signaling Attacks in a SIP-based VoIP Environment,” Telecommunication Systems, vol. 36, pp. 153–159, 2007.

[33] Azfar, A., Choo, K. K. R., & Liu, L. (2014). A study of ten popular Android mobile VoIP applications: Are the communications encrypted?.

In *System Sciences (HICSS), 2014 47th Hawaii International Conference on*, pp. 4858-4867.

[34] Wright C. V., Ballard L., Monrose F.N. and Masson G.M. “Language Identification of Encrypted VoIP Traffic: Alejandra y Roberto or Alice and Bob?,” in Proc. 16th USENIX Security Symposium, pp. 1–12, 2007.

[35] Zhang R., Wang X., Farley R., Yang X., and X. Jiang, “On the Feasibility of Launching the Man-In-The-Middle Attacks on VoIP from Remote Attackers,” in Proc. 4th International ACM Symposium on Information, Computer, and Communications Security (ASIACCS), pp.61–69, 2009.

[36] Guo J.-I., Yen J.-C., and Pai H.-F. “New Voice over Internet Protocol Technique with Hierarchical Data Security Protection,” IEE Proc. — Vision, Image and Signal Processing, 149, pp. 237–243, 2002.

[37] Talevski A., Chang E., Dillon T. “Secure Mobile VoIP,” in Proceedings of International Conference on Convergence Information Technology, pp. 2108–2113, 2007.

[38] Reynolds B. and Ghosal D. "STEM: Secure Telephony Enabled Middlebox," in IEEE Communications Magazine, 40(10), pp. 52-58, 2002.

[39] Cretu G. F., A. Stavrou, M. E. Locasto, S. J. Stolfo, and Keromytis A. D. “Casting out Demons: Sanitizing Training Data for Anomaly Sensors,” in Proc. IEEE Security and Privacy Symposium, pp. 81–95, 2008

[40] Seo, D., Lee, H., & Nuwere, E. (2013). SIPAD: SIP–VoIP anomaly detection using a stateful rule tree. *Computer Communications*, *36*(5), pp. 562-574.

[41] Geneiatakis d., T. Dagiuklas, C. Lambrinoudakis, G. Kambourakis, and Gritzalis S. “Novel Protecting Mechanism for SIP-based Infrastructure against Malformed Message Attacks: Performance Evaluation Study,” in Proc. 5th International Conference on Communication Systems, Networks and Digital Signal Processing (CSNDSP), pp. 261–266, 2006.

[42] Gritzalis, D., Marias, G., Rebahi, Y., Soupionis, Y., & Ehlert, S. (2011). SPIDER: A platform for managing SIP-based Spam over Internet Telephony (SPIT). *Journal of Computer Security*, *19*(5), pp.835-867.

[43] Kolan P., Dantu R. “Socio-technical Defense Against Voice Spamming,” ACM Transactions on Autonomous and Adaptive Systems (TAAS), 2, 2007.

[44] Madhosingh A. “The Design of a Differentiated SIP to Control VoIP Spam,” Masters Thesis Report SPIT, CAPTCHA, Florida State University, Computer Science Department, 2006.

[45] Akbar M.A., Farooq M. “Application of Evolutionary Algorithmsin Detection of SIP based Flooding Attacks,” in Proc. Genetic and Evolutionary Computation Conference (GECCO), 2009.

[46] Hunter P. “VOIP the Latest Security Concern: DoS Attack the Greatest Threat,” Network Security, 11, pp. 5–7, 2002.

[47] Batchvarov A. “Security Issues and Solutions for Voice over IP Compared to Circuit Switched Networks,” tech. rep., INFOTECH Seminar Advanced Communication Services (ACS), 2004

[48] Geneiatakis D., Kambourakis G., Lambrinoudakis C., Dagiuklas T. and Gritzalis S. “SIP Message Tampering: THE SQL code INJECTION attack,” in Proc. 13th IEEE International Conference onSoftware, Telecommunications and Computer Networks (SoftCOM), 2005.

[49] McGann S. and Sicker D. “An Analysis of Security Threats and Tools in SIP-Based VoIP Systems,” in Proc. 2nd VoIP Security Workshop, 2005.

[50] Rebahi, Y., Nassar, M., Magedanz, T., & Festor, O. (2011). A survey on fraud and service misuse in voice over IP (VoIP) networks. *Information Security Technical Report*, *16(1)*, pp.12-19.

[51] Kolias, C., Kambourakis, G., & Maragoudakis, M. (2011). Swarm intelligence in intrusion detection: A survey. *computers & security*, *30*(8), pp.625-642.

[52] Geneiatakis D., Lambrinoudakis C., Kambourakis G. “An OntologyBased Policy for Deploying Secure SIP-based VoIP Services,”Computers and Security, 27, pp. 285–297, 2008

[53] Sisalem D., S. Ehlert, D. Geneiatakis, G. Kambourakis, T. Dagiuklas, J. Markl, M. Rokos, O. Botron, J. Rodriguez, and Liu J. “Towards a Secure and Reliable VoIP Infrastructure,” Tech. Rep. Deliverable D2.1, SNOCER COOP-005892, 2005.

[54] Sher M. and Magedanz T. “Protecting IP Multimedia Subsystem (IMS) Service Delivery Platform from Time Independent Attacks,” in Proc. 3rd International Symposium on Information Assurance and Security (IAS), pp. 171–176, 2007

[55] Armoogum, S., & Mohamudally, N. (2014, May). Survey of practical security frameworks for defending SIP based VoIP systems against DoS/DDoS attacks. In *IST-Africa Conference Proceedings, 2014* (pp. 1-11). IEEE.

[56] Rieck K., S. Wahl, P. Laskov, P. Domschitz, and Muller K.-R. “A Self-learning System for Detection of Anomalous SIP Messages,” in Proc. 2nd Internation Conference on Principles, Systems and Applications of IP Telecommunications. Services and Security for Next Generation Networks: Second International Conference, (IPTComm), pp. 90–106, 2008.

[57] Bessis T., Rana A. and Gurbani V.K. “Session Initiation Protocol (SIP) Firewall for Internet Multimedia Subsystem (IMS) Core,” Bell Labs Technical Journal, 2010.

[58] Sengar H., Wijesekera D., Wang H., and Jajodia S. “VoIP Intrusion Detection Through Interacting Protocol State Machines,” in Proc. International Conference on Dependable Systems and Networks (DSN), pp. 393–402, 2006.

[59] Geneiatakis D., G. Kambourakis, T. Dagiuklas, C. Lambrinoudakis, and Gritzalis S. “A Framework for Detecting Malformed Messages in SIP Networks,” Computer Networks: The International Journal of Computer and Telecommunications Networking, 51, pp. 2580-2593, 2007.

[60] Mehta A., N. Hantehzadeh, V. K. Gurbani, T. K. Ho, J. Koshiko, and Vishwanathan R. “On the inefficacy of Euclidean classifiers for detecting self-similar Session Initiation Protocol (SIP) messages,” in Proc. 12th IFIP/IEEE International Symposium on Integrated Network Management (IM), 2011 .

[61] Tu, H., Doupé, A., Zhao, Z., & Ahn, G. J. (2016, May). SoK: Everyone Hates Robocalls: A Survey of Techniques against Telephone Spam. In *Security and Privacy (SP), 2016 IEEE Symposium on*, pp. 320-338.

[62] Cao F., Ha B., Padmanabhan R., A. Yuan, and Tran K., S. Phithakkitnukoon and R. Dantu "Defense Against SPIT Using Community Signals," in Proc. IEEE International Conference on Intelligence and Security Informatics (ISI), 2009.

[63] Banerjee N., S. Saklikar, and Saha S. "Anti-vamming Trust Enforcement in Peer-to-peer VoIP Networks," in Proc. International Conference on Communications and Mobile Computing (IWCMC), pp. 201–206, 2006.

[64] Haberler M. and Lendl O. "Secure Selective Peering with Federations," in Proc. 3rd Workshop on Securing Voice over IP, 2006.

[65] Quittek J. S. Niccolini, S. Tartarelli, and Schlegel R. "Prevention of Spam over IP Telephony (SPIT)," NEC Technical Journal, 1(2), pp. 114–119, 2006.

[66] Kolan P., R. Dantu, and Cangussu J.W. "Nuisance of a Voice Call," ACM Transactions on Multimedia Computing, Communications and Applications (TOMCCAP), 5(6), pp. 1–22, 2008.

[67] Ehlert, S., Geneiatakis, D., & Magedanz, T. (2010). Survey of network security systems to counter SIP-based denial-of-service attacks. *Computers & Security*, *29*(2), pp.225-243.

International Journal of Computer Applications Technology and Research
Volume 7–Issue 03, 122-128, 2018, ISSN:-2319–8656

Improving Student Enrollment Prediction Using Ensemble Classifiers

Stephen Kahara Wanjau
Directorate of ICT
Murang'a University of Technology
Murang'a, Kenya

Geoffrey Muchiri Muketha
School of Computing and IT
Murang'a University of Technology
Murang'a, Kenya

Abstract: In the recent years, data mining has been utilized in education settings for extracting and manipulating data, and for establishing patterns in order to produce useful information for decision making. There is a growing need for higher education institutions to be more informed and knowledgeable about their students, and for them to understand some of the reasons behind students' choice to enroll and pursue careers. One of the ways in which this can be done is for such institutions to obtain information and knowledge about their students by mining, processing and analyzing the data they accumulate about them. In this paper, we propose a general framework for mining student data enrolled in Science, Technology, Engineering and Mathematics (STEM) using performance weighted ensemble classifiers. We train an ensemble of classification models from enrollment data streams to improve the quality of student data by eliminating noisy instances, and hence improving predictive accuracy. We empirically compare our technique with single model based techniques and show that using ensemble models not only gives better predictive accuracies on student enrollment in STEM, but also provides better rules for understanding the factors that influence student enrollment in STEM disciplines.

Keywords: Ensemble classification, STEM, predictive modeling, machine learning, WEKA.

1. INTRODUCTION

Strengthening the scientific workforce has been and continues to be of importance for every country in the world. Preparing an educated workforce to enter Science, Technology, Engineering and Mathematics (STEM) careers is important for scientific innovations and technological advancements, as well as economic development and competitiveness [1]. In addition to expanding the nation's workforce capacity in STEM, broadening participation and success in STEM is also imperative for women given their historical underrepresentation and the occupational opportunities associated with these fields.

Higher Education Institutions (HEIs) in Kenya offer a variety of academic programs with admission of new student held every year. Student applications are selected based exclusively on one criterion, their performance in the Secondary School Final Examination (KCSE), an academic exam that largely evaluates four components: Mathematics, Sciences, Social sciences, and Languages. Every academic program has a previously defined number of places that are occupied by the students with higher marks, ensuring a high academic quality of the students. As HEIs increasingly compete to attract and retain students in their institutions, they can take advantage of data mining, particularly in predicting enrollment. These institutions can collect data about students from the admission process including the test scores results, the decision for enrollment, and some socio-demographic attributes. This data can be used to predict future student enrollment using data mining techniques.

Machine learning has in the recent years found larger and wider applications in Higher Education Institutions and is showing am increasing trend in scientific research, an area of inquiry, termed as Educational Data Mining (EDM) [1]. EDM aims towards discovering useful information from large amounts of electronic data collected by educational systems. EDM typically consists of research to take educational data and apply data mining techniques such as prediction (including classification), discovery of latent structure (such as clustering and q-matrix discovery), relationship mining (such as association rule mining and sequential pattern mining), and discovery with models to understand learning and learner individual differences and choices better [2], [3].

Researchers in educational data mining have used many data mining techniques such as Decision Trees, Support Vector Machines, Neural Networks, Naïve Bayes, K-Nearest neighbor, among others to discover many kinds of knowledge such as association rules, classifications and clustering [4]. The discovered knowledge has been used for prediction regarding enrolment of students in a particular course, alienation of traditional classroom teaching model, detection of unfair means used in online examination, detection of abnormal values in the result sheets of the students, prediction about students' performance among others [5].

Prediction modeling lies at the core of many EDM applications whose success depends critically on the quality of the classifier [6]. There has been substantial research in developing sophisticated prediction models and algorithms with the goal of improving classification accuracy, and currently there is a rich body of such classifiers. However, although the topic of explanation and prediction of enrollment is widely researched, prediction of student enrollment in higher education institutions is still the most topical debate in higher learning institutions. These institutions would like to know, for example which student will enroll in which particular course, and which students will need assistance in order to graduate [7]. One approach to effectively address these student challenges is through the analysis and presentation of data or data mining.

Predicting student enrollment in higher education institutions is a complex decision making process that is more than merely relying on test scores. Previous research indicate that student enrollment, particularly STEM courses depends on diverse factors such as personal, socio-economic, family and other environmental variables [8], [9]. The scope of this paper is to predict enrollment in STEM disciplines and to determine the factors that influence the enrollment of students, using data mining techniques.

Ensemble classification has received much attention in the machine learning community and has demonstrated promising capabilities in improving classification accuracy. Ensemble methods combine multiple models into one usually more accurate than the best of its components. In this paper, we suggest an ensemble classifier framework for assessing and predicting student enrollment in STEM courses in Higher Education Institutions. The study focuses on improving the quality of student enrollment training data by identifying and eliminating mislabeled instances by using multiple classification algorithms.

The rest of the paper is organized as follows: Section II describes the related works including ensemble methods in machine learning and related empirical studies on educational data mining using ensemble methods. Section III describes the methodology used in this study and the experiment conducted. Section IV presents results and discussion. Finally, section V presents the conclusions of the study.

2. ENSEMBLE CLASSIFICATION

Ensemble modeling has been the most influential development in Data Mining and Machine Learning in the past decade. The approach includes combining multiple analytical models and then synthesizing the results into one usually more accurate than the best of its components [9]. An ensemble of classifiers blends predictions from multiple models with two goals: The first goal is to boost the overall prediction accuracy compared to a single classifier and the second one is to achieve a better generalizability owing to different specialized classifiers. Consequently, an ensemble can find solutions where a single prediction model would have difficulties. The main underlying principle is that an ensemble can select a set of hypotheses out of a much larger hypothesis space and combine their predictions into one [10]. The philosophy of the ensemble classifier is that another base classifier compensates the errors made by one base classifier. The following sub sections details different base classifiers and the ensemble classifiers.

2.1 Base Classifiers

Rahman and Tasnim [11] describe base classifiers as individual classifiers used to construct the ensemble classifiers. The following are the common base classifiers: (1) Decision Tree Induction – Classification via a divide and conquer approach that creates structured nodes and leafs from the dataset. (2) Logistics Regression – Classification via extension of the idea of linear regression to situations where outcome variables are categorical. (3) Nearest Neighbor – Classification of objects via a majority vote of its neighbors, with the object being assigned to the class most common. (4) Neural Networks – Classification by use of artificial neural networks. (5) Naïve Bayes Methods – Probabilistic methods of classification based on Bayes Theorem, and (6) Support Vector Machines – Use of hyper-planes to separate different instances into their respective classes.

2.2 Ensemble Classifiers

Many methods for constructing ensembles have been developed. Rahman and Verma [12] argued that ensemble classifier generation methods can be broadly classified into six groups that that are based on (i) manipulation of the training parameters, (ii) manipulation of the error function, (iii) manipulation of the feature space, (iv) manipulation of the output labels, (v) clustering, and (vi) manipulation of the training patterns.

2.2.1 Manipulation of the Training Parameters

The first method for constructing ensembles manipulates the training data set to generate multiple hypotheses. The learning algorithm is run several times, each time with a different subset of the training data set [13]. This technique works especially well for unstable learning algorithms whose output classifier undergoes major changes in response to small changes in the training data: Decision tree, neural network, and rule learning algorithms are all unstable, linear regression, nearest neighbor, and linear threshold algorithms are generally very stable. Different network weights are used to train the base neural network learning process [11]. These methods achieve better generalization.

2.2.2 Manipulation of the Error Function

The second method for constructing ensembles is by augmenting the error function of the base classifiers. In this case, an error is imposed if base classifiers make identical errors on similar patterns [11]. An example of such an ensemble is the Negative correlation learning. The idea behind negative correlation learning is to encourage different individual networks in an ensemble to learn different parts or aspects of a training data so that the ensemble can learn the whole training data better [14].

2.2.3 Manipulation of the Feature Space

The third general technique for generating multiple classifiers is to manipulate the set of input features (feature subsets) available to the learning algorithm. According to Dietterich [13] this technique only works when the input features are highly redundant.

2.2.4 Manipulation of the Output Labels

A fourth general technique for constructing an ensemble of classifiers is to manipulate the output targets. Each base classifier is generated by switching the class labels of a fraction of training patterns that are selected at random from the original training data set [12]. Each member of each class receives a vote and the class with the most votes is the prediction of the ensemble.

2.2.5 Ensemble Classifier Generation by Clustering

Another method of generating ensemble classifiers is by partitioning the training data set into non-overlapping clusters and training base classifiers on them [12] and the patterns that tend to stay close in Euclidean space naturally are identified by this process [13]. A pattern can belong to one cluster only therefore; a selection approach is followed for obtaining the ensemble class decision. These methods aim to reduce the learning complexity of large data sets

2.2.6 Manipulation of the Training Patterns

The last method for constructing ensembles is by manipulating the training patterns whereby the base classifiers are trained on different subsets of the training patterns [12]. The largest set of ensembles are built with different learning parameters, such as number of neighbors in a k Nearest Neighbor rule, and initial weights in a Multi Layer Perceptron.

3. RELATED EMPIRICAL STUDIES

Stapel, Zheng, and Pinkwart [15] study investigated an approach that decomposes the math content structure underlying an online math learning platform, trains specialized classifiers on the resulting activity scopes and uses those classifiers in an ensemble to predict student performance on learning objectives. The study results suggested that the approach yields a robust performance prediction setup that can correctly classify 73.5% of the students in the dataset. This was an improvement over every other classification approach that they tested in their study. Further examinations revealed that the ensemble also outperforms the best single-scope classifier in an early prediction or early warning setting.

In their study, Satyanarayana and Nuckowski [16] used multiple classifiers (Decision Trees-J48, Naïve Bayes and Random Forest) to improve the quality of student data by eliminating noisy instances, and hence improving predictive accuracy. The results showed that student data when filtered can show a huge improvement in predictive accuracy. The study also compared single filters with ensemble filters and showed that using ensemble filters works better for identifying and eliminating noisy instances.

Pardos, Gowda, Baker, and Heffernan [17] study investigated the effectiveness of ensemble methods to improve prediction of post-test scores for students using a Cognitive Tutor for Genetics. Nine algorithms for predicting latent student knowledge in the post-test were used. The study found that ensembling at the level of the post-test rather than at the level of performance within the tutor software resulted to poor prediction of the post-test, based on past successes of combined algorithms at predicting the post-test. The study gave a few possible reasons for this. First of all, the data set used in this study was relatively small, with only 76 students. Ensembling methods can be expected to be more effective for larger data sets, as more complex models can only achieve optimal performance for large data sets. This is a general problem for analyses of post-test prediction.

In their study, Shradha and Gayathri [18] used educational data mining to analyze why the post-graduate students' performance was going down and overcome the problem of low grades at AIMIT College, Mangalore, India for the academic year 2014-2015. In their study, they compared base classifiers with an ensemble model. The study used J48, Decision Table and Naïve Bayes as base classifers and bagging ensemble model. The study concluded that J48 algorithm was doing better than the Naïve Bayesian. Also, bagging ensemble technique provided accuracy which was comparable to J48. Hence, this approach could aid the institution to find out means to enhance their students' performance.

4. METHODOLOGY

4.1 Study Design

This study adapted the Cross Industry Standard Process for Data Mining (CRISP-DM) process model suggested by Nisbet, Elder and Miner [19] as a guiding framework. The framework breaks down a data mining project in phases which allow the building and implementation of a data mining model to be used in a real environment, helping to support business decisions. Figure I give an overview of the key stages in the adapted methodology.

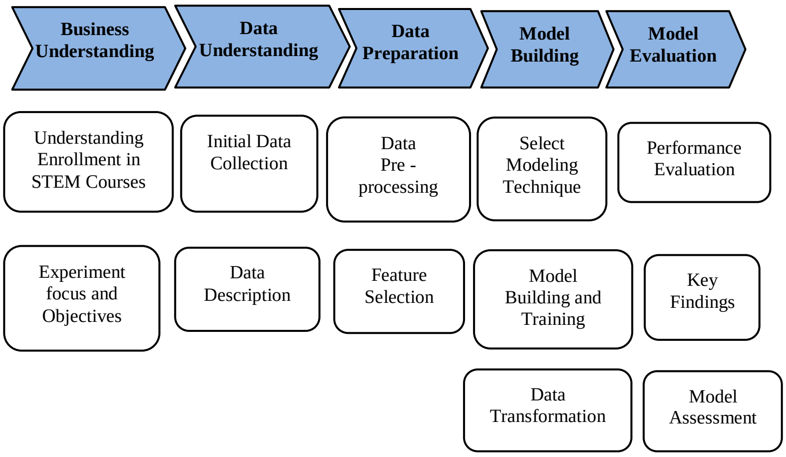


Figure I: Adapted Methodology for Research Implementation

4.1.1 Business Understanding

This phase begins with the setting up of goals for the data mining project. The goal of this stage of the process is to uncover important factors that could influence the outcome of the project [19]. Some of the activities in this stage include identifying the target variable, listing all the important predictor variables, acquiring the suitable institutional dataset for analyses and modeling, and generating descriptive statistics for some variables.

4.1.2 Data Understanding

Data understanding phase starts with data collection and getting used to the data to identify potential patterns in the data. This stage involves activities including data acquirement, data integration, initial data description, and data quality assessment activities. Data has to be acquired before it can be used. The data set used in this study was collected through the questionnaire survey at Murang'a University of Technology, a Public University in Kenya.

4.1.3 Data preparation

Data preparation is the phase of the data mining project that covers all activities needed to construct the final dataset. Initially the dataset was collected in Ms Excel sheet and preprocessing done. Feature selection was used as a method to select relevant attributes (or features) from the full set of attributes as a measure of dimensionality reduction. Two statistical methods were adopted to determine the importance of each independent variable. These methods include Chi-Square Attribute evaluation and Information Gain Attribute evaluation.

4.1.4 Modeling

This phase in data mining project involves building and selecting models. The usual practice is to create a series of models using different statistical algorithms or data mining techniques. The open source software WEKA, offering a wide range of machine learning algorithms for Data Mining tasks, was used as a data mining tool for the research implementation. The selected attributes were transformed into a form acceptable to WEKA.

4.1.5 Evaluation

This stage involves considering various models and choosing the best one based on their predictive performance. The resultant models, namely J48, Naïve Bayes, and CART were evaluated alongside bagging. Classification accuracy of the models was calculated based on the percentage of total prediction that was correct.

4.2 Experiment

4.2.1 Data Collection

Data was collected from sampled students through a personally administered structured questionnaire at Murang'a University of Technology, Kenya for the academic year 2016-2017. The target population was grouped into two mutually exclusive groups namely; STEM (Science, Technology, Engineering and Mathematics) and non-STEM Majors. Aside from the demographic data, data about their interests and motivations to enroll in the courses of their choice, academic qualification and educational contexts was collected. Table I shows the identified attributes and possible values that were taken as an input for our analysis.

Table I: Factors affecting Students Enrollment in STEM

S/No	Attribute	Possible Values
1	Career Flexibility	{Yes, No}
2	High School Final Grade	{A,A-,B+,B,B-,C+}
3	Math Grade	{A,A-,B+,B,B-,C+}
4	Pre - University awareness	{Yes, No}
5	Teacher Inspiration	{Yes, No}
6	Financial Aid	{Yes, No}
7	Extracurricular	{Yes, No}
8	Societal Expectation	{Yes, No}
9	Parent Career	{STEM , Non-STEM}
10	Self Efficacy	{Yes, No}
11	Career Earning	{Yes, No}
12	Gender	{Male, Female}
13	Age	Below 20 Years 20 – 25Years 26 – 30 Years 31 and above

14	Family Income	Less than 10,000;
		10,001 – 20,000;
		20,001 – 30,000;
		30,001 – 40,000;
		40,001 – 50,000;
		50,001 and above

4.2.2 Data Transformation

The collected data attributes were transformed into numerical values, where we assigned different numerical values to each of the attribute values. This data was then transformed into forms acceptable to WEKA data mining software. The data file was saved in Comma Separated Value (CSV) file format in Microsoft excel and later was converted to Attribute Relation File Format (ARFF) file inside WEKA software for easy use.

4.2.3 Data Modeling

To find the main reasons that affects the students' choice to enroll in STEM courses the study used three base classification algorithms together with an ensemble model method, so that we can find accurate or exact factors affecting students' enrollment in STEM. Using algorithms in ensemble model, we will find the actual factors that effects students' choice to enroll in STEM. The following are the methods that we were using for classification:-

4.2.3.1 J48 Algorithm

J48 is a decision tree algorithm and an open source Java implementation of the C4.5 algorithm in the Weka data mining tool. In order to classify a new item, the algorithm first needs to create a decision tree based on the attribute values of the available training data. So, whenever it encounters a set of items (training set) it identifies the attribute that discriminates the various instances most clearly.

4.2.3.2 Naïve Bayes Algorithm

The Naïve Bayes algorithm is a simple probabilistic classifier that calculates a set of probabilities by counting the frequency and combinations of values in a given dataset [20]. The Naive Bayesian classifier is based on the Bayes' theorem with independence assumptions between predictors.

4.2.3.3 CART

Classification and Regression Tree (CART) is one of the commonly used Decision Tree algorithms. It is a recursive algorithm, which partitions the training dataset by doing binary splits. At each level of the decision tree, the algorithm identify a condition - which variable and level to be used for splitting input node (data sample) into two child nodes.

4.2.3.4 Bagging

Bagging is the technique that combines the predictions from multiple machine learning algorithms together to make more accurate predictions than any individual model. Bagging algorithm uses bootstrap samples to build the base predictors. Each bootstrap sample of *m* instances is formed by uniformly sampling m instances from the training dataset with replacement.

5. RESULTS AND DISCUSSION

We collected students' information by distributing structured questionnaire among 220 students and 209 responses were collected. This data was preprocessed and recorded into Microsoft Excel file and then through online conversion tool, the Excel file was converted into .arff file which is supported by the WEKA software tool [21]. We used Weka 3.6 software for our analysis. Table II shows the results obtained from the experiment.

Table II: Comparison of Algorithms

S/No	Algorithm	Correctly Classified instances (%)	Incorrectly Classified instances (%)
1	J48	84	16
2	CART	77	23
3	Naïve Bayes	72	28
4	Bagging	82	18

The information on Table II shows comparison details of the algorithms that were used in our analysis. When we compared the models, we found that the J48 Algorithm correctly classified 84% of the instances and 16% of the instances incorrectly classified. The classification error is less compared to the other two baseline classification algorithm, that is, CART (23% Incorrectly Classified Instances) and Naïve Bayes (28% Incorrectly Classified Instances). From these results we can conclude that among the three base classification algorithms that we used J48 algorithm was best suited for predicting enrollment of students in STEM courses.
We observed in the experiments with the baseline classifiers, that their classification accuracy can vary a lot based on random sampling of the training and test data. One of the reasons for this instability is because the base classifiers are highly susceptible to noisy training data and have a tendency to overfit.

To reduce chances of over-fitting, the most popular and simple techniques is called ensemble learning where multiple models are trained and their results are combined together in some way. One of the most popular methods is called bagging. In bagging, samples of the training data are bootstrapped. In other words, the samples are selected with replacement from the original training set.

The models are trained on each sample. Bagging makes each training set different with an emphasis on different training instances. In this study, bagging ensemble model was developed that gave 82% of Correctly Classified Instances.

Table III shows the attributes and the values obtained by applying the Karl Pearson Co-efficient Technique.

Table III: Values obtained by Karl Pearson Co-efficient Technique

S/No	Attribute	Coefficient of Determination (R^2) Value
1	High School Final Grade	0.981
2	Career Flexibility	0.842
3	Math Grade	0.763
4	Self Efficacy	0.714
5	Teacher Inspiration	0.692

The results from Table III show the five most significant attributes that highly affects the students choice to enroll in STEM courses in the University. These are the attributes that we can consider as factors which the institutions must focus on while considering enrollment of students in STEM related courses.

6. CONCLUSIONS

There are many factors that may affect students' choice to enroll and pursue a career in STEM in higher education institutions. These factors can be used during the admission process to ensure that students are admitted in the courses that best fit them. To categorize the students' based on the association between choice to enroll in a STEM major and attributes, a good classification is needed. In addition, rather than depending on the outcome of a single technique, ensemble model could do better. In our analysis, we found that J48 algorithm is doing better than Naïve Bayesian and the CART algorithms.

Also, the study results demonstrated that bagging technique provides accuracy which is comparable to J48. Moreover, the correlation between the attributes and the choice to enroll in STEM courses was computed and found that five significant attributes were highly affecting the students' choice to enroll in STEM courses. These attributes include the score obtained from the high school final exam, student score in Mathematics subject, expected career flexibility, belief in the ability to succeed in a STEM related career, and the inspiration from the high school teacher. Therefore, this approach could help institutions of higher learning to find out means to enhance student enrollment in STEM disciplines.]

In future work, the effects of using different base classifiers alongside other ensemble algorithms on classification accuracy and execution time as parameters can be investigated.

7. REFERENCES

[1] Lichtenberger, E. and George-Jackson, C. “Predicting High School Students’ Interest in Majoring in a STEM Field: Insight into High School Students’ Postsecondary Plans,” *Journal of Career and Technical Education, 28*(1), 19-38, 2013.

[2] Kulkarni, S., Rampure, G., and Yadav, B. “Understanding Educational Data Mining (EDM),” *International Journal of Electronics and Computer Science Engineering*, 2(2), 773-777, 2013.

[3] Baker, R. and Yacef, K. “The State of Educational Data mining in 2009: A Review and Future Visions, “ *Journal of Educational Data Mining, 1*(1), 3-17, October, 2009.

[4] Romero, C. and Ventura, S. “Educational Data Mining: A Review of the State of the Art,” *Systems, Man, and Cybernetics,Part C: Applications and Reviews, IEEE Transactions, 40*(6), 601-618, 2010.

[5] Sarala, V. and Krishnaiah, J. “Empirical Study of Data Mining Techniques in Education System,” *International Journal of Advances in Computer Science and Technology (IJACST)*, 15-21, 2015.

[6] Baradwaj, B. and Pal, S. “Mining Educational Data to Analyze Students’ Performance,” *International Journal of Advanced Computer Science and Applications, 2*(6), 63-69, 2011.

[7] Namdeo,V., Singh, A., Singh, D. and Jain, R. “RESULT ANALYSIS USING CLASSIFICATION,” *International Journal of Computer Applications, 1*(22), 22-26, 2010.

[8] Nandeshwar, A. andChaudhari, S. *Enrollment Prediction Models Using Data Mining.* [Unpublished], April 22, 2009.

[9] Wang, X. “Modeling Entrance into STEM Fields of Study among Students Beginning at Beginning at Community Colleges and Four-Year Institutions,” *Research in Higher Education*, 54 (6), 664-669, September, 2013.

[10] Rokach, L. “Ensemble-based classifiers,” *Artificial Intelligence Review*, 33, 1-39, 2010.

[11] Rahman, A. and Tasnim, S. “Ensemble classifiers and their applications: A review,” *International Journal of Computer Trends and Technology*, 10(1), 31-35, 2014.

[12] Rahman, A. and Verma, B. “Ensemble Classifier Generation using Non–uniform Layered Clustering and Genetic Algorithm,” *Elsevier Knowledge Based Systems*, 43, 30-42, May, 2013.

[13] Dietterich, G. T. (n.d.), *Ensemble Methods in Machine Learning.* Retrieved November 2016, from web.engr.oregonstate.edu/~tgd/publications/mcs-ensembles.pdf

[14] Liua, Y. and Yao, X. “Ensemble learning via negative correlation,” *Neural Networks, 12*, 1399-1404, 1999.

[15] Stapel, M., Zheng, Z. and Pinkwart, N. “An Ensemble Method to Predict Student Performance in an Online Math Learning Environment,” *Proceedings of the 9th International Conference on Educational Data Mining*, pp. 231-238, 2016.

[16] Satyanarayana, A. and Nuckowski, M. “Data Mining using Ensemble Classifiers for Improved Prediction of Student Academic Performance,” *ASEE Mid-Atlantic Section Spring 2016 Conference.* Washington D.C: George Washington University, April 8-9, 2016.

[17] Pardos, Z., Gowda, S., Baker, R., and Heffernan, N. “Ensembling Predictions of Student Post-Test Scores for an Intelligent Tutoring System,” *Educational Data Mining*, 2011.

[18] Shradha, S. and Gayathri, “Approach for Predicting Student Performance Using Ensemble Model Method,” *International Journal of Innovative Research in Computer and Communication Engineering, 2*(Special Issue 5), 161-169, October, 2014.

[19] Nisbet, R., Elder, J., and Miner, G. *Handbook of statistical analysis and data mining applications.* Amsterdam: Elsevier, 2009.

[20] Sage, S. and Langley, P. “Induction of Selective Bayesian Clasifiers,” *ARXIV*, pp. 399- 406, 2013.

[21] School, W. (2015). *Introduction to Weka - A Toolkit for Machine Learning.* Retrieved April 22, 2015, from http://www.iasri.res.in: http://www.iasri.res.in/ebook/win_school_aa/notes/WEKA.pdf

Stephen Kahara Wanjau currently serves as the Director of ICT at Murang’a University of Technology, Kenya. He received his BSc. degree in Information Sciences from Moi University, Kenya in 2006 and a Master of Science degree in Organizational Development from the United States International University – Africa in 2010. He is a master student in the Department of Computing, School of Computing and IT at Jomo Kenyatta University of Agriculture and Technology, Kenya. His research interests are machine learning, artificial intelligence, Knowledge management, and cloud computing.

Geoffrey Muchiri Muketha is Associate Professor of Computer Science & Dean of School of Computing and Information Technology at Murang'a University of Technology. He received his BSc. degree in Information Sciences from Moi University, Kenya, his MSc. degree in Computer Science from Periyar University, India, and his PhD degree in Software Engineering from Universiti Putra Malaysia. His research interests are software metrics, software quality and intelligent systems.

International Journal of Computer Applications Technology and Research
Volume 7–Issue 03, 129-132, 2018, ISSN:-2319–8656

Malware Family Detection Approach using Image Processing Techniques: Visualization Technique

Poonam Parmuval
Department of Computer Engineering
BVM Engineering College, V.V.Nagar, India

Mosin Hasan
Department of Computer Engineering
BVM Engineering College, V.V.Nagar, India

Samip Patel
Department of Computer Engineering
BVM Engineering College, V.V.Nagar, India

Abstract: - The risk of malicious software has increased a lot since last decade as the use of internet has increased drastically. According to Avast Test report, 22,000 to 25,000 new malware have been reported every day. Even though huge malwares having different structures are introduced every day, their nature of working is almost similar to old malwares. The malwares with the similar functionalities are considered to be the member of the same family. Classification and detection of malware family are important to design its signature of anti-malware software. In this article, we represent the concise study carried out on detecting various malware family. This paper mainly focus on visualization technique for classifying malware family. Visualization technique uses image processing approaches to classify the malwares. The malware executable binary files are transformed into image and this images are used to detect the family of malware.

Keywords: - Malwares, Malware Family, Malware Visualization, Malware Detection, Malware family classification

1. INTRODUCTION

Nowadays it becomes difficult to live without mobile, internet, computers. As the digital world grows today the security and protection of computer system have become biggest concern. Malware: Malware is malevolent software which is designed to breach the security of the system or to harm the computer’s operating system [1] [2]. Harms caused by malwares can be stealing personal information, locking file system, password stealing, showing unwanted content, etc. This malwares are classified into different types.

Adware: Adware is an advertisement-focused application that installs themselves on systems [2].

Spyware: It spies on activities performed by victims and tracks the internet activities to send an advertisement to the system [2].

Virus: It is contagious code that link itself to another software and then regenerates itself [2] [3].

Worm: Worms are the self-replicating code that deletes or corrupts the files on the computer. It works to eat operating system files and data files [2].

Trojan: It arrives as useful to the user and tries to enter into victims system. It discovers personal information (financial).

Ransomware: Ransomware is introduced to lock the data of victim. Then attacker demands to pay for unlocking data [2].

Rootkit: Attacker would gain root permissions and install various applications and utilities (maybe malicious), called "kit," on the victim’s system [4].

Key loggers: It note every key press on the keyboard and gains the important information like username, password, and email content, etc.

1.1 Malware Family

Many approaches have been made to detect and prevent malwares but the attacker advances their technique and develops many new malwares. This makes the traditional anti-virus software difficult to resist the violation of malicious codes. According to AV-Test Report approx. 250,000 new malwares have been reported every day [5]. The new malwares are generated from the previous malwares with the help of techniques like encryption, obfuscation, mutation, etc. [1]. This have been proved by researchers working on malware. The variants can also be generated using executable packers. Packer is a utility that applies compression and encryption on executables to make them undetectable by malware scanners [6]. The attackers generate many new variants of malware by modifying the code or by using the packers to evade the detection by current anti-malware software. Though the variants seem new to anti-malware, their functionalities remain similar to old malwares. The malwares with similar functionalities are considered to be the member of the same family [1].

The following are few family of malwares [1].

Agent: Agent is family that most of its variant download and install adware or malware on the attacked system. It may also change the configuration properties for Windows [7].

Allaple: Win32/Allaple is network worm family that spread to other devices connected to a LAN and perform denial-of-service (DoS) attacks [8].

Fakerean: This family of security program pretends to examine your system against malware, and generate a report that shows lots of malwares. The program will demand money to scan deeply [8].

Rbot: Rbot is a family of backdoor malwares who allows attackers to control victim's computers [9].

C2LOP: It is a Trojan family that changes browser settings, a bookmark to advertisements, show advertisements [9].

Once the malware family is detected, it becomes easy to know the vulnerabilities of the malware and hence easy to prevent it. To prevent such malicious attacks many defensive techniques have been developed. But the group of attackers comes up with the new solutions to evade these defence techniques and generate thousands of new variants. So it continuously required to identify all new malwares and find their solutions.

1.2 Malware Detection Techniques

The techniques for malware detection are broadly classified into '*static analysis'* and '*dynamic analysis'.*

Static Analysis:

Analysing malware without running them are considered as Static analysis [10]. This approach includes Signature-based, Permission-based, and Component-based analysis. The Signature-based method extracts the semantic patterns from malware and generates a unique signature to match particular malware [3]. It won't detect the variant or unknown malware. The Permission-based method identifies dangerous permission requested by malware to detect malware [10]. The Component-based method disassembles the malware to extract and analyse the important components (i.e. opcodes, activities, services, receivers etc.), for identification of the vulnerable attacks. The major limitation of the static analysis strategy is that these techniques fail to identify malicious behaviour obfuscated malware [10].

Dynamic Analysis:

In dynamic analysis, the behaviour of malicious code is observed and noted by running the malware executable in a virtual environment or emulator [10] [11]. It monitors the system level calls and the attributes. These strategies give more accurate result than static analysis but it is the time-consuming process as it requires several executions in a virtual machine [11].

2. VISUALIZATION TECHNIQUE

Dynamic analysis can identify malwares more accurately but it is very time consuming process. L. Nataraj [1] has proposed a technique which depend on image processing methods to classify malware families. This technique is called Visualization technique. The malware executable binary files or PE files are converted into image and this image is used to identify the type of malware.

Visualization technique has two main strands. One focuses in Dataset and dataset generation technique and second focuses on image processing aspect.

2.1 Data Set for Malware family:

Maligm dataset comprises of 9339 malware samples distributed in 25 malware families with the varying number of variants per family [1]. It contains malwares in form of grayscale images.

Table 1 Malimg Dataset families

No.	Class	Family Name	No. of Variants
1	Worm	Allaple.L	1591
2	Worm	Allaple.A	2949
3	Worm	Yuner.A	800
4	PWS	Lolyda.AA 1	213
5	PWS	Lolyda.AA 2	184
6	PWS	Lolyda.AA 3	123
7	Trojan	C2Lop.P	146
8	Trojan	C2Lop.gen!G	200
9	Dialer	Instant access	431
10	Trojan-Downloader	Swizzor.gen!I	132
11	Trojan-Downloader	Swizzor.gen!E	128
12	Worm	VB.AT	408
13	Rogue	Fakerean	381
14	Trojan	Alueron.gen!J	198
15	Trojan	Malex.gen!J	136
16	PWS	Lolyda.AT	159
17	Dialer	Adialer.C	125
18	Trojan-Downloader	Wintrim.BX	97
19	Dialer	Dialplatform.B	177
20	Trojan-Downloader	Dontovo.A	162
21	Trojan-Downloader	Obfuscator.AD	142
22	Backdoor	Agent.FYI	116
23	Worm:AutoIT	Autorun.K	106
24	Backdoor	Rbot!gen	158
25	Trojan	Skintrim.N	80

2.2 Image Processing

This strand is divided in three phases that are Malware image generation, Feature extraction and classification.

2.2.1 Malware Image Generation

The malware binaries are grouped into 8-bit vectors which represent hex value from 00 to FF. These vectors are

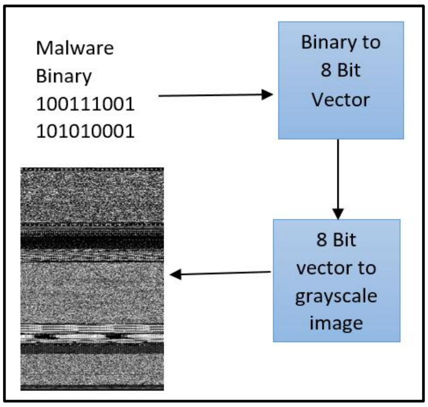


Fig 1. Malware Binary to image [1]

represented as pixel values i.e. intensity of grayscale image

ranging from 0-255 [1]. The width of the images are predefined but the height of images are allowed to vary based on size. By visualizing malware as image one can notice that the malware variants that are the member of the same family show structural and visual similarity [1]. Along with that, it is also noticed that the malware variant from different family shows structural and visual dissimilarities.

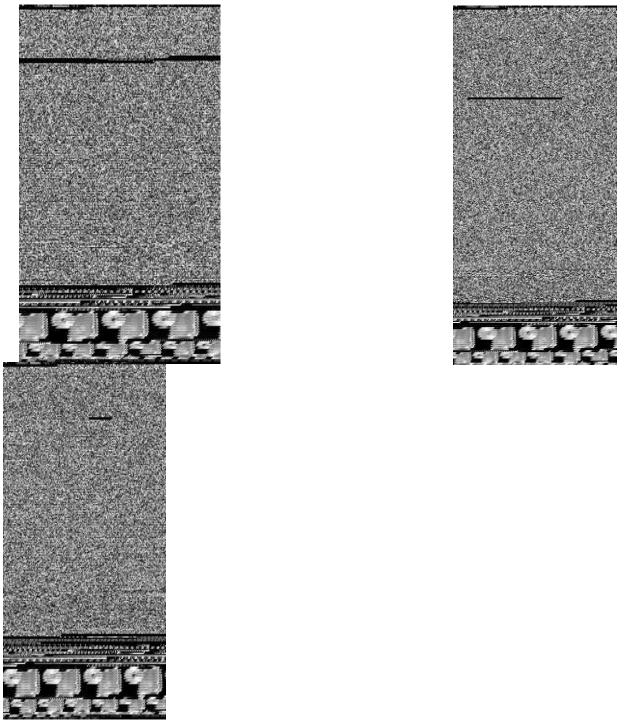


Fig 2. Variants of Fakrean family

2.2.2 Feature Extraction

The features of images are used to classify the malwares into their family. The features can be texture pattern, frequencies in image, intensity, colour feature, etc. These features are gathered by computing mean, standard deviation, Euclidean Distance, etc [6]. For the image. Many algorithms like CLD (Colour Layout Descriptor), HTD (Homogeneous Texture Descriptor), GIST are available to fetch different features of the image and generate the feature vector.

2.2.3 Classification

This feature vector can be applied to any classifier to identify the family of malware. The classifier can be SVM (Support vector machine), K-mean classifier, neural network, etc.

The main reason for using visualization method is, that execution of binary is not required [1]. It is independent of operating system.

3. RELATED WORK

Nataraj, Jacob, et al. [1] describe visualization technique for malware classification which is based on image processing. Greyscale image called malware image is generated from executable binary files. This shows that there exist structural similarities between malware of same family [1]. It uses GIST algorithm for obtaining feature vector from malware image. The feature vector is provided to K-mean classifier for classification. The author obtains accuracy of 0.9718 by using this strategy that works without executing any the malware binary.

Nataraj, Yegneswaran et al. [11] shows comparative study between dynamic analysis of malware and malware image analysis. Their experiments prove that the image based method is more efficient and useful than dynamic analysis.

Nataraj, Manjunath, et al. [6] developed a system called SARVAM. It is content based system for searching retrieving matching images from large databases. The content of a query object is used to find similar objects in a larger database [6]. During the initial phase, first, it generates the fingerprint of a large set of malware image samples using GIST. It obtains the Antivirus (AV) labels that are used to describe nature of malware from Virustotal, and uses Nearest Neighbours (NN) algorithm to extract similar fingerprints. To increase the efficiency of Nearest Neighbour method Balltree structure is used. During the second phase i.e. querying, it compute the fingerprints of the new samples and match it with the existing fingerprints in the database to retrieve the top matches [6].

Hasan [3] describe malware, impacts of malware, various malware and their identification and prevention techniques like signature-based and heuristic method and limitations of this techniques. The author concludes that traditional malware identification techniques and anti-malware techniques are not sufficient. New techniques have to be developed for obfuscated malwares [3].

LIU et al. [12] described an efficient static method to detect and classify malware variants. It works in two stages: first is feature extraction; the other is classification. For extracting features the executable files are translated into controlled disassembly files and then mapped into the grayscale images (0-255 pixel range) by dividing a file into 8-bit blocks. Then, a local mean method is applied to compact the gray-scale images to improve the efficiency. Each pixels of this image represent a feature of that malware [12]. Finally, they uses K-mean and the diversity selection based novel ensemble learning to classify malware. Ensemble learning is a method which assemble multiple weak classifiers to build single strong classifier [12].

Kancherla et al. [13] presented a visualization based method for malware detection. The binary executable file is converted to 8-bit 1-dimensional vector. One vector represents the intensity of one pixel of the image. The image width is kept fixed on basis of the size of the file. Later, it extracts low-level features. They have extracted three different sets of features: Intensity-based (average intensity, no. of pixels with same intensity), Wavelet-based (Horizontal, Diagonal and Vertical coefficients) and Gabor based features (specific frequency content) [13]. Then apply those features to SVM (support vector machine) algorithm for malware detection and classification. This method does not need to unpacking or decryption.

Zainudeen et al. [14] shows a new dynamic analysis technique that work by highlighting the behaviour of malware for malware visualization. This technique represents the malware behaviour in the images (called behaviour image). It starts with monitoring API calls i.e. malware behaviour by executing malware in a VM [14]. Behaviour- to- colour map is generated to represent malicious features of malware. Behaviour – to – colour mapping is done by grouping and sorting APIs based on the level of the maliciousness. Here hot- to- cold colour ramp is used to assign colours (RGB Colour model) to APIs [14]. Hot colours (e.g. red, orange, etc.) represents malicious APIs and the cold colours (e.g. cyan,) represent APIs that are non-malicious. Using this map generate the behaviour image by assigning colours to each captured behaviour i.e. APIs. They noted that variants of a family have recognizable similar pattern even if they have different size and hashes [14].

Zhang et al. [15] developed a technique to classify malware using opcode. They disassemble executable files into opcodes sequences and then converts the opcodes into images. First, they decompile the unpacked binaries to extract their opcodes sequences. Now for each executable, it generate an opcode profile, where each profile contains a list of the opcode sequences with length 2 and their frequencies [15]. Each pixel is a multiplication with the probability of the opcodes sequence and its information gain. To make images easier to recognized and classified it histogram normalization, erosion and dilation are applied. Finally, uses the convolutional neural network (CNN) for identification and classification of malware images.

Mohanaiah et al. [16] present an application of GLCM to get texture based features. GLCM stand for “grey level co-occurrence matrix”. They compute features like ‘Angular second moment’ (ASM), ‘Inverse difference moment’ (IDM), correlation, and Entropy.

4. CONCLUSION

Based on the above study it can be concluded that the malwares are growing continuously so it is required to develop or to improve current techniques to handle malware attacks. The visualization based technique is proved to be the current trend for malware detection as in this technique there is no requirement of executing malware. It eliminates need of emulator and efficient for new malware detection.

5. FUTURE WORK

The current research is made on grey scale image. It is possible to elaborate the work towards the coloured image. The research can be extended towards reducing time and space by compressing the feature vector size and finding a specific highly matching region on the image.

6. REFERENCES

[1] L. Nataraj, S. Karthikeyan, J. Gregoire and B. S. Manjunath, "Malware Images: Visualization and Automatic Classification," in *International Symposium on Visualization for Cyber Security*, pittsburgh, usa, 2011.

[2] N. DuPaul, "Common Malware Types: " ,12 October 2012. [Online]. Available: https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101. [Accessed 20 December 2017].

[3] M. Hasan, "Boyer Moore Algorithm Application in Malware Detection," *International Journal of Scientific Research in Engineering*, vol. I, pp. 69-77, 2017.

[4] Wikipedia, "Rootkit," 12 December 2017. [Online]. Available: https://en.wikipedia.org/wiki/Rootkit. [Accessed 20 December 2017].

[5] The AV-TEST Institute, "www.av-test.org," 10 January 2018. [Online]. Available: https://www.av-test.org/en/statistics/malware/. [Accessed 20 January 2018].

[6] L. Nataraj, B. Manjunathan, D. Kirat and Giova, "SARVAM: Search And RetrieVAl of Malware," in *Annual Computer Security Applications Conference (ACSAC)*, 2013.

[7] F-secure LAb, "Win32/Agent," [Online]. Available: https://www.f-secure.com/v-descs/agent.shtml. [Accessed December 2017].

[8] F- Secure Lab, "Virus," 18 November 2011. [Online]. Available: https://www.f-secure.com/v-descs/. [Accessed December 2017].

[9] "Win32/Rbot," 16 April 2011. [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Rbot. [Accessed 21 December 2017].

[10] Wikipedia, "Malware analysis," 24 September 2017. [Online]. Available: https://en.wikipedia.org/wiki/Malware_analysis. [Accessed 22 December 2017].

[11] L. Nataraj, V. Yegneswaran and P. Porras, "A Comparative Assessment of Malware Classification using Binary Texture Analysis and Dynamic Analysis," in *Workshop on Artificial Intelligence and Security (AISec)*, Chicago, 2011.

[12] L. LIU and B. WANG, "Malware Classification Using Gray-Scale Image and Ensemble Learning," in *International Conference on System and Informatics*, 2016.

[13] K. Kancherla and S. Mukkamala, "Image Visualization based Malware Detection," in *Symposium on Computational Intelligence in Cyber Security (CICS)*, 2013.

[14] S. Zainudeen and M. A. Maarof, "Malware Behavior Image for Malware Variant," in *International Symposium on Biometric and Security Technologies (ISBAST)*, 2014.

[15] J. Zhang, Z. Qin, H. Yin, L. Ou and Y. Hu, "IRMD: Malware variant Detection using opcode," in *International Conference on Parallel and Distributed Systems*, 2016.

[16] Mohanaiah , Sathyanarayana and GuruKumar, *International Journal of Scientific and Research Publications*, vol. 3, no. 5, p. Image Texture Feature Extraction Using GLCM, 2013.

International Journal of Computer Applications Technology and Research
Volume 7–Issue 03, 133-138, 2018, ISSN:-2319–8656

Access Control System: A Smart Home Solution

Nermin Hamza *
Faculty of computing and
information technology
King Abdul Aziz University
B.P. 42808 Zip Code 21551
Girl Section, Jeddah, KSA
* Institute of Statistical Studies
and Research, Cairo University
Cairo, Egypt

Amjad Khalid Al-Harthi
Faculty of computing and
information technology
King Abdul Aziz University
B.P. 42808 Zip Code 21551
Girl Section, Jeddah, KSA

Maram Hassan Al-Safri
Faculty of computing and
information technology
King Abdul Aziz University
B.P. 42808 Zip Code 21551
Girl Section, Jeddah, KSA

Abstract- Nowadays, the technological applications have the widest range in our daily life, for instance, automation systems, robotics, and smart home. Smart home is an automated system developed to achieve some actions performed frequently in daily life to obtain more comfortable and easier life environment. Elderly and People has special needs can get benefit from smart home technologies. They can use their mobile to allow their assistance to do many services. In this paper, we proposed a smart home solution based on remote controlling in the house door called Smart Access Control.

The solution allowed to the authorized people to enter their home using their mobiles or just if registered in the system. In addition, it monitors who tries to access the home at any time. The proposed work uses integrated technologies such as face recognition and embedded system together to handle the access permission and the user can administer it remotely by using a mobile application.

Keywords- IOT; smart home; (Raspberry Pi); embedded system and Face recognition

1. INTRODUCTION

Internet of Things (IoT) is a concept and a paradigm that uses the variety of things/objects/ Devices through wireless and wired connections and unique addressing schemes are able to interact with each other and cooperate with other things/objects to create new applications/services and reach common goals. [1]. People are becoming busier and loaded. IOT try to make all home services smarts, and Hardware devices can do their job remotely.

The smart home is technology features that improve quality of life, monitor activities of their peoples. It is a cost-effective way of improving home care. Smart homes are equipped with sensors, and/or monitors. These devices operate in a network connected to a remote center for data collection and processing. [2].

In this proposed work we try to introduce solution help the life to be more easy and smart. The home accessing one of the main Jobs we do every day. People may forget their keys or forget to lock their homes and many security issues are related to who want to access the home.

Our contribution is to propose a solution to enable the homeowners to do many Jobs related to the home Door using their mobile Application called smart access control system. The solution utilizes the face recognition system to identify the authorized people face in order to allow them to access their home like young people or home owners who forget their keys. In addition, it includes a mobile application to let the owner control the access of his building remotely in case of older people cannot able to go and open the door. We apply this solution at Jeddah, KSA.

The paper is organized as follows: The next section gives an overview of Internet of Things and smart home creation and concept. The third section presents the alternative solutions in access control. Section four explains the proposed system, component and architecture. Section five presents the solution description. the discussion will be in section six. it's used Technologies at section seven.

2. IOT OVERVIEW

British technology pioneer Kevin Ashton who the first person used the term "Internet of Things" (IoT) at the early of this century. He described a system in which objects in the physical world could be connected to the Internet by sensors [3]. Internet of Things (IoT) is a concept and a paradigm that considers pervasive presence in the environment of a variety of things/objects that through wireless and wired connections and unique addressing schemes are able to interact with each other and cooperate with other things/objects to create new applications/services and reach common goals. [4] IOT could be wide network of interconnected objects that are unique addressable based on the standard communication protocols. The Internet of Things is based on the fact that the interoperability of the solutions for both the communication and the services must be provided on various platforms. [5];

IoT describes a system where items in the physical world, and sensors within or attached to these items, are connected to the Internet via wireless and wired Internet connections. [6] In IOT the data can be small in size and frequent in transmission. The number of devices, or nodes, that are connecting to the network are also greater in IoT than in traditional PC computing. A S Abdul-Qawy at 2015 [5] determine the key elements of IOT as the following: a) Identification and Addressing, b) Embedded sensors, c) Protocols and Middle ware, d) cloud-based storage and analytic e) Applications and f) Core Hardware. IOT could be used indifferent issues for example: Human like Devices attached or Human Body, Home; at Building where people live, it could be Vehicle as System inside moving Vehicle and finally may be Factories as standard production issue. Marsan at [3] lists Four IOT models: a) Device-to-Device Communications, b) Device-to-Cloud Communications, c) Device-to-Gateway Model and d) Back-End Data-Sharing Model [3].

Homes of the 21st century will become more and more self-controlled and automated due to the comfort it provides, especially when employed in a private home. One of the greatest opportunities still lies ahead in the form of the “smart home”. a smart home is understood as an integration system, which takes advantage of a range of techniques such as computers, network communication as well as produced wiring to connect all indoor subsystems that attach to home appliances and household electrical devices as a whole. [7].

Many existing, well-established home automation systems are based on wired communication. This does not pose a problem until the system is planned well in advance and installed during the physical construction of the building. But Wireless systems can be of great help for automation systems with the advancement of wireless technologies such as Wi-Fi, cloud networks in the recent past, wireless systems are used every day and everywhere [8]. IOT for smart Homes is the solution.

3. PREVIOUS WORK

There are several systems has been published which designed to control the access and few of them are almost similar to our proposed system. In the following sections, we will evaluate some of the related works.

3.1. August Smart Lock

The August Smart Lock was funded by angels and designed by Swiss designer Yves Behar. Users can control and manage the lock with an iOS, Android, or web app. [9],

This system uses smart phone. The limitation of the August Smart Lock is: it is Only available in CA and US, in case of a smartphone out of charge or not have Wi-Fi so, the product doesn’t work properly. when owner proximity of the door then its open automatically via smart phone location.

3.2. Danalock Bluetooth Low Energy Smart Lock

The Danalock outperforms other smart locks by offering both Bluetooth and Z-Wave technologies. Through use, it will automatically unlock the door for the user. [10] This system used also smart phone. In This System People using smartphone to lock or unlock your door.in addition, an owner can share others limited or unlimited access keys for home.

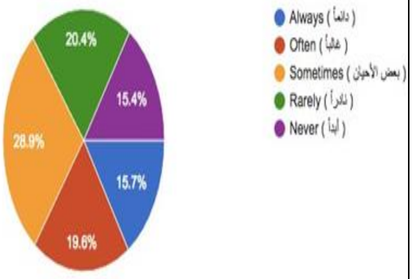
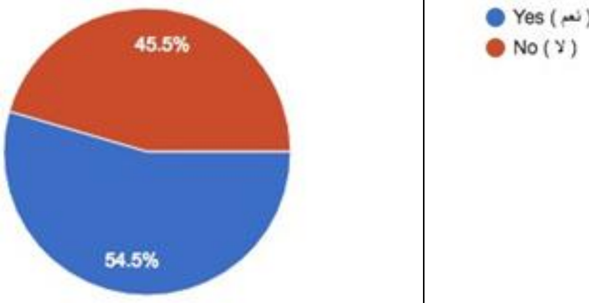
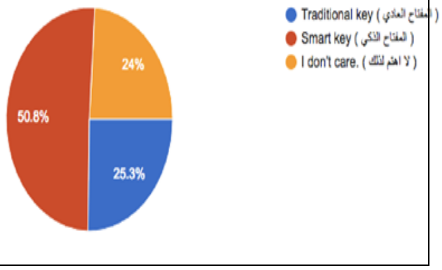
The limitation of this solution is: Opening the door using smartphone via Bluetooth Smart technology.

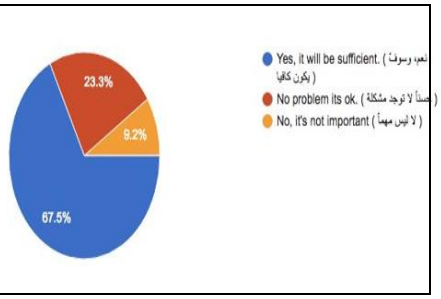
4. THE PROPOSED WORK

First, we start by analysis phase by defining the process of collecting the accurate data, understanding the involved processes, identifying challenges, and recommend logical suggestions to enhance the system functionality in the basis of the system requirements. We gathered the data from questionnaire in order to find the user requirements and create a user profile.

We asked the main questions about gender, old, education etc. in addition we asked about phone platform, concerning about mobile phone service, home dependency of other to open home etc. About 1064 persons response our questionnaire. Table 1 discuss in brief the questions and the statistical answers.

Table 1 Presents Sample of the statistical questionnaires

Question about	Population answers.
Age	88% between 18-25 9.6% between 26-35
Language	99% speak Arabic
Educational	47.5% high school 47.3 % Bachelors
Marital status	90.1 % single 9.9% married
Having children	88% no 12% yes
Platform	80.8% iOS 19.2 % Android
Are you depend on others to open home for you?	
In case you forget a home, key is there any problem you're faced?	
Do you prefer using tradition key or smart?	

Do you like to notify when any one access home?	

We designed the solution based on 3 main components: 1. User (application), 2. Web Server and database engine and 3. The Smart Devices included embedded system. Figure 1 illustrate the system components. This part will discuss the 3 main components as following:

A. User and Application

The End use who has the Application on his/ her mobile. the user is the owner of the building who the only authorized person and who get the permission to enter or refuse also, who can add person to authorized list manually.

B. Database Server

Which is ta Database Engine server connected to both the Application of End user and the Smart Device. The Database store the face pattern for the authorized persons.

C. Smart Device

The smart device is Hardware Device connected with a smart Device include data SIM card to connect with the WIFI, the hardware device is a web camera (high definition) used to capture the face of the guests; the camera is connected with a microcontroller called Raspberry Pi.

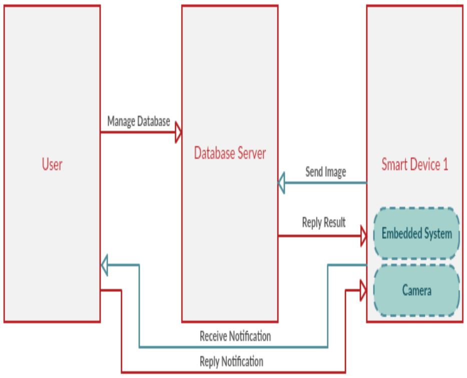


Figure1: (SAC) System components

A use case diagram is the simplest representation of a user's interaction with the system that shows the relationship between the user and the different use cases in which the user is involved. Figure 2 illustrate the use case diagram which has 3 actors and many function requirements.

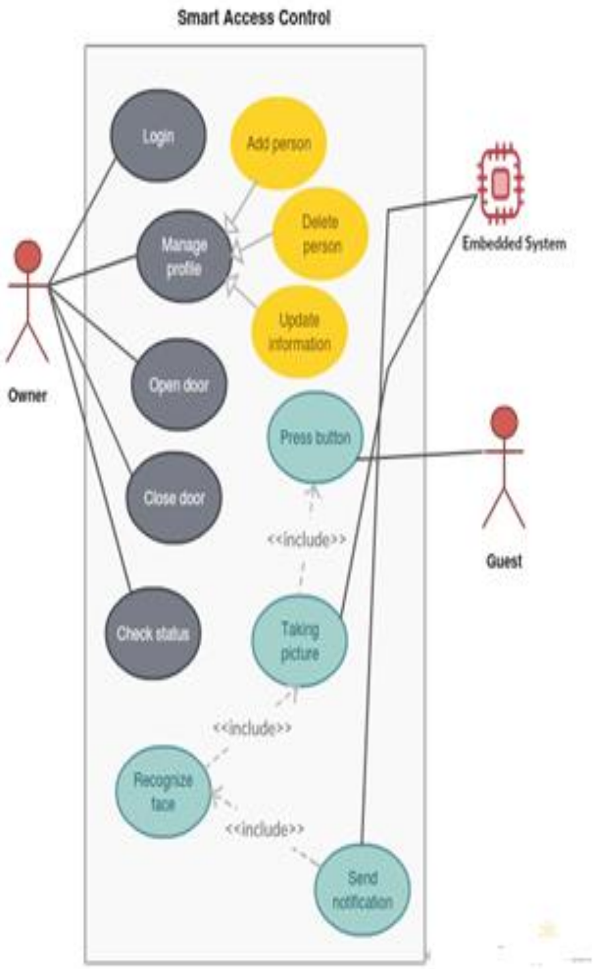
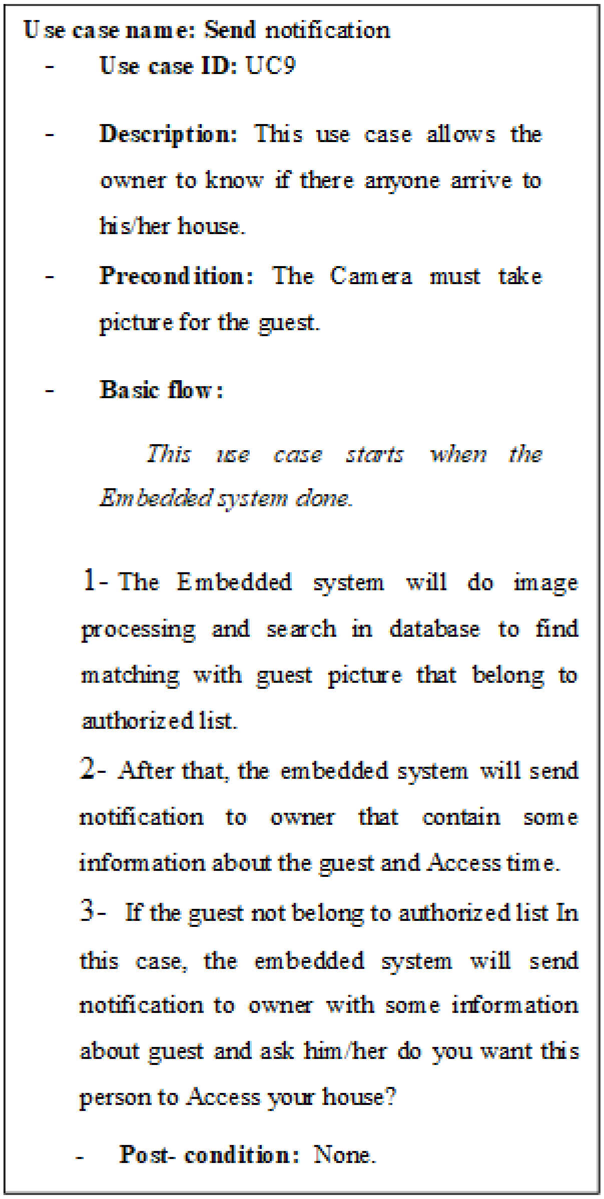


Figure 2 Use Case Diagram

All use cases in Figure 2 designed. Every use case was described in details. For example: **Use case name: Send notification** allows the owner to know if there anyone arrive to his/her house. Figure 3 discuss "Send Notification use case".

5. SOLUTION DESCRIPTION

The user first register to build his own database on the database server. And inserts authorized people to program and stores it in the database. The device also registered to the same account. Then embedded system interacts with the access trials.



Use case name: Send notification

- **Use case ID:** UC9
- **Description:** This use case allows the owner to know if there anyone arrive to his/her house.
- **Precondition:** The Camera must take picture for the guest.
- **Basic flow:**

  This use case starts when the Embedded system done.

  1- The Embedded system will do image processing and search in database to find matching with guest picture that belong to authorized list.

  2- After that, the embedded system will send notification to owner that contain some information about the guest and Access time.

  3- If the guest not belong to authorized list In this case, the embedded system will send notification to owner with some information about guest and ask him/her do you want this person to Access your house?

- **Post- condition:** None.

Figure 3: Discuss Send Notification use case.

The door will be opened in two scenarios, the guest is either in the authorized list or the owner allow to the door to be opened via the mobile application. Figure 4 explain the solution flow.

- In case of any unknown guest click the door, what happen?

The guest presses push button to send a signal to embedded system. The embedded system will start working by turning on the camera to take a picture of the guest. The server will send notification to the owner; included guest picture to for asking him/her what to do? The owner is the only who can decide to allow the door to be opened or not.

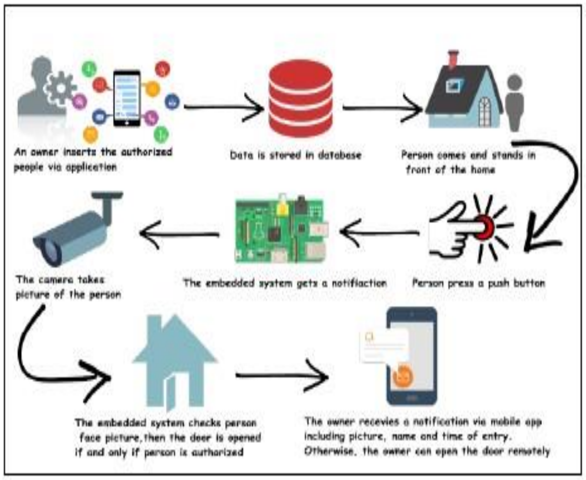

An owner inserts the authorized people via application
Data is stored in database
Person comes and stands in front of the home
Person press a push button
The embedded system gets a notifiaction
The camera takes picture of the person
The embedded system checks person face picture,then the deer is opened if and only if person is authorized
The owner recevies a notification via mobile app including picture, name and time of entry. Otherwise, the owner can open the door remotely

Figure 4 The SAC Description

In our solution we produced services to the owner, and services to the guest. As the following:

A. Owner Services

- The owner can open/ close the door remotely
- If the owner can allow or refuse opening the door for other. Figure 5 illustrate the owner services.

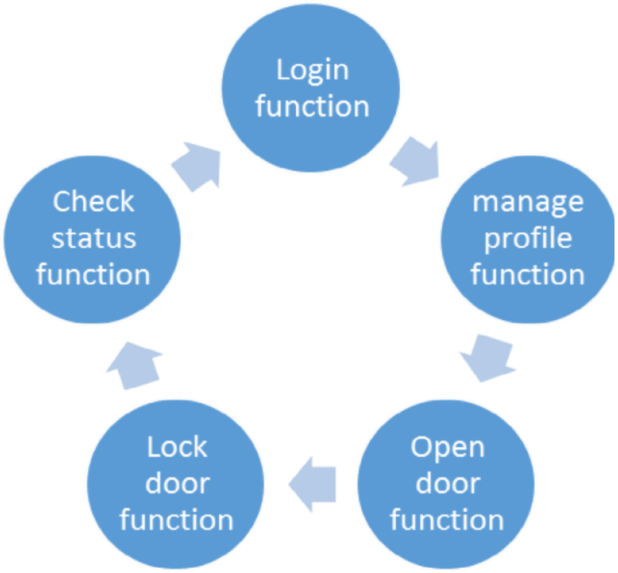


Figure 5: owner service*s*

B. Guest services

- The solution enables Younger people to enter their home in case no one there, open the door for who want to help the older people they cannot service their selves.
- If any stranger tries to enter the home the solution send notification to the owner, how only could decide to allow for them to enter or not.

6. INTEGRATED TECHNOLOGIES

The main two technologies we used Face Recognition and Raspberry Pi. Face recognition is a biometric-based Technique that can recognize individuals throw their digital image by analyzing and comparing patterns. The main applications can apply face recognition systems are commonly security purposes and face Identity. [11].

[There exist several techniques for extracting the useful features from (preprocessed) face images to perform face recognition. We select Local Binary Pattern (LBP) method. This approach was introduced in 1996. With LBP divide the image into several small regions from which the features are extracted. These features consist of binary patterns that describe the surroundings of pixels in the regions. According to several studies face recognition using the LBP method provides very good results. [12]

The other technology is The Raspberry Pi, which is a credit card-sized computer that plugs into your TV and a keyboard. It is a capable little computer which can be used in electronics applications, and for many of the things that your desktop PC does, like spreadsheets, word processing, browsing the internet, and playing games. It also plays high-definition video. [13]. The Raspberry Pi is a dynamic microcontroller that is capable of doing just about anything a computer does. It runs with the Python programming language. [14] With Raspberry Pi can doing applications for example:

Smart Home Automation, Robots ،ROV and UAV Camera Streamers, Remote Monitor and supercomputers.

We used more than one tools to implement the proposed solution. First, we build the solution for Android systems so we select one of the android Development tool which is the official Integrated Development Environment (IDE) for Android app development, based on IntelliJ IDEA. Second, we need web server contains the database we select MAMP. MAMP installs a local server environment in a matter of seconds on your computer. It comes free of charge, and is easily installed. MAMP will not compromise any existing Apache installation already running on your system. You can install Apache, PHP and MySQL without starting a script or having to change any configuration files! Furthermore, if MAMP is no longer needed, just delete the MAMP folder and everything returns to its original state (i.e. MAMP does not modify any of the "normal" system). [15,16]. IDLE (Integrated Development Environment or Integrated Development and Learning Environment) another tool we used. IDLE is an integrated development environment for Python, which has been bundled with the default implementation of the language.

Because of using Face recognition Technique, a webcam was needed. A webcam is a video camera that feeds or streams its image in real time to or through a computer to a computer network. When "captured" by the computer, the video stream may be saved, viewed or sent on to other networks via systems such as the internet, and emailed as an attachment.

7. DISCUSSION

Smart Access Control (SAC) is a smart home solution helps the owner to control his home using the mobile application. The owner can open or lock his door without need to use his key. Figure 6 illustrates screenshots of SAC solution.

The owner can open the door remotely for his children or trusted persons. If the owner is old or has an elder person inside the home or people have special needs, the owner can use the solution for them.

In addition, the system gives a Security service, as we mentioned, if the guest is authorized person; it could be the owner himself/ herself or any one of the family list; the door will open. Else the guest may be anyone not allowed to enter or unknown persons or may be a thief, the system will not allow entering and send notification to the owner.

An important feature or service in our solution, we used face recognition where smartphone was out of charge, so the server can recognize the authorized persons and give signal to embedded system for opening the door without the need to take agreement from the user.

Smart Access control (SAC) presents many services in the internet of things environment, but it has little limitations associated with the implementation of the solution and it will be our future work. These limitations could be in the camera position; it must be in a fixed position, high resolution and had spot light; also, the quality of the capturing the face might affect the system performance in terms of recognizing faces properly.

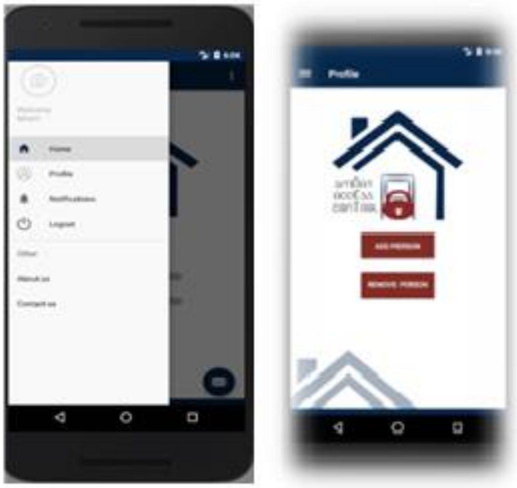


Figure 6 screens of SAC solution

8. CONCLUSION

Smart Home is one of IOT technologies. The IOT widely used to solve many problems and help to improve the home services. This paper proposed smart solution to control the home accessibility. The solution based on integrated technologies such as face recognition and embedded system (Raspberry Pi) to control the hardware device; which is a strong and reliable embedded system device in the complex and challenging tasks. Using these technologies in our proposed system to handle the access permission and the user can administer it remotely by using a mobile application.

The mobile application is connected to a camera in front of the building's entrance and it can communicate with the owner via the application. Furthermore, the holder can send and receive a request to/from the smart access system such as opening the door, show the picture of whom wish to enter the place and create access list for authorized people depending on their facial image.

The face recognition is used in the proposed solution to give permission to open the door for some people who are existed in the authorized list. An important feature in our solution, we used face recognition where smartphone was out of charge, so the server can recognize the authorized persons and give signal to embedded system for opening the door without need to take agreement from the user.

By using this solution, we believe that it may provide an assistance for a better safety and security, life consistent support, offering interactive and efficiency, saving time and effort.

9. REFERENCES

[1]. Ovidiu, V. and Peter, F. 2013. Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. River Publishers, ISBN: 978-87-92982-96-4

[2]. Blanson, H. Olivier, A., Alpay, Laurence, L., and Dumay Adrie, C.M. 2010. Aging in Place: Self-Care in Smart Home Environments, Smart Home Systems, INTECH Open Access Publisher, pp. 105-120, (February 2010).

[3]. Karen, R., Scott, E. and Lyman, C. 2015. internet of things : an overview understanding the issues and challenges of a more connecting world , The Internet Society (ISOC).

[4]. LOPEZ. R. 2013. An Introduction of internet of things, LOPEZ-Research.

[5]. Antar, S. A., Pramod P. J., E. M. and T. S. The Internet of Things (IoT): An Overvsiew. 2015. Int. Journal of Engineering Research and Applications ISSN:2248-9622, Vol. 5, Issue 12, (Part - 2)(December 2015), pp.71-82

[6]. Nicoleta-Cristina, G.,2, Vasile Gheorghita, G. and Ioan, U. A Survey on the Internet of Things Software Arhitecture. 2015. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 12

[7]. Jin, C. and Thomas, K. A Survey on Smart Home Networking. 2009 , Carleton University, Systems and Computer Engineering, Technical Report SCE-09-10, (September 2009)

[8]. Vinay, sagar .K N. and Kusuma, S. M. Home Automation Using Internet of Things.2015, International Research Journal of Engineering and Technology (IRJET) eISSN: 2395 -0056 Volume: 02 Issue: 03 (June-2015)

[9]. August Smart Lock. August Smart Lock | August. 2016. August.

[10]. Patrick, S. Comparing the Danalock vs August Smart Lock - All Home Robotics. 2016 All Home Robotics. Retrieved from: http://www.allhomerobotics.com

[11]. Divyarajsinh,, N. P. and Brijesh, B. M. Face Recognition Methods & Applications. 2013 Divyarajsinh N Parmar et al ,Int.J.Computer Technology & Applications,Vol 4 (1),84-86

[12]. Abdur Rahim, Najmul, H. Tanzillah, W. and Shafiu,l A. Face Recognition using Local Binary Patterns (LBP). 2013 . Global Journal of Computer Science and Technology Graphics & Vision Volume 13 Issue 4 Version 1.0

[13]. Nikhil, P. , Samuel, K. and Manoj, B.Raspberry Pi Augmentation: A cost effective solution to Google Glass. 2017 . International Research Journal of Engineering and Technology (IRJET) Volume: 04 Issue: 03 (Mar -2017)

[14]. CAS,. The Raspberry Pi Education Manual. 2012. Computing at School (CAS) Version 1.0 (December 2012)

[15]. MAMP . MAMP 3 – User Guide. March 2014 (c) appsolute GmbH

[16]. MAMP . MAMP PRO 3 – User Guide. March 2014 (c) appsolute GmbH

International Journal of Computer Applications Technology and Research
Volume 7–Issue 03, 139-157, 2018, ISSN:-2319–8656

Determinants of Behavioral Intention in Adopting Network Monitoring System

Shafiq Mugerwa
Assistant Systems Administrator
(MIS-Unit)
Makerere University Business School,
Kampala, Uganda

Musa B. Moya
Associate Professor
Dean Faculty of Computing and Informatics
Makerere University Business School,
Kampala, Uganda

Geoffrey Mayoka Kituyi
Senior Lecturer
Computer Science and Engineering
Makerere University Business School,
Kampala, Uganda

Abstract.: Makerere University Business School(MUBS) staff and student population stands to over 15,000 (MUBS HR report 2014) but on average, MUBS digitized online network can support about 700 users pick time and approximately 300 off pick hours which is not sufficient (Management Information Systems Unit Network statistics, 2015). Could the low support be attributed to the determinants of behavioral intention? This study therefore examined the relationships between performance expectancy, effort expectancy, social influence, facilitating conditions and behavioral intentions in the adoption of an integrated network monitoring system (NMS) at Makerere University Business School (MUBS). The study followed a cross sectional quantitative research design that focused on describing and drawing inferences from the findings on the relationship between the variables. The study population comprised of 189 administrative staff using the survey instrument based on the UTAUT constructs tailored for the study. Data was analyzed using descriptive statistics, correlations and regressions analysis using Statistical package for social sciences (SPSS). The results indicate that there were significant positive relationships between Performance Expectancy, Effort expectancy Social influence and Facilitating Conditions on Behavioral intention. Emphasis should be placed on performance expectancy, effort expectancy, social influence and facilitating conditions as determinants of behavioral intention for better network monitoring system.

Key words: Network monitoring system, UTAUT, behavioral intention, performance expectancy, effort expectancy, social influence and facilitating conditions.

1. INTRODUCTION

Network Monitoring Systems (NMSs) are essential in managing the complex computer networks of today. They ensure all faults on the network are known and assist the network operator in fixing these faults. They involve the collection of tools integrated in a single operator interface with a powerful but user-friendly set of commands for performing most or all network management tasks (Stallings, 2007).

Currently, MUBS network is managed by the dynamic host control protocol (DHCP) server and the cyber roam. In an incident where either the cyber roam is off or the DHCP server, it is hard to detect which equipment are connected on the network and which one is offline.

The failure to adopt a network monitoring tool by many staff in MUBS is of particular concern. Most of the studies on innovation in higher education have centered on ICT software and hardware designs that are driven from information science (IS) or information technology (IT) perspective of behavioral intention to use the system on an individual Level (Fishbein & Ajzen, 1975; Venkatesh & Davis, 2000), (Venkatesh 2012) , (Moya et.al 2016; Engotoit et.al 2016; Lukwago et.al 2016; 2017; Nyesiga et al. ,2017; Moya et al, 2017).

1.1 Statement of the problem

MUBS staff and student population stands to over 15,000 (MUBS HR report 2014) but on average, digitized online network can support about 700 users pick time and approximately 300 off pick hours which is not sufficient (MISU Network statistics, 2015). Could the low support be attributed to the determinants of behavioral intention? This study therefore examined the relationships between performance expectancy, effort expectancy, social influence, facilitating conditions and behavioral intentions in the adoption of an integrated network monitoring system at Makerere University Business School (MUBS).

1.2 Objectives of the study

This study focus particularly on the influence of network monitoring system adoption that technology complexity in MUBS has in relation to the intention to use a new technology. Similarly, the study seeks to establish the relationship between Performance Expectancy, Effort Expectancy, Social Influence and Facilitating Conditions on the Behavioral Intention of adopting a NMS at MUBS. This study was intended to promote significant knowledge on how important monitoring equipment is, beneficial to the academicians and researchers and understanding the role of network monitoring.

2. THEORETICAL FRAMEWORK AND LITERATURE REVIEW

The UTAUT is a unified model that was developed by Venkatesh et al (2003) based on social cognitive theory with a combination of eight prominent information technology (IT) acceptance research models. The authors examined the predictive validity of eight models in determining the behavioral intention and usage to allow fair comparison of the models.

There are some analytical models dealt with technology or system adopting problems based on information systems, psychological, or sociological theories.

Owing to these models almost could explain 40% of the variance in individual intention to adopt technology at least, the follow-up studies met an arduous decision to choose appropriate models or even constructs involved in different models without overlooking important functions obtained from other competing models. Venkatesh, Morris, Davis and Davis (2003) integrated eight models from reviewing past related user acceptance literature to formulate a mix model, referred to as "Unified Theory of Acceptance and Use of Technology" (UTAUT).UTAUT has condensed the 32 variables found in the existing eight models into four main effect and four moderating factors. The combinations of the constructs and moderating factors have increased the predictive efficiency to 70%, a major improvement over previous TAM model rates. Self-efficacy has been shown to influence choices of whether to engage in a task, the effort expended in performing it, and the persistence shown in accomplishing it.

The greater people perceived their self-efficacy to be, the more active and longer they persist in their efforts. Computer anxiety has been defined as a fear of computers (ICT) when using one, or fearing the possibility of using ICT, opined that attitudes towards computer are very critical issues. Monitoring the users' attitudes towards computers (ICT) should be a continuous process if ICT is to be used for effective training and learning (Oye & A.Iahad, January 2012).

Various models were developed, such as the Theory of Reasoned Action (TRA) (Fishbein and Ajzen, 1975) and Technology Acceptance Model (TAM) (Davis, 1989). Each model has its own independent and dependent factors for user acceptance and there are some overlaps (Dillon and Morris, 1996). TAM has failed to provide meaningful information about the user acceptance of a particular technology due to its generality (Mathieson et al., 2001). Consequently, a number of modified TAM models were proposed which are applicable to contemporary technologies (Horton et al., 2001; Chau and Hu, 2001).However, to confront some of the limitations and uncertainties that multiple models may pose to researchers the Unified Theory of Acceptance and Use of Technology (UTAUT) model was developed (Venkatesh *et al.*, 2003).

UTAUT has four key constructs (i.e., performance expectancy, effort expectancy, social influence, and facilitating conditions) that influence behavioral intention to use a technology and/or technology use. We adapt these constructs and definitions from UTAUT to the consumer technology acceptance and use context. There are many papers quoted UTAUT model or adopted partial dimensions and added other dimensions along with their own topics to understand new IT purchase/use intentions. Mäntymäki and Salo (2013) proposed an extended UTAUT model to predict the young people's purchasing intention in social virtual world. Gruzd, Staves and Wilk (2012) directly utilized the UTAUT model to interpret and explore how the social media are used in research practices. Martín and Herrero (2012) added innovativeness into original UTAUT model to find out the user's psychological influential factors on the online purchase intention in rural tourism.

2.1 Performance Expectancy and Behavioral Intention to adopt NMS

This looks at the degree to which individuals believe that adopting a system will help them improve their job performance. It contains five variables namely; performance expectancy, extrinsic motivation, job-fit, relative advantage and outcome expectations (Venkatesh et al, (2003); Campeau and Higgins, (1995); Davis *et al., (*1989, 1992); Thompson et al., (1991). Performance expectancy is the strongest predictor of intention and consistent with earlier models tested by Agarwal and Prasad (1998). Users of Information Systems give high regard to the level at which the system is advantageous to them in their daily routine.

The evidences in Davis et al. (1989), Taylor and Todd (1995) and Venkatesh et al (2003) suggest that users have more intention to use a new information technology if this information technology can help improve their work performance. Users believe that using NMS is substantially beneficial to them; therefore, they are willing to adopt the system if the operating process is improved. In MUBS, NMS can increase the efficiency of accessing the systems on the network due to the more relative advantages than the traditional monitoring. With this, the user expectations will be high. Agarwal and Prasad (1998),Venkatesh et al., (2003), Lukwago et al. (2017), Engotoit et al. (2016 ; 2017), Nyesiga et al. (2017) and Moya et al. (2017) have pointed out that users have more intention to use a new information technology if it is easy to operate.

H1. The study hypothesizes that performance expectancy has a positive influence on behavioral intentions to adopt Network Monitoring System.

2.2 Effort Expectancy and Behavioral Intention to adopt NMS

Perceived ease of use is the degree of ease associated with the adoption of the Technology (Venkatesh et al., 2003).

Users of Information Systems are concerned with the ease that is associated with the use of the information system. A complex system or a web interface that is difficult to navigate can make users uninterested in adopting the system or website (Byun & Finnie, 2011). The issue regarding the level of computer literacy amongst the population can alter the perception of respondents to the ease associated with adopting an information system, because computer savvy users may be indifferent.

In other words it is the level of simplicity associated with a technology. However, Moore and Benbasat (1991) and Davis et al., (1989) defined ease of Use as the degree to which an individual believes that using a particular system would be free of physical and mental effort. The evidences in Agarwal and Prasad (1998), Karahanna et al. (1999) , Venkatesh et al., (2003), Lukwago et al. (2017), Engotoit et al. (2016 ; 2017), Nyesiga et al. (2017) and Moya et al. (2017) suggest that users have more intention to use a new information technology if people important to them think it is necessary for them to adopt the new technology.

H2. The study hypothesizes that effort expectancy has a positive influence on behavioral intentions to adopt Network Monitoring System.

2.3 Social Influence and Behavioral Intention to adopt NMS

Social influence is the degree to which one is affected by others to adopt the information system (Venkatesh et al., 2003). Religion, ethnicity, culture, economic status and education determine one’s intention to adopt a system and eventually use it. Taylor and Todd (1995) and Venkatesh et al. (2003) have pointed out that users will use a new information technology more frequently and positively if they perceive rich resources for use of this technology. Besides an effective and easy to use information system, end-users might not be obliged to use the system until they are motivated by important others (people) that can influence their attitude and behavior. With the way people's life are molded round role models, public figures, sportsmen and celebrities, an encouragement by such important figures to use the system can motivate users to adopt the use of an information system (Taiwo et al.,2012).

Thompson et al., (1991), Venkatesh et al., (2003), Wu et al., (2010) define subjective norm as the degree, to which users consider that it is necessary for others to adopt NMS, social factors look at degree to which users are affected by a certain group culture to adopt NMS and finally image considers the degree to which users perceive that adopting NMS can increase their personal images. Most studies have established positive relationship between social influence and behavioral intention (Venkatesh et al (2012; 2016), Lukwago et al. (2017), Engotoit et al. (2016 ; 2017), Nyesiga et al. (2017)).

H3. The study hypothesizes that social Influence has a positive influence on behavioral intentions to adopt Network Monitoring System.

2.4 Facilitating Conditions and Behavioral Intention to adopt NMS

Venkatesh et al., (2003) refers to facilitating conditions as the degree to which an individual believes that organizational and technical infrastructure exists to support adoption and use of the system. It constitutes of perceived behavioral control and facilitating conditions. The former looks at the ability of the users to adopt the systems and the later looks at degree to which users believe that the existing software and hardware supports their adoption of system in case it is adopted, Thompson et al.,(1991), Venkatesh et al.,(2003), Wu et al., (2010). Venkatesh and Morris (2000) and Venkatesh et al., (2003) suggest that higher behavioral intention leads to a higher frequency of use of a system. Facilitating conditions have had a positive relationship with behavioral intention as reported by (Lukwago et al.,(2017), Engotoit et al.,(2016; 2017), Nyesiga et al.,(2017)).

H4. The study hypothesizes that facilitating conditions have a positive influence on behavioral intention to adopt the NMS at MUBS.

2.4. Conceptual Framework

The conceptual framework is adopted from the Unified Theory of Acceptance and Use of Technology (UTAUT) model (Venkatesh et al, 2003).Venkatesh et al. (2003) proposed an acceptance model combining eight existing tools into one model called the "Unified Theory of Acceptance and Use of Technology (UTAUT)", which has been shown to outperform other models for studying the acceptance of technology. The UTAUT model by Venkatesh et al. (2003) postulates six constructs; performance expectancy, effort expectancy, social influence, self-efficacy, anxiety, and attitude toward using technology. These constructs determine the behavioral intent, whereas another two constructs behavioral intent and facilitating conditions influence the usage behavior of the technology (Moya et.al 2016; Engotoit et.al 2016; Lukwago et.al 2016; 2017; Nyesiga et al. ,2017; Moya et al, 2017).

The figure 1 shows the UTAUT model with the related modifiers (external) variables.

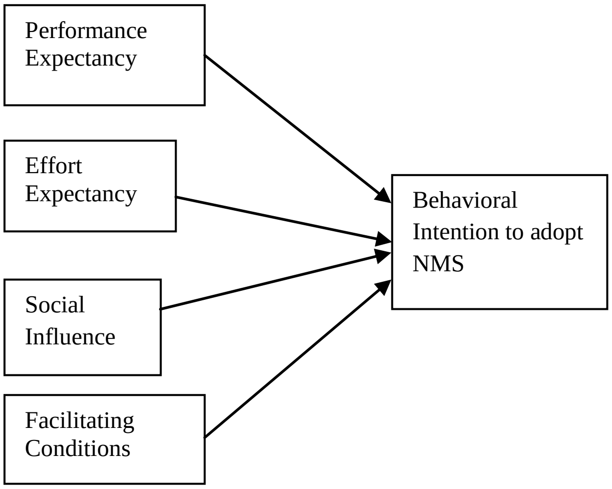


Figure1: Unified Theory of Acceptance and Use of Technology (UTAUT) Model.

Source: Adopted Research model by Venkatesh, Morris, Davis, & Davis 2003; Venkatesh et al. 2016; Engotoit et al, 2016; Lukwango et al. 2017; Nyesiga et al. 2017; Moya et al, 2016; 2017.

3. METHODOLOGY

This brings out the methodology that was used in conducting the research. It entails the research design, the study population, the sampling procedure and sample size, the variables and their measurements, reliability and validity of research instruments, data collection methods and data processing and analysis procedures and techniques.

3.1 Research Design

The study took a cross sectional survey design to study the relationships between the quantitative variables of the study. Since the study meant to test rather than generate theory, it adopted a correlational approach which focused on describing and drawing inferences from the findings on the relationships among the study variables.

3.2 Study Population and Sample Size

The study population was 189 administrative staff at Makerere University Business School who were directly given questionnaires to respond to the questions. A sample of 126 administrative staff was taken in this study. Krejcie and Morgan (1970) sample size determination table was used and simple random sampling was used in the selection of the sample of 126 where all elements in the population had an equal chance of being selected in the sample. The lottery method of identifying the simple random sample was used.

3.3 Data collection, Analysis and Presentation

The data was collected using a pre-coded questionnaire and analyzed using the descriptive statistics analysis method which employs the use of percentages, means and frequencies (Janssens *et al*., 2008).Statistical Package for Social Scientists (SPSS) was used for data entry and analysis, a linear regression to interpret the degree of relationship between variables. Linear regression analysis helped to provide evidence that the independent variables significantly explain behavioral intentions to adopt NMS.

3.4 Survey Instruments

The survey instrument was based on the constructs defined in the UTAUT model by Venkatesh et al. (2003), with the constructs tailored for this study. The study questionnaire was distributed to a total of 140 administrative staff, 133 collected questionnaires, seven (7) were discarded (because the respondents gave more than one answer to a question that expected only one answer and or many questions were unanswered. This meant that the final samples of 126 questionnaires were used for all subsequent analysis.

3.5 Measurements of Study Variables

Items used to measure these study variables were performance expectancy, effort expectancy, social influence, facilitating conditions and behavioral intention. These were adopted from Venkatesh et al., (2003); Lukwago et al. (2017), Engotoit et al. (2016 ; 2017), Nyesiga et al. (2017) and Moya et al. (2017) . Performance expectancy was measured using perceived usefulness, extrinsic motivation, job fit, relative advantage and outcome expectations. Effort expectancy was measured using ease of use, complexity and perceived ease of use. Social influence was measured using subjective norms, social factors and image. Facilitating conditions were measured using perceived behavioral control, conditions and compatibility.

3.6 Data Reliability and Validity

A pilot study was conducted to test the validity and reliability of the research instrument. Cronbach's' Alpha was used to calculate and determine the reliability of the items. A Cronbach's alpha value of greater than 0.6 is also considered acceptable (Yong, Hua, & Mei, 2007).

Cronbach's alpha reliability coefficient for the individual scales to confirm the internal consistency and reliability of measures was calculated and they were above 0.6. Validity of instruments was done in two ways; face validity and content validity. Face validity through getting comments on relevance of the questions to the study variables which were later incorporated in the final instrument. Content validity was also obtained by using Content Validity Index at 0.7742 for expert one and 0.8387 for expert two making an average Content Validity Index of 0.8064. Since they were all above 0.7, this means that the questions were all relevant to the study variables as shown in table 1.

Table 1: Reliability Test

Variable	Scale	Number of Items	Cronbach's alpha
Performance Expectancy	1-5	5	.751
Effort Expectancy	1-5	4	.730
Social Influence	1-5	2	.600
Facilitating Conditions	1-5	6	.711
Behavioral Intention	1-5	4	.726

Source: Primary data

Since the Cronbach's alpha is 0.60 and above, the questionnaire was reliable.

4. PRESENTATION OF FINDINGS

The findings of the study were generated from data analysis and its interpretation. It includes descriptive statistics, factor analysis, correlation coefficient analysis and regression analysis. The results were presented in line with research objectives.

4.1 Demographic Characteristics

The respondents were categorized under gender, marital status, education, age positions at work and length of service as shown in tables 2, 3,4,5,6 and 7.

4.1.1 Distribution by Gender

The respondents comprised of both female and male majority of which 57% were male and 43% were female. This means that most of the sample was taken from the male. This is shown in the table 2.

Table 2: Gender

	Frequency	Percent
Male	72	57.1
Female	54	42.9
Total	126	100.0

Source: Primary data

4.1.2 Distribution by Marital status

The respondents were majorly married at 55% from the total population, single at 42%, 2% cohabiting and 1% catered for the others .This is shown in the table 3.

Table 3: Marital status

	Frequency	Percent
Single	53	42.1
Married	69	54.8
Cohabiting	2	1.6
Others	2	1.6
Total	126	100.0

Source: Primary data

4.1.3 Distribution by Education

Majority of the respondents were Bachelor's degree holders. This meant that many of them were considered to have attained the minimum knowledge for the adoption of a new system. These were followed by Master's degree holders at a percentage of 31% and followed by Ordinary diplomas at 13%. From the above, this meant that from the sample, the largest population had the knowledge to take on the system. This is shown in table 4.

Table 4: Education attained

	Frequency	Percent
Bachelors Degree	83	73.1
Post Graduate Diploma	4	3.2
Masters Degree	39	31.0
Total	126	100.0

Source: Primary data

4.1.4 Distribution by Age

The majority of the respondents were between 25-35 years at 65%. These were followed by 21% at an age between 35-45 years. Few respondents were seen to be between 45-55 years and above. This is shown in table 5.

Table 5: Age of respondents in years

	Frequency	Percent
Below 25 years	12	9.5
25-35 Years	82	65.1
35-45 Years	26	20.6
45-55 Years	5	4.0
Above 55 years	1	.8
Total	126	100.0

Source: Primary data

4.1.5 Distribution by Staff category

Majority of the respondents were administrative assistant at 46% and the least response was got from directors at 2.4%. This implied that the higher the staff rank, the lower the response. This is shown in the table 6.

Table 6: Staff category

	Frequency	Percent
Director	3	2.4
Deputy Director	5	4.0
Assistant Director	11	8.7
Senior Administrator	17	13.5
Administrator	31	24.6
Administrative Assistant	59	46.8
	126	100.0

Source: Primary data

4.1.6 Distribution by length of Service with the Institution

Majority had worked with the institution for a period between 11-15 years at 58%, followed by those with 6-10 years at 42%. Very few responses were got from staff who worked for more than 16 years at 4% and 5%. This is showed in table 7.

Table 7: Length of Service with the institution

	Frequency	Percent
6-10 Years	42	33.3
11-15 Years	73	57.9
16-20 Years	5	4.0
Above 20 years	6	4.8
Total	126	100.0

Source: Primary data

4.2 Descriptive Statistics of the Study Variables

Descriptive statistics for performance expectancy, effort expectancy, social influence, facilitating conditions and behavioral intention were performed using mean and standard deviation as shown in table 8.

Table 8: Descriptive statistics for study variables

	N	Mean	Std. Deviation
Performance Expectancy	126	4.3611	.60249
Effort Expectancy	126	4.0079	.58342
Social Influence	126	3.4286	.89055
Facilitating Conditions	126	3.9947	.73180
Behavioral Intention	126	4.0893	.58776

Source: Primary data

There were positive perceptions on performance expectancy (Mean = 4.3611), effort expectancy (Mean = 4.0079), facilitating conditions (Mean = 3.9947), and behavioral intention (Mean = 4.0893). This implied that the Network monitoring system is easy to use, useful, and facilitative in terms of infrastructure, can improve performance at work and is usable. However, they were indifferent on social influence (Mean = 3.4286).

4.3 Factor Analysis of the Study Variables

Exploratory factor analysis using principal component and extracting factors or items with factor loadings greater or equal to ±0.3 as shown in tables 9 to table 18.

4.3.1 Performance Expectancy

The most important items used to measure performance expectance were three explaining 73.370% variance as shown in table 9.

Table 9: Performance Expectancy Descriptive statistics

	Mean	Std. Deviation	Loadings
Adopting the system enables me to accomplish tasks more quickly.	4.3810	.65553	.917
Adopting the system increases my productivity.	4.2778	.71149	.850
I would find the system useful in my job.	4.4246	.75118	.798
Eigen value			**2.201**
% of Variance			**73.370**

Determinant = .301

Source: Primary data

The sample used on performance expectancy was adequate (Kaiser-Meyer-Olkin Measure of Sampling Adequacy = .647, Bartlett's Test of Sphericity Approx. Chi-Square = 147.744, df = 3, Sig. =.000). The loadings are well above 0.5 an indication that the three items converged to measure performance expectancy as shown in table 10.

4.3.2 Effort Expectancy

The most important items used to measure effort expectance were three explaining 63.474% variance as shown in table 10.

Table 10: Effort Expectancy Descriptive statistics

	Mean	Std. Deviation	Loadings
It would be easy for me to become skillful at using the system.	4.1667	.64187	.861
Learning to operate the system is easy for me	4.1032	.74651	.803
. I would find the system easy to use in case I adopt it.	3.7540	.81669	.720
Eigen value			**1.904**
% of Variance			**63.474**

Source: Primary data

The sample used on effort expectancy was adequate (Kaiser-Meyer-Olkin Measure of Sampling Adequacy = .631, Bartlett's Test of Sphericity Approx. Chi-Square = 76.744, df = 3, Sig. =.000).The loadings are well above 0.5 an indication that the three items converged to measure effort expectancy.

4.3.3 Social Influence

The most important items used to measure social influence were three explaining 65.174% variance as shown in table 11.

Table 11: Social Influence Descriptive statistics

	Mean	Std. Deviation	Loadings
People who influence my behavior think that I should adopt the system.	3.2500	1.18786	.859
Adopting the system will raise my status among staff.	3.3968	1.10330	.811
Other staffs who wish to adopt the system will influence me.	3.6389	1.01121	.748
Eigen value			**1.955**
% of Variance			**65.174**

Determinant = .508

Source: Primary source

The sample used on social influence (Kaiser-Meyer-Olkin Measure of Sampling Adequacy = .652, Bartlett's Test of Sphericity Approx. Chi-Square = 83.334, df = 3, Sig. =.000). The loadings are well above 0.5 an indication that the three items converged to measure social influence.

4.3.4 Facilitating Conditions

The most important items used to measure facilitating conditions were three explaining 66.483% variance as shown in table 12.

Table 12: Facilitating Condition Descriptive statistics

	Mean	Std. Deviation	Loadings
The institutional ICT infrastructure will support the system.	3.7857	.91745	.844
The institution can afford to buy the system.	3.9286	.96481	.811
I have access to the computer to adopt the system.	4.2698	.80660	.789
Eigen value			**1.994**
% of Variance			**66.483**

Determinant = .497

Source: Primary data

The sample used on facilitating conditions (Kaiser-Meyer-Olkin Measure of Sampling Adequacy =.682, Bartlett's Test of Sphericity Approx. Chi-Square = 86.104, df = 3, Sig. =.000).The loadings are well above 0.5 an indication that the three items converged to measure.

4.3.5 Behavioral Intention

The most important items used to measure facilitating conditions were four explaining 61.750% variance as shown in table 13.

Table 13: Behavioral intention descriptive Statistics

	Mean	**Std. Deviation**	**Loadings**
I intend to update my computer for the systems adoption.	4.0794	.66457	.816
I intend to adopt the system for faster completion of tasks.	4.1270	.78978	.815
I plan to use the system to improve my performance at work.	4.1905	.68951	.772
I intend to adopt and use the system at work for the next years.	3.9603	.85230	.738
Eigen value			**2.470**
% of Variance			**61.750**

Determinant = .289
Source: Primary data

The sample used on behavioral intention (Kaiser-Meyer-Olkin Measure of Sampling Adequacy = .741, Bartlett's Test of Sphericity Approx. Chi-Square = 152.331, df = 6, Sig. =.000). The loadings are well above 0.5 an indication that the four items converged to measure behavioral intention.

4.4 Diagnostic Tests

4.4.1 Normality Test for Study Variables using Skewness and Kurtosis

The results in table 27 below on skewness indicate statistics ranging from -.077 to -1.842 which is within the recommended range of -2 to +2 implying that the study variables are approximately normally distributed. Kurtosis values range from -.437 to 7.515 which are within the range of -10 to +10 implying that there is a fairly normal distribution as shown in table 14.

Table 14: Skewness and kurtosis

	Mean	**Std. Deviation**	**Skewness**	**Kurtosis**
	Statistic	Statistic	Statistic	Statistic
Performance Expectancy.	4.3611	.60249	-1.842	7.515
Effort Expectancy.	4.0079	.58342	-1.083	4.895
Social Influence.	3.4286	.89055	-.496	-.437
Facilitating Conditions.	3.9947	.73180	-1.147	2.485
Behavioral Intention.	4.0893	.58776	-1.414	3.691

Source: Primary data

4.4.2 Normality test using Shapiro Wilk Statistics

According to Shapiro wilk statistics, the sig values were greater than 0.05 an indication that the data for all the study variable was approximately normally distributed as shown in the table 15.

Table 15: Shapiro wilk statistics

Shapiro wilk	**Statistic**	**Df**	**Sig.**
Performance Expectancy	.811	126	.187
Effort Expectancy	.900	126	.177
Social Influence	.952	126	.145
Facilitating Conditions	.912	126	.162
Behavioral Intention	.872	126	.225

Source: Primary data

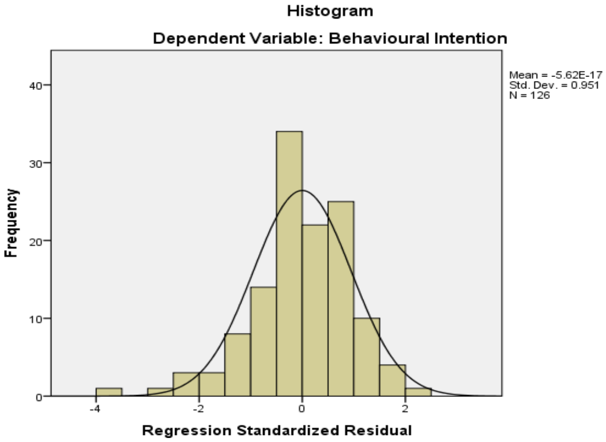


Figure 2: Histogram showing behavioral intention as a dependent variable

4.4.3 Linearity Test for the Study Variables

Using the F statistic values in the ANOVA table, results show that there was a linear relationship between the study variables (F =19.436, Sig = .000). Performance expectancy, effort expectancy, social influence, facilitating conditions and usage predicted 44.7% of behavioral intention, with performance expectancy (beta= .194), effort expectancy (beta =-.101), social influence (beta = .260), facilitating condition (beta = .418) and usage (beta = -.044) as shown in tables 16, 17 and 18.

Table 16: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
	.669	.447	.424	.44591

Predictors: (Constant), Usage, Effort Expectancy, Social Influence, Facilitating Conditions, Performance Expectancy.

Source: Primary data

Table 17: ANOVA

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	19.323	5	3.865	19.436	.000
Residual	23.860	120	.199		
Total	43.183	125			

Dependent Variable: Behavioral Intention

Source: **Primary data**

Table 18a : Regression Coefficients

	B	Beta	T	Sig.	VIF
(Constant)	1.089		2.947	.004	
Performance Expectancy	.189	.194	2.232	.027	1.572
Effort Expectancy	.102	.101	1.233	.220	1.486
Social Influence	.172	.260	3.596	.000	1.132
Facilitating Conditions	.335	.418	5.010	.000	1.814

Dependent Variable: Behavioral Intention

Source: Primary data

4.4.4 Multi co-linearity and Homogeneity test

Multi co-linearity test was tested using variance inflation factor (VIF).

All VIF were small and less than 2 and this implied that there was no multi co linearity between the independent variables as shown in table 31.

Homogeneity of variance was tested using ZPRED and ZRISD scatter plot and levene test. The scatter plot indicated data converging towards the right an indication of homogeneity of variance. Also levene statistic was insignificant (Sig>0.05) an indication that the data was homogeneous.

Table 18 b: Levene Statistic

Levene Statistic		df1	df2	Sig.
Performance Expectancy	.098	1	124	.755
Effort Expectancy	.167	1	124	.684
Social Influence	5.532	1	124	.020
Facilitating Conditions	.926	1	124	.338
Behavioural Intention	2.515	1	124	.115

4.5 Relationship between Study Variables using Inferential Statistics

4.5.1 Correlation Analysis

Correlation analysis was also conducted to establish associations between the study variables.

The results are presented in the table 19.

Table 19: Correlations Matrix of the study variables

	1	2	3	4	5
Performance Expectancy (1)	1				
Effort Expectancy (2)	.487**	1			
Social Influence (3)	.143	.059	1		
Facilitating Conditions (4)	.505**	.491**	.094	1	
Behavioral Intention (5)	.475**	.408**	.318**	.579**	1

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Source: Primary data

Results in table 19 indicate significant positive relationships between Facilitating Conditions, Performance Expectancy, Effort Expectancy and Social Influence with Behavioral Intention (r=.579**;.475**;.408**;.318**; p-value<0.01). This implied that facilitating conditions positively associated with behavioral intention, performance expectancy associated positively with behavioral intention, effort expectancy positively associated with behavioral intention and social influence associated positively with behavioral intention.

4.5.2 Regression of Facilitating Conditions, Performance Expectancy, Effort Expectancy and Social Influence with Behavioral Intention.

Using SPSS version 20 hierarchical linear regression models were fitted as shown in table 20 and as Summarised below.

Results in table 20, Model 1 Predictors were only control or confounding variables (Constant), Length of service dummy, Lower Education dummy, Gender dummy, under 25 dummy, Staff Category dummy, Marital Status dummy, Postgraduate dummy, Degree dummy predicted .3%, (F=1.052, Sig=.402) of behavioral intention with Lower Education dummy, Postgraduate dummy, Degree dummy and Staff Category dummy as only significant predictors.

Model 2 Predictors: (Constant), Length of service dummy, Lower Education dummy, Gender dummy, under 25 dummy, Staff Category dummy, Marital Status dummy, Postgraduate dummy, Degree dummy, Facilitating Conditions linearly and significantly (F=8.234, Sig=.000) predicted 34.2% of behavioral intention with Lower Education dummy, Postgraduate dummy, Degree dummy , Staff Category dummy and facilitating condition as significant predictors of behavioral intention.

Model 3 Predictors: (Constant), Length of service dummy, Lower Education dummy, Gender dummy, under 25 dummy, Staff Category dummy, Marital Status dummy, Postgraduate dummy, Degree dummy, Facilitating Conditions, Performance Expectancy linearly and significantly (F=8.520, Sig=.000) predicted 37.6% with Lower Education dummy, Postgraduate dummy, Degree dummy , Staff Category dummy, facilitating conditions and Performance Expectancy as the significant predictors of behavioral intention.

Model 4 Predictors: (Constant), length of service dummy, lower education dummy, gender dummy, under 25 dummy, staff category dummy, marital status dummy, postgraduate dummy, degree dummy, facilitating conditions, performance expectancy, effort expectancy linearly and significantly (F=7.821, Sig=.000) predicted 37.5% of behavioral intention with lower education dummy, postgraduate dummy, degree dummy ,facilitating conditions , performance expectancy and effort expectancy as the significant predictors of behavioral intention.

Model 5 Predictors: (Constant), Length of service dummy, Lower Education dummy, Gender dummy, under 25 dummy, Staff Category dummy, Marital Status dummy, Postgraduate dummy, Degree dummy, Facilitating Conditions, Performance Expectancy, Effort Expectancy, Social

Influence (F=8.455, Sig=.000) predicted 41.7% of behavioral intention with lower education dummy, postgraduate dummy, degree dummy , facilitating conditions , performance expectancy , effort expectancy and social influence as the significant predictors of behavioral intention.

Table 20: Hierarchical Linear Regression

	Model 1	Model 2	Model 3	Model 4	Model 5
Variables	B	B	B	B	B
Constant	3.056**	1.548**	.706**	.437**	.420**
Gender	-.050	-.145	-.064	-.053	-.090
Marital status dummy	.034	-.003	.004	.008	.009
Lower education dummy	.929**	.703**	.958**	1.061**	.779**
Degree dummy	.840**	.598**	.844**	.966**	.702**
Post graduate dummy	.916**	.722**	.962**	1.066**	.777**
Under 25 dummy	.144	.039	.023	.013	.029
Staff category dummy	.266**	.210*	.133*	.112	.061
Length of service dummy	-.091	-.104	-.100	-.086	-.081
Facilitating conditions		.468**	.363**	.335**	.344**
Performance expectancy			.236**	.217**	.175**
Effort expectancy				.088	.168*
Social influence					.145*
R^2	.067	.390	.426	.430	.473
Adjusted R^2	.003	.342	.376	.375	.417
R^2 Change	.067	.323	.036	.005	.043
Sig. F Change	.402	.000	.009	.344	.003
F	1.052	8.234	8.520	7.821	8.455
Sig F	.402	.000	.000	.000	.000

**. Sig <0.01; *. Sig<0.05

Source: Primary data

4.5.2.1 The relationship between performance expectancy and the behavioral intention in adopting the NMS at MUBS.

There was a significant positive relationship between Performance Expectancy and Behavioral Intention to adopt network monitoring system at MUBS (B = .175, sig<0.01) .This implied that a positive change in performance expectancy is associated with a positive change in behavioral intention to adopt Network monitoring system by administrative staff at MUBS.

4.5.2.2 The relationship between effort expectancy and behavioral intention in adopting NMS at MUBS.

There was a significant positive relationship between Effort Expectancy and Behavioral Intention to adopt Network monitoring system at (B = .168, sig<0.05).This implied that a positive change in effort expectancy is associated with a positive change in behavioral intention to adopt Network monitoring system by administrative staff at MUBS.

4.5.2.3 The relationship between social influence and the behavioral intention in adopting NMS at MUBS.

There was a significant positive relationship between social Influence and Behavioral Intention to adopt Network monitoring system at MUBS (B = .145, sig<0.05). This implied that a positive change in social influence is associated with a positive change in behavioral intention to adopt Network monitoring system by administrative staff at MUBS.

4.5.2.4 The relationship between the facilitating conditions and the behavioral intention in adopting NMS at MUBS.

There was a significant positive relationship between facilitating conditions and Behavioral Intention to adopt Network monitoring system at MUBS (B = .344, sig<0.01). This implied that a positive change in facilitating conditions is associated with a positive change in behavioral intention to adopt Network monitoring system by administrative staff at MUBS.

5. DISCUSSION OF FINDINGS

5.1 Hypothesis 1: Performance expectancy has a positive influence on behavioral intentions to adopt NMS.

There was a significant positive relationship between PE and BI to adopt NMS at MUBS .This implied that performance expectancy influenced behavioral intention to adopt Network monitoring system by administrative staff at MUBS. Finding the system useful in my job, adopting the system to enable accomplishing tasks more quickly, increasing staff productivity enhanced the intention to adopt and use the system at work for subsequent years, planned to use the system in improving performance at work, updating computers for the systems adoption and intending to adopt the system for faster completion of tasks.

Therefore, hypothesis 1 is supported, the evidences in Davis et al. (1989), Taylor and Todd (1995) and Venkatesh et al (2003) suggest that users have more intention to use a new information technology if this information technology can help improve their work performance. Users believe that using NMS is substantially beneficial to them; therefore, they are willing to adopt the system if the operating process is improved. In MUBS, NMS can increase the efficiency of accessing the systems on the network due to the more relative advantages than the traditional monitoring. With this, the user expectations will be high. Agarwal and Prasad (1998) , Lukwago et al. (2017), Engotoit et al. (2016 ; 2017), Nyesiga et al. (2017) and Moya et al. (2017) have pointed out that users have more intention to use a new information technology if it is easy to operate and Venkatesh et al., (2003) have pointed out that users have more intention to use a new information technology if it is easy to operate.

5.2 Hypothesis 2: Effort expectancy has a positive influence on behavioral intention to adopt NMS at MUBS.

There was a significant positive relationship between EE and BI to adopt Network monitoring system at MUBS. This implied that effort expectancy influenced behavioral intention to adopt Network monitoring system by administrative staff at MUBS. Employees ease to become skillful at using the system, easy use of the system if adopted, easy learning to operate the system enhanced the intention to adopt and use the system at work for subsequent years, planned to use the system in improving performance at work, updating computers for the systems adoption and intending to adopt the system for faster completion of tasks.

Therefore hypothesis 2 is supported, the evidences in Agarwal and Prasad (1998), Karahanna et al., (1999), Venkatesh et al., (2003), Lukwago et al.,(2017), Engotoit et al.,(2016 ; 2017), Nyesiga et al. ,(2017) and Moya et al., (2017) have pointed out that users have more intention to use a new information technology if it is easy to operate suggest that users have more intention to use a new information technology if people important to them think it is necessary for them to adopt the new technology.

5.3 Hypothesis 3: Social influence has a positive influence on behavioral intentions to adopt NMS at MUBS.

There was a significant positive relationship between SI and BI to adopt Network monitoring system at MUBS .This implied that social influence influenced behavioral intention to adopt Network monitoring system by administrative staff at MUBS. Peer influence on individual staff behavior to adopt the system, adopting the system to raise status among staff and peers' adoption of the system enhanced the intention to adopt and use the system at work for subsequent years, planned to use the system in improving performance at work, updating computers for the systems adoption and intending to adopt the system for faster completion of tasks.

Therefore, hypothesis 3 is supported, Taylor and Todd (1995) , Venkatesh et al., (2003), Lukwago et al., (2017), Engotoit et al., (2016 ; 2017) and, Nyesiga et al., (2017) have pointed out that users have more intention to use a new information technology if it is easy to operate have pointed out that users will use a new information technology more frequently and positively if they perceive rich resources for use of this technology. Besides an effective and easy to use information system, end-users might not be obliged to use the system until they are motivated by important others (people) that can influence their attitude and behavior. With the way people's life are molded round role models, public figures, sportsmen and celebrities, an encouragement by such important figures to use the system can motivate users to adopt the use of an information system (Taiwo et al.,2012).

5.4 Hypothesis 4: Facilitating conditions has a positive influence on behavioral intentions to adopt NMS at MUBS.

There was a significant positive relationship between FC and BI to adopt Network monitoring system at MUBS. This implied that facilitating conditions influenced behavioral intention to adopt Network monitoring system by administrative staff at MUBS. Intention to adopt and use the system at work for the subsequent years, planning to use the system to improve performance at work, Intending to update computers for the systems adoption and adopting the system for faster completion of tasks enhanced the intention to adopt and use the system at work for subsequent years, planned to use the system in improving performance at work, updating computers for the systems adoption and intending to adopt the system for faster completion of tasks.

Therefore, hypothesis 4 is supported, Thompson et al.,(1991), Venkatesh et al.,(2003), Wu et al., (2010). Venkatesh and Morris (2000) ,Venkatesh et al., (2003), Lukwago et al., (2017), Engotoit et al., (2016 ; 2017) and Nyesiga et al., (2017) have pointed out that users have more intention to use a new information technology if it is easy to operate suggest that higher facilitating conditions leads to a higher frequency of use of a system.

6. CONCLUSION AND RECOMMENADATIONS

There was strong influence of performance expectancy, effort expectancy, social influence, facilitating condition on behavioral intention in adopting an integrated network monitoring system. Therefore performance expectancy, effort expectancy, social influence, facilitating condition were determinants of behavioral intention in the adoption of NMS at MUBS in improving network monitoring system.

Performance expectancy should be improved in terms of

consistence at work, improved productivity and usefulness of the system so as to improve on the behavioral intention of staff to adopt Network monitoring system at MUBS.
Effort expectancy should be improved in terms of clarity of the system to the staff, easiness of the system and simplicity of understanding and operating the system so as to improve on the behavioral intention of the staff to adopt the NMS at MUBS.

Social influence should be improved in terms of raising staff status on the system so as to improve the behavioral intention of staff to adopt the NMS at MUBS.

Facilitating conditions should be improved in terms of institutional ICT infrastructure, ability to purchase the system, access to the computers and hardware so as to improve the intention of the staff to adopt the NMS at MUBS

7. LIMITATIONS AND AREAS FOR FURTHER RESEARCH

The study was quantitative, therefore need for qualitative study.

The study used cross-sectional approach that gathered the perceptions on the behavioral intention to adopt Network monitoring system, however future research should focus on the longitudinal and experimental research designs to have the in depth understanding of the key predictors of behavioral intentions to adopt the network monitoring system.

This study focused on administrative staff as the unit of inquiry at the same time the unit of analysis. Hence future scholars / researchers should attempt investigate the same phenomenon using academic staff and or public universities as the unit of analysis.

The study particularly focused on the behavioral intention to adopt the networking system in third world setting, further researchers should carry out a comparative research in other developing countries.

8. REFERENCES

[1]. Agarwal, R. and Prasad, J. “A conceptual and operational definition of personal innovativeness in the domain of information technology,” Information Systems Research, (9:2), 1998. Pp, 204-215.

[2]. Agarwal, R. and Prasad, J. “The role of innovation characteristics and perceived voluntariness in the acceptance of information technologies,” Decision Sciences, (28:3), 1997. Pp. 557- 583.

[3]. Alawadhi, S., and Morris, A. "The Use of the UTAUT Model in the Adoption of E- government Services in Kuwait, “Proceedings of the 41st Hawaii International Conference on System Sciences, 2008.

[4]. Alrawashdeh, T. A., Muhairat, M. I., & Alqatawnah, S. M. (2012). Factors affecting acceptance of web-based training system: Using extended UTAUT and structural equation modeling. ArXiv preprint arXiv: 1205.1904. http://arxiv.org/abs/1205.1904.

[5]. Birth, A., & Irvine, V. (2009). Preservice teachers' acceptance of ICT integration in the classroom: applying the UTAUT mode.

[6]. Davis, F. D. (1989) "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," MIS Quarterly, (13:3), 1989, pp. 319-339.

[7]. Dishaw, M. T. & Strong, D. M. (1999). Extending the Technology Acceptance Model with task technology fit constructs. Information and Management, vol. 36, no. 1, pp. 9 – 21.

[8]. Engebretsen, T. (2005). Acceptance of Information Technology by Health Research Projects in Low-Income Countries: Intention to Use and Acceptance of Using Epiphany (IUAUE). Master’s Thesis. University of Bergen, Norway.

[9]. Engotoit Benard, Mayoka Kituyi Geoffrey, Moya Musa Bukoma, (2016) "Influence of performance expectancy on commercial farmers’ intention to use mobile-based communication technologies for agricultural market information dissemination in Uganda", Journal of Systems and Information Technology, Vol. 18 Issue: 4, pp.346-363, https://doi.org/10.1108/JSIT-06-2016-0037- Emerald-ISSN: 1328-7265. October, 2016.

[10]. Engotoit Benard, Moya Musa, Kituyi Geoffrey Mayoka, Abima Bonface, (2016) “A Mobile-Based Communication Adoption Model for agricultural market information dissemination in Uganda”, Global Journal of Computers & Technology Vol.

5, No. 1; ISSN: 2394-501X, October, 2016.

[11]. Fishbein, M., & Ajzen, I. (1975). Belief, Attitude, Intention, and Behavior: In an Introduction to Theory and Research Reading. MA: Addison-Wesley.

[12]. Gandal, Neil, Michael Kende, and Rafael Rob (2000). "The Dynamics of Technological Adoption in Hardware/Software Systems: The Case of Compact Disc Players," Rand Journal of Economics 31: 43-61.

[13]. Ghobakhloo, M., Zulkifli, N., & Aziz, F.(2010). The interactive model of user information technology acceptance and satisfaction in small and medium-size enterprises.European Journal of economics, finance and administrative sciences, (Accessed 18 June 2010).

[14]. Gruzd, A., Staves, K., and Wilk, A. (2012). Connected scholars: Examining the role of social media in research practices of faculty using the UTAUT model. Computers in Human Behavior, 28, 2340-2350.

[15]. Gubahar, Y. (2008). ICT Usage in Higher Education: A Case study on Preservice Teacher and Instructors. The Turkish Online Journal of Educational Technology, 7(1).

[16]. Lukwago Ismail, Musa B. Moya, Keefa Bwiino, Kato Ismael (2017) " Examining Determinants of Behavioural Intention in Adoption of Mobile Money Transfer Services in Uganda", ICTACT Journal on Management Studies Volume: 3 , Issue: 1 February 2017.

[17]. Lukwago Ismail, Moya B. Musa ., Kato Ismael, (2016) "Structured Equation Model for Determinants of Adoption and Use of Mobile Money Transfer Services in Uganda", Global Journal of Computers & Technology Vol. 5, No. 1; ISSN: 2394-501X, October, 2016.

[18]. Marchewka, Liu & Kostiwa 2007. An Application of the UTAUT Model for Understanding Student Perceptions Using Course Management Software, http://www.iima.org/CIIMA/13%20CIIMA%207-2-07%20Marchewka%2093-104.pdf

[19]. Moran, M. J. (2006). College Student's Acceptance of Tablet PCs and Application of the Unified Theory of Acceptance Technology (UTAUT) Model. Ph. D. Thesis. Papellas University. Minnesota, USA. Retrieved on 26 Sept. 2007, from: http://www.homepages.dsu.edu/moranm/Research/Mark-_for_research_v3.51with_IRB.doc.

[20]. Morris, M. G. and Venkatesh, V. "Age differences in technology adoption decisions: Implications for a changing work force," Personnel Psychology, 53, 2000. pp. 375- 403.

[21]. Moya Musa , Engotoit Benard , (2017) "Behavioral Intention mediator of performance expectancy and adoption of Commercial farmers' to Use Mobile-based Communication Technologies for Agricultural market Information Dissemination in Uganda", Operations Research Society of Eastern Africa - ORSEA Journal Vol. 7 (1), 2017.

[22]. Moya Musa, Nakalema Eva Stella, Nansamba Christine, (2017) "Behavioral Intention: Mediator of Effort Expectancy and Actual System Usage" Operations Research Society of Eastern Africa - ORSEA Journal Vol. 7 (1), 2017.

[23]. Nyesiga Catherine, Kituyi Mayoka Geofrey, Musa B. Moya, Grace Aballo (2017) "Effort Expectancy, Performance Expectancy, Social Influence and Facilitating Conditions as Predictors of Behavioural Intentions to Use ATMs with Fingerprint Authentication in Ugandan Banks" is in GJCST-E Volume 17 Issue 5 Version 1.0

[24]. Oye, N. D., A.Iahad, N., & A.b.Rahim, N. (2012a). Computer Self Efficacy, Anxiety and Attitudes towards Use of Technology among University academicians: A Case Study of University of Port Harcourt- Nigeria. International Journal of Computer Science and Technology. 3(1), 295-301.

[25]. Oye, N. D., A.Iahad, N., & NorZairah, A. (2011). An Application of the UTAUT Model for Understanding Acceptance and Use of ICT by Nigerian University Academicians. International Journal of Information Communication Technologies and Human Development, 3(4), 1-16.

[26]. Perez, M. P., Sanchez, A. M., Carnicer, P. L., & Jimenez, M. J. V. (2004). A technology acceptance model of innovation adoption: the case of teleworking. European Journal of innovation management, 7(4), 280-291.

[27]. Pu-Li, J. and R. Kishore, (2006). How Robust is the UTAUT Instrument? A Multigroup Invariance Analysis in the Context of Acceptance and Use of Online Community Weblog Systems. Retrieved on 28 Sept. 2006, from http://portal.acm.org/poplogin.cfm?dl.

[28]. Saloner, Garth, and Andrea Shepard (1995). "Adoption of Technologies with Network Effects: an Empirical Examination of the Adoption of Automated Teller Machines." Rand Journal of Economics, Vol. 26(3), pp 479-501.

[29]. Venkatesh, V., Morris, M.G., Davis, G.B., and Davis, F.D, (2003). User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, 27(3), 425- 478.

[30]. Venkatesh, V., and Davis, F. D. (2000) "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies," Management Science (45:2), 2000, pp.342-365.

[31]. Yahya, M., Nadzar, F., Masrek, N., & Rahman, B. A. (2011). Determinants of UTAUT in Measuring User Acceptance of E-Syariah Portal in Syariah Courts in Malaysia. Paper presented at the 2nd International Research Symposium in Service Management Yogyakarta Indonesia.

[32]. Yamin, M., & Lee, Y. (2010).Level of acceptance and factors influencing students' intention to use UCSI University's e-mail system. Paper presented at the User Science and Engineering (i-USEr), 2010 International Conference.