ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Issue 12, December 2016

Contribution of Emotional Intelligence and Cross Cultural Intelligence for Security Measures to Protect the Risk Management for Shaping Learning Organizations in the E-Voting Technology

[1]Megala L, [2]Devanathan B,
[1]Assistant Professor, Department of Electronics and Communication, V. R. S College of Engineering and Technology, Tamilnadu, India
[2]Lecturer, Department Electronics and Communication, University College of Engineering, Villupuram Tamilnadu, India

Abstract: In Today's world the implementation of remote electronic voting technology, one of the key issues that should be addressed is the security. Security solution has been a challenging task in the E-Voting Technology. Low voter's turn out problem can be compensated by introducing vote via mobile/internet. E-voting Technology can be used in countries like Brazil, Canada, Estonia, France, Germany, India, Ireland, Italy, Netherlands, Nigeria, Norway, South Africa, Switzerland, United Kingdom (UK), and United States of America (USA).Emotional Intelligence plays an vital role in the life of individuals. Emotionally intelligent steps candidate should be keep with the voters to get the votes from the people. Voters also should be emotionally intelligent to select the right person by the secure voting system. Towards achieving the specific objectives were as follows; To identify security challenges from the technical perspective that hinder the implementation of remote electronic voting, to identity security perspective in the operation of E-voting technology by the people (cross cultural Intelligence) in the rural and urban areas with different Qualification. Learning Organizations provide operations of E-Voting Technology to all sorts of people. To design a secure remote electronic voting model to overcome security challenges. The proposed system does not give room for making out any chance for guessing encryption and decryption pattern due to the use of quadruple vector algorithm and the use of sync code with the corresponding session key. The proposed system senses all these attacks after understanding an attempt of intrusion and take appropriate step to prevent the E-Voting technology from these attacks.500 Males and 500 Females were taken for study to test the Emotional Intelligence, Learning Organizations and Security Measures to protect the E-Voting Technology using Chi-Square and Rank Co-orelation. Study was made to prevent from third party in voting wrong vote instead of trusted vote and also study was made whether the E-voting Technology is secure or female feel that it is secure.

Keywords: Emotional Intelligence, Learning organizations, Cross cultural Intelligence, Quadruple vector algorithm

I. INTRODUCTION

Emotional Intelligence accounts for about 80% of a person's success in Life.IQ contributes 20 %.Being emotionally and culturally intelligent to efficiently manage the personal, social, cultural, Environmental change by coping with immediate solutions. Candidate standing in Election should show themselves emotionally intelligent for the people to select the efficient candidate. Emotionally intelligent in Technical perspective was designed and operations are performed to the people to show them the security measures designed to conduct the Election in the perfect manner. Charles Darwin (1872) speculated that emotions must be the key to the survival of the fittest. Information and communication era and the era of learning organizations or Cultural Intelligence the progress of advanced Technologies such as Networks, Telecommunications, satellites, Internet etc made it possible to have intense competition in various social, political,

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Issue 12, December 2016

educational, Scientific and Economic fields in different countries. Learning organization provide Training to operate the E-Voting Technology to vote in a secure manner. Remote electronic voting must be reliable and secure In particular, security requirements for remote electronic voting are as follows: to keep all votes secret , to ensure accuracy of the system without errors, to achieve democracy by allowing legal voters to vote only once with the password and destroy, to provide individual and universal verification to ensure that votes are registered correctly, and to ensure the system is available and accessible for all voters with the confirmation code and counted correctly and free from possibility to declare results before the election closes.

The idea is to give voters the possibility to vote from the location of their choice without the necessity of going to the polling station. The common sources of vulnerabilities are described below.

(i) **Voter Computer**: malicious computer can cast a vote without concern of the voter. But voter should be given user name and pass word where password is the confirmation code used only by the user to register the vote and destroy the password after putting vote.

(ii) **Voter Forwarding Server** (VFS): The communication link between voter's computer and Internet. There are different kinds of attack in this communication link. They are Close Quarters Battle Receiver Attack, Adaptive compat Rifle Attack, Heckier & Koch HK 416, Vektor- R4 attack.

(iii) **Voter Storage Server (VSS):** VSS database application faults enable irregular access to data and ignoring restrictions, therefore the fault freeness of VSS applications is also a major security issue.

(iv) **Voter Counting Server (VCS):** VCS is the most important component in the system. The voters vote with private key is Encrypted and digitally signed with Time stamp and send to vote counting server and the counting administrator decrypt with public key is decrypted at the end of election to declare the result.

(v) **Voter Anonymity:** VSS has encrypted and signed vote. VSS can identify the voter from this encrypted and signed vote but cannot decrypt the vote. Only VCS can decrypt the vote. If VFS and VCS both are corrupted then it can violate the voter's anonymity. Because VSS can unwrap the digital signature and mark the vote by time stamp or any other means then can send this to VCS. VCS can decrypt the vote and learn about the choice. Citizens cannot verify if their vote has been registered and counted correctly.

a.) Purpose of Study

Security Measures to Protect E-Voting Technology from attacks. Study was made among 500 males & 500 females and findings was made by chi-square, rank correlation, 2*2 contingency, Yules Q

Objective

(i) security measures were introduced in E-voting technology for its protection

(ii) Study was made to analyze whether the security measures was accepted by the individuals

(iii) Study was made to analyze whether the male feel the E-Voting technology is secure or female feel that is secure

(iv) Study was made to analyze learning organizations, Emotional intelligence and security Measures in the E-voting technology

b.) Low Robustness and Security of ICT Infrastructure

Although the government has established a National Information and Communication Technology Broadband Backbone, there is no government-wide established ICT security architecture and standardization.

Client-Side Attacks

Voters will be using their mobile phones or computers connected to the Internet to cast their votes. Mobile phones and computers are vulnerable to attacks and cannot be controlled by National Election Commission and therefore it is difficult to apply security measures at client side: (1) an attacker may alter a voter's choice without the user knowledge (2) an attacker cast the vote instead of the real voter, (3) an attacker could tamper with secrecy by recording the voter name and choice to then be made public, and (4) an attacker can also launch a denial of service attack to the voter's machine and hence hinder the possibility of the voter to vote.

Internet-Side/Gsm Attacks

Electronic votes will be transmitted via Internet or GSM network; an attacker can affect integrity, availability and confidentiality of the votes.

Server-Side Attacks

Server side attack can be initiated by political groups which may commit a wide scale fraud in order to safeguard their political interests.

Voter Coercion and Vote Buying

Coercion or vote buying takes place when a voter is pressured by others to vote in a way that he or she would not

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Issue 12, December 2016

have otherwise. This high level of vote buying and coercion was linked to the high level of corruption and poverty in the country.

Cyber Threats in the E-Voting Technology Addressing a Denial of Service Attacks to the Server

One of the typical network related attacks to the server is the denial of service attack. The DOS attack renders the services of the server unusable to the clients. Generally the DOS attack is possible by generating excessive load to the server and consequently exhausting its computing resources. In some cases by taking over legitimate nodes, attackers can swamp the server with unwanted messages. As passive attacks to servers attackers use malicious code such as virus and worms to cause malfunctions or halt their functions partially. Servers can be recovered by rebooting or some other methods when they cannot function properly.

Voters Identification and Authentication Mechanism

We propose three-factor authentication mechanism for identification and authentication of eligible voters. This will be enabled by Public Key Infrastructure (PKI) and a national electronic identity card (e-ID card).Before a vote is cast, a voter must be provided with e-ID card with PKI capability. Currently the government is issuing e-ID but a complete public key infrastructure is yet to be established.

HECKIER & KOCH HK416 ATTACK

The attacker intercepts an encrypted frame and uses the access point to guess the clear text. The attack is performed as follows: The intercepted encrypted frame is chopped from the last byte. Then the attacker builds a new frame 1 byte smaller than the original frame. The attacker makes a guess on the last clear byte. To validate the guess he/she made the attacker will send the new frame to the base station using a multicast receive address. If the frame is not valid (i.e., the guess is wrong) then the frame is silently discarded by the access point. The frame with the right guess will be relayed back to the network. The hacker can then validate the guess he/she made. The operation is repeated until all bytes of the clear frame are discovered.

Adaptive Compat Rifle Attack

The attacker sends a frame as a successive set of fragments. The access point will assemble them in to a new frame and send it back to the wireless network. Since the attacker knows the clear text of the frame, he can recover the key stream used to encrypt the frame. The attacker can use the key stream to encrypt new frames or decrypt a frame

Vektor-R4 Attack

The attacker exploits vulnerability in the virtual carrier-sense mechanism and sends a frame with the NAV field set to a high value. This will prevent any station from using the shared medium before the NAV timer reaches zero. Before expiration of the timer, the attacker sends another frame. By repeating this process the attacker can deny access to the wireless network.

II. LITERATURE SURVEY

Gomez et al.(2005) defined organizational learning as the capability of creation ,acquisition, transfer and integration of knowledge and improvement of organization's behavior to reflect new situation in order to improve the performance of organizations bar-on(1997) describes emotional intelligence as an arrangement of non-cognitive abilities competencies and skills influencing the ability of a person to make hm successful in consistency with environmental demands and pressures. The results of the works carried out by Lee-Kelley et al (2007) Ellinger et al(2002) ,Kane (2000) chang et al (2007) and vong chavalitkul et al (2005) show the impacts of learning Organizations a review of the researches carried out previously on learning organizations reveals that researchers classified organizational commitment and knowledge management (Massingham & Diment 2009)

Smaresim: An Improved Model of E-Voting System Based on Biometric Key Binding V.C. Ossai *, K.C. Okafor, H.C. Inyama , A.O. Agbonghae. The work in presented e-voting Schemes and explained that e-voting is a promising application of cryptography, which can have positive impact on democratic process. The work discussed cryptographic aspects of constructing e-voting schemes and approached the scheme from three perspectives viz: scientific, technical, and politico-sociological and tried to generate a preliminary framework on the notion of choice. The author added that on the internet, implementing cryptographic protocols like digital encryption and signature has been widely accepted. The authors in described the theory behind a practical voting scheme based on homomorphic encryption and gave an example of an ElGamal-style encryption scheme, which can be used as the underlying cryptosystem. The work presented the most important goals for electronic voting schemes viz: Privacy, Robustness, Universal verifiability and freeness.

An IC-Card-Based and Flexible t-out-of-n Electronic Voting Mechanism Chin-Chen Chang1,∗ and

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Issue 12, December 2016

Ting-Fang Cheng21Department of Information Engineering and Computer Science Feng Chia University Taichung 407, Taiwan

An electronic voting system must address essentials such as mobility, efficiency, verifiability, and robustness. Jan and Tai presented an electronic voting scheme using IC cards in 1997, and Chang and Lee proposed a out-of-electronic voting protocol in 2006. According to their different traits of out-of-and IC-card-based protocol, we consequently proposed a novel version to integrate these two protocols in this paper. By adopting IC cards, the authentication performance can be effectively promoted. The security of our scheme is based on symmetric and asymmetric cryptosystems. Our proposed scheme not only confirms most of the essentials of the general electronic voting scheme but also prevents potential malicious attacks. Furthermore, the computation overhead of the proposed scheme is less than that of the related methods.

The Technical Feasibility and Security of E-Voting Abdalla Al-Ameen and Samani Talab Department of Information Technology, University of Neelain, Sudan. An Electronic voting (E-voting) system is a voting system in which the election data is recorded, stored and processed primarily as digital information. E-voting may become the quickest, cheapest, and the most efficient way to administer election and count vote since it only consists of simple process or procedure and require a few worker within the process. The main task of this paper is to introduce the idea of the internet voting systems. It discusses the different ways in which voters can vote, then we introduce the concepts of E-voting system .This paper observes the security threats that may affect E-voting system. This paper discusses technical and secure attributes of a good E-voting system and the reason for each attributes with respect to the voting process. In this paper we analyze some researcher's efforts in E-voting systems in order to minimize the threats that compromise E-voting systems. We end with our opinion about technical feasibility of E-voting in developing countries.

Secure Electronic Voting Prof Dr. Dimitris Gritzalis Dept. of Informatics Athens University of Economics & Business & Data Protection Commission of Greece. An electronic voting (e-voting) system is a voting system in which the election data is recorded, stored and processed primarily as digital information. A PC-Based Open-Source Voting Machine with an Accessible Voter-Verifiable Paper Ballot Arthur M. Keller, UC Santa Cruz and Open Voting Consortium. Voting is the foundation of a democratic system of government, whether the system uses direct or representative governance. The heart of voting is trust that each vote is recorded and tallied with accuracy and impartiality. There is no shortage of historical examples of attempts to undermine the integrity of electoral systems. The paper and mechanical systems we use today, although far from perfect, are built upon literally hundreds of years of actual experience.

Encrypted Receipts for Voter-Verified Elections Using Homomorphic Encryption by Joy Marie Forsy the Voters are now demanding the ability to verify that their votes are cast and counted as intended. Most existing cryptographic election protocols do not treat the voter as a computationally-limited entity separate from the voting booth, and therefore do not ensure that the voting booth records the correct vote. David Chaum and Andrew Neff have proposed mix net schemes that do provide this assurance, but little research has been done that combines voter verification with homomorphic encryption. This thesis proposes adding voter verification to an existing multi-candidate election scheme (Baudron et al.) that uses Paillier encryption. A "cut and choose" protocol provides a probabilistic guarantee of correctness. The scheme is straightforward, and could easily be extended to multiauthority elections. The feasibility of the proposed scheme is demonstrated via a simple implementation

Citizens 'Readiness for Remote Electronic Voting in Tanzania Sylvester Kimbi1Irina Zlotnikova2 the Nelson Mandela African Institution of Science and Technology (NMAIST) School of Computational and Communication Science and Engineering

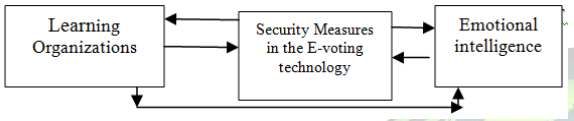
Remote electronic voting through Internet or mobile phones can potentially increase citizens' electoral participation in countries with low voter turnout such as those in Sub-Saharan Africa. This paper measures citizen's readiness for remote electronic voting in Tanzania.Factors influencing citizens' readiness was identified. These factors were further analyzed using SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis Primary data were collected from eligible voters us in questionnaires. Using descriptive statistics and Chi-square, we determined socio-demographic and technical factors impacting voters' perception of remote electronic voting versus the current paper ballot system. The results indicate that the majority of

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Issue 12, December 2016

Tanzanians prefer remote electronic voting as an alternative to the existing voting system. However, they have concerns related to security, privacy and reliability of this new technology. We conclude that remote electronic voting entails a promising opportunity to increase voter participation in Tanzania; however the "right" enabling environment should be created to ensure its successful implementation and sustainability.

Conceptual Frame work of the research



III. EXISTING & PROPOSED MODEL

A. System and participating parties

The proposed model consists of the following components.

(i) Electronic Voting Client Application (e VCA): This is an application that runs on voter's computer or mobile phone. The application consists of the candidate information, the key storage and generation functions

(ii) Electronic Voting Central System (e VCS): This is a core system responsible for collection of electronic ballots, storage and tabulation. The roles of the e VCS are fulfilled by four different servers as follows.

(a) Mobile Authentication Module (MAM) which is an entity within GSM network but is considered as part of electronic voting central system. This component is used to authenticate voters who would like to vote via mobile phones. MAM generates the authentication parameters and authenticates the mobile phone users.

(b) Vote Relying Server (VRS) which is responsible for authenticating voters who would like to vote via internet, distributing electronic ballot to voters and accepting the votes. The VRS should be available over the Internet.

(c) Vote Storage Server (VSS) which is responsible for storing the electronic votes over the period of time and for the anonymization of the votes before the actual tabulation is done. The VSS should be kept behind a firewall

(d) Vote Counting Server (VCS) which is responsible for the tabulation process. VCS should be offline at all the times to avoid attack.

(iii) Receipt Generator. This component is responsible for computation of confirmation codes. The confirmation codes are sent directly to the voters, after receiving this feedback the voter can compare between his choice of options and receipt code, If the receipt codes matches the selected options, the voter can be assured that his vote is recorded as intended.

(iv) Key Management Server (KMS): This component generates and manages the key pair(s) of the system. The public key (keys) are integrated into e VCA, private key(s) are delivered to VCS.

(v) Auditing Module: This component is an application which solves disputes and complaints using logged information from the central voting system

(vi) Population Register: This component is a database for citizens' personal data. It is maintained by National Identity Authority

(vii) Voters and candidate registers: This is a database for eligible voters and candidates. The database is maintained by National Election Commission

(viii) Digital Certificate Validation Server: This server checks the validity of digital certificates of e-card holders. The server should be operated by independent entity.

A total of 530 Electronic Voting Machines and 265 control units would be used for the by-election while 1,150 election officials would be on duty and 230 additional employees would also be there on polling day (June 27). Two lakh forty thousand and forty three people are there in RK Nagar consistency. Among that one lakh eighteen thousand nine hundred people are men and one lakh twenty one thousand five hundred and eight are females.75 people are gay.

Disadvantages of Existing System

The existing systems suffer fromt the following problems

- Poor Hardware Infrastructure
- Very Low Virtual Memory
- Very Low Hard disk Capacity
- Slow Processors
- Virus infected Systems often created problems
- No Intrusion Protection Mechanism

B. Proposed System

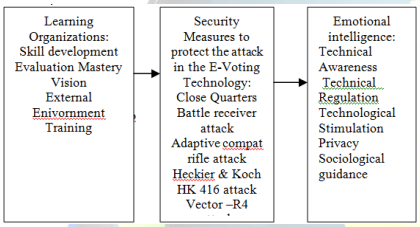
Synchronization code is generated, the public part of which is integrated into client software and is used to encrypt the vote. The private component of the syn code is used in the vote counting server to decrypt the vote. To increase the security of the counting server, the code should only be used during counting period. When the election period ends, the private key must be destroyed and should not be used in any other election. The Proposed Local Area

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Issue 12, December 2016

Networking has a lot of enhanced future. There is a high powered and capacity servers/back up servers well connected to workstations node through switches. Election in R.K Nagar at Chennai introduced Electoral assistant system to send email, sms, or by phone to know the voters list and which booth have to vote .in that proposed idea I given is secured password to be given which user have to utilize during election to vote which was known by the third party but known by the counting administrator who will reveal the result when the election is over on that particular day itself. by phone how the names in the voters list will be identified and displayed EPIC 1 voter number, voter name will be displayed by sms. Election both where to vote can be identified by EPIC 2 voter number then the election both where to vote will be displayed by phone. EPIC voter number epicsearch@chennaicorporation.gov.in to identify the voter name in list and booth to vote by email.

Operational Frame work of research



Yule's Q

Yule's Q is a popular measure of association for nominal data and a method which is very easy to compute. It was named after a famous statistication qutelet. This measure rests on the principle that if values are set in a four cell table the cross products of the internal diagonal cells will be equal when no relationship exists between the two variables. This principle is reflected in the formula given below

$$Q = \frac{AD - BC}{AD + BC}$$

A,B,C and D refer to the cells of the relevant table. The computation of Yule's Q is very simple .It involves the following steps.

Step 1: First we set up a four – cell table with its cells clearly marked using letters from A to D

Step 2: Substitute the values in the formula and compute Q.

2*2 fold contingency table

When the contingency table is 2*2 fold x2 may be calculated without first computing the four expected frequencies the four independent values

Chisquare

Chisquare are the most popular and most frequently used tests of significance in Social Sciences. They Provide information about whether the corrected data are close to the value considered to be Typical and generally expected and whether two variables are related to each other

Rank Correlation

Spearmans coefficient of correlation after the name of the inventor, Rank order correlation co-efficient is computed by the formula

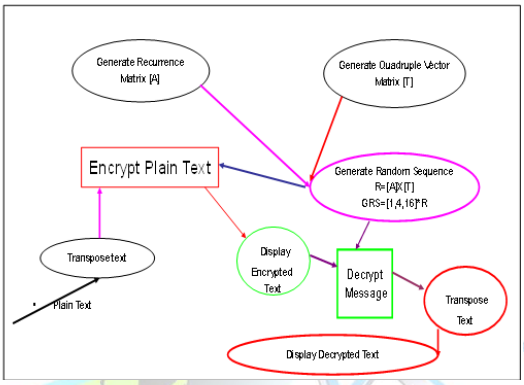
$$\text{Rank Correlation} = 1 - \frac{6ED^2}{N(N^2 - 1)}$$

Where D is the difference between two sets of ranks

ED^2 is the sum of the squared difference of the ranks

N is the Total number of observations

ARCHITECTURE



IMPLEMENTATION

Following Quadruple vector Algorithm is used for implementing the process

1. A recurrence matrix used is as a key. Let it be A.
2. Generate a "quadruple vector" T for 44 values, i.e from 0 to 255.
3. Multiply r=A*T;
4. Consider the values to mod 4.
5. A Sequence is generated using the formula [40 41 41]*r.
6. This Sequence is used as a key
7. Convert the plain text to equivalent ASCII Value
8. Add the key to the individual numerical values of the message
9. New offset the values using the offset rules
10. This would be the cipher text generated

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Issue 12, December 2016

11. For the Decryption the key is subtracted from the cipher text and use the offset rule to get the original message.

A Study on introduced security measures will be useful in the e-voting technology analysis between 500 males and 500 females carried out in the following table whether there is positive or negative response in males and females.

Attitude	females	males	total
positive	270 A	260 B	530
negative	240 C	230 D	470
total	500	500	1000

$$Q = \frac{AD - BC}{AD + BC}$$

$$Q = \frac{(270 * 240) - (260 * 230)}{(270 * 230) + (260 * 230)}$$

$$Q = \frac{5000}{A121900} = 0.041$$

A sample of 500 boys drawn at random from the population showed 220 at or above the national norm in the E-voting security usefulness 170 below the national norm.A random sample of 500 girls showed 240 at or above the national norm and 240 below. are the boys really better than girls in knowing the analysis of e-voting technology data are arranged in a fourfold table as follows

A 220	B 170	A+B 390
C 240	D 240	C+D 400
A+C 410	B+D 420	790

$$X^2 = \frac{N(AD - BC)^2}{(A + B)(C + D)(A + C)(B + D)}$$

$$= \frac{790(52800 - 40800)^2}{(390)(400)(410)(420)}$$

$$= 4.21$$

Chisquare : f0 fe f0-fe (f0-fe)2 (f0-fe)2/fe

Learning Organizations	**100**	**100**	**0**	**0**	**0**
Security Measures to protect the attack	**150**	**100**	**+50**	**2500**	**25**
Emotional intelligence	**50**	**100**	**-50**	**2500**	**25**

We find that the critical value of ChiSquare for 2 degrees of Freedom at 5% (o.5) level of Significance is 5.99%.The Calculated value of ChiSQuare is 50 which is greater than its critical Value 5.9,our chisquare is significant and H0 is regected.

Rank correlation:

Individuals A	Learning organizations	Emotional intelligence Y	**R1**	**R2**	**D2**
A	105	90	3	2	1
B	50	120	1	3	-2
C	130	45	4	1	3
D	140	150	5	4	1
E	75	175	2	5	-3

$$\text{Rank Correlation} = 1 - \frac{6(0)}{5(24)} = 1$$

III. Conclusion

This study identified security challenges from technical perspective that hinder the implementation of remote electronic voting. The study also identified security requirements that remote electronic voting must comply with. These requirements are in line with general principles of democratic elections. We reviewed and analyzed several remote electronic voting models with respect to security. Study was made to analyze whether the security measures was accepted by the individuals. Study was also made to analyze whether the male feel the E-Voting technology is secure or female feel that is secure was derived using 2*2 contingency, Yules-Q derived successfully. Emotional intelligence, Learning Organizations with security Measures to protect the attack in the E-voting by Chi-square and rank correlation.

References

[1]. ACE Electoral Knowledge Network. "Focus on EVoting".Retrieved on 26th July 2012 from the website www.aceproject.org/ace-en/focus/e-voting/countries?toc,2012.

[2]. Alvarez, M. R., Thad, E. H. and Trechsel, A. H."Internet Voting in Comparative Perspective: The Case of Estonia". Political Science and Politics, 42: 497–505, 2009.

[3]. Barrat, J., and Goldmith, B. "International Experience with E-Voting: Norwegian E-Vote Project". Retrieved on 13th September 2012 from the website www.regjeringen.no, 2013

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Issue 12, December 2016

[4]. Cranor, L., and Cytron, R. "Sensus: a securityconscious electronic polling system for the Internet". In:Proceedings of the Thirtieth Hawaii International Conference on System Sciences,2007,Vol. 3, pp. 561-570.

[5]. Chowdhury, M. J. "Comparison of e-voting schemes: Estonian and Norwegian solutions". International Journal of Applied Information Systems, Vol 6, No 2, 2013, pp 47-54.

[6]. The European Union (EU). "Tanzania Final Report –General Elections of October 2010". Retrieved on 16thMarch 2014 from the website http//eeas.europa.eu,2010

[7]. Fennazi, S. "Security questions hang over e-voting plans". Retrieved on 4th January 2014 from the website"http://origin.swissinfo.ch/eng/security-questions-hangover-e-voting-plans/32567608, 2011.

[8]. Gerlach, J., and Gasser, U. "Three Case Studies from Switzerland: E-Voting, 2009". Retrieved on 4th January 2013 from the website http://cyber.law.harvard.edu,2009.

[9]. Giampiero, E.G. "E-Voting through the Internet and with Mobile Phones". Retrieved on 27th December 2013 from the website http://unpan1.un.org,2010.

[10]. Heiberg, S. "Internet Voting – the Estonian Experience". Retrieved on 6th November 2013 from the website http://cyber.ee,2010.

[11]. The International Telecommunication Union (ITU). "ICT facts and figures". Retrieved on 3rd January 2014 from the website www.itu.int,2013

[12]. Kimbi, S. G. and Zlotnikova, I. "Citizens' Readiness for Remote Electronic Voting in Tanzania". Advances in Computer Science: an International Journal, Vol. 3, 2014, Issue 2, pp 150-159.

[13]. Kowero, A. B,"Exploiting the Potentials of the National Information and Communication Technology Broadband Backbone (NICTBB) in Tanzania". Retrieved on 29th June 2013 from the website http://www.tanzania.go.tz/egov_uploads, 2012

[14]. Kothari, C. R. "Research Methodology: Methods and Techniques", New Age Publication", New Delhi, 2004.

[15]. Maaten, E. "Towards Remote E-voting: Estonian Case". Retrieved on 6th July 2013 from the website http://subs.emis.de/LNI/Proceedings/Proceedings47/Proceeding.GI.47-9.pdf2004, 2004

[16]. Senge PM(1990).The Fifth discipline :Art and Practice of the learning Organizations

[17]. Zeidner M.Matthews G.Roberts RD(2004) Emotional intelligence in the work place a critical review