iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 Issue: VII Month of publication: July 2015

DOI:

www.ijraset.com

Call: ✆08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Security Measures To Protect The Risk Management In The E-Voting Technology

S.Binilsundar,(Phd)[1], Annie Steffi Sydney[2]
[1]Assistant professor, Computer science and Engineering, [2]ME 2nd year
Savetha university, Loyola institute of technology and science
Chennai, Thovalai,kanyakumari dist,Tamilnadu

Abstract— ***The rapid evolution of Information and Communication Technology (ICT) in today's world, However, prior to the implementation of remote electronic voting technology, one ofthe key issues that should be addressed is the security. The importance of security in electronic voting system has been recognized for some time now but implementing a comprehensive security solution has been a challenging task. Countries with similar problems have introduced electronic voting via mobile phone and/or Internet in an attempt to alleviate low voters' turnout problem. These countries include Brazil, Canada, Estonia, France, Germany, India, Ireland, Italy, Netherlands, Nigeria, Norway, South Africa,Switzerland, United Kingdom (UK), and United States of America (USA). Literature review shows that electronic voting was successful in some countries including Estonia and Switzerland while others such as USA and UK have stopped using them due to security concerns. 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 requirements for the remote electronic voting system,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.study was made between male and female and checked whether it will be acceptable by the public.Analysis was made among 500 males and females and been successful for the implementation of security measures in E-voting technology***

I. INTRODUCTION

The government is currently issuing national digital identity cards equipped with a computer-readable microchip. The microchip contains all the information and personal data of the citizens, cryptographic keys, random number generators and algorithms needed to carry out all the computations on behalf of the voter. It also contains an image of the citizen, as well as their fingerprints . The problem with the current digital electronic cards being issued is that a complete PKI support is yet to be implemented However, plans are underway to have the complete PKI implemented. Secure Electronic Registration and Voting Experiment (SERVE) which was introduced in 2004 in USA. SERVE is the Internet based voting system built for the Department of Defense's federal voting assistance program. However, the project was abandoned due to anonymity issue where the web server could know the vote of each voter. There were no public key infrastructure and digital identity cards used for authentication in SERVE.

In 2009 Norway initiated a procurement procedure for "E-valg 2011", an electronic voting pilot project for 2011 municipal and regional elections. The Norwegian model also uses double envelope system to insure integrity of votes and voter's secrecy. Many other remote electronic voting models, such as Australian and Canadian models have been implemented over the years. However, most of these models havelimitations. Estonian model and the Swiss model which address most of the security issues. Remote electronic voting must be reliable and secure as traditional democratic elections and referendums which do not involve the use of electronic means . In particular, security requirements for remote electronic voting are as follows: to keep all votes secret , to ensure accuracy of the system without interference or errors, to achieve democracy by allowing legal voters to vote only once, to provide individual and universal verification to ensure that votes are counted correctly, and to ensure the system is available and accessible for all voters and free from possibility to declare results before the election closes. Remote electronic voting in Estonia is meant to supplement the traditional methods of voting. 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 .

A. Voter Computer (VC):

©IJRASET 2015: All Rights are Reserved

The computer could be virus affected or affected by any kind of malware. A malicious computer can cast a vote without concern of the voter.

B. Voter Forwarding Server (VFS)

The communication link between voter's computer and VFS is Internet. There are different kinds of attack in this communication link. Internet connection provider can stop the traffic or delay the traffic. Since VFS is in open Internet, denial of service attack is also possible against VFS.

C. Voter Storage Server (VSS)

VSS database application faults enable irregular access to data and ignoring restrictions, therefore the faultfreeness of VSS applications is also a major security issue.

D. Voter Counting Server (VCS)

VCS is the most important component in the system. The public key of VCC is open to all voters and used in encryption of the vote. VCA private key should under no conditions become public and must not under any circumstances be destroyed or become unusable. The source of vulnerability in VCS is from operating system, memory or any kind of virtualization.

E. 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. Now if VSS and VCS collaborate together it can identify the voter and learn about his choice. The remote electronic voting model used in Switzerland is an adaptation of its postal model. From security perspective Switzerland does not use digital signatures like Estonia. However, the system operates similarly with respect to the envelope feature which keeps the ballot and voter's identity separate . With the system used so far in electronic voting trials "citizens cannot verify if their vote has been registered and counted correctly . Like Estonian system. Swiss system is also subjected to various security threats. These threats include (1) denial of service attack, (2) vote buying and coercion, and (3) web spoofing.

II. OBJECTIVE

Security measures were introduced in E-voting technology for its protection

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

A. Low Roubustness 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.

B. 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 countermeasures at client side. The majority of the respondents (77 percent) were concerned that unreliable voters computers or mobile phones would create serious problems leading to compromising the integrity of the entire election. Depending on the nature of the attack, possible risks could be as follows: (1) an attacker may randomly alter a voter's choice without the user noticing, (2) an attacker can impersonate a real voter and 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.

C. 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.

©IJRASET 2015: All Rights are Reserved

D. Server-Side Attacks

There was a possibility for an attacker to interact with the remote electronic voting system, its interfaces or parts of it to exploit vulnerabilities. This may compromise security and affects all voting system components. This can be initiated by political groups which may commit a widescale fraud in order to safeguard their political interests.There is also a possibility for denial of service attack that would prevent voters from casting their vote in the system. This may result into having the legitimacy of the whole election being compromised.

E. Voter Coercion And Vote Buying

Remote electronic voting would present a greater opportunity for voter coercion or 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 have otherwise. This high level of vote buying and coercion was linked to the high level of corruption and poverty in the country.

F. 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 can not function properly. Normally these recoveries actions can be taken in to short time since servers are always cared by authorized operators. In this sense the damage on servers would have little impact on the functions of clients and it is unlikely to cause any severe damage such as power outage to the system. Compared to servers attacks to clients will make more dangerous effects since they are directly responsible for operations in the field and are installed mostly unattended in remote site. There is no a technical solution that can totally prevent a Denial of Service (DOS) attacks. However, there are administrative controls to reduce the impact of the attack when it occurs Moreover a robust disaster recovery plan should be implemented to minimize the impact associated with DOS attacks.

G. 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

H. Identification,Authenticationand Authorization

National digital identity card (e-card) with Public Key Infrastructure (PKI). currently issuing e-cards but a full PKI support is yet to be implemented. We therefore propose that full PKI and e-cards should be used for authentication and identification of eligible voters. If fully implemented, the new e-card will support most authentication technologies, including storing password,one-time passwords, PKI certificate and supports the generating of symmetric key pairs. Each card should therefore contain two pairs of asymmetric keys. The first pair should be used for authentication and the second one digital signature. Certificates binding the public keys to the cardholder’s identity should be stored on the card and in an online database. As an additional security control each key should be associated with a secret code (PIN) to authorize every operation.

I. Ensuring Authenticity,Secrecy And Integrity Of The Votes

To ensure votes authenticity, secrecy and integrity of the votes, we adopt the double envelope scheme adopted from the Estonian model, the The votes are collected, sorted, voter’s eligibility is verified and invalid votes are removed. Then the outer envelopes (digital signatures) are separated from inner envelopes (encrypted votes). Voter lists are compiled from outer envelopes. Inner envelopes (which are not associated with the identity of the voter any more) are forwarded to the vote counting server. The vote counting server decrypts the votes using is private key and produces results of electronic voting.To ensure integrity of the votes, a client computes a “digital hash" of the encrypted ballot before the voter sends it off. The vote storage server computes the same “digital hash” and returns this hash value to the voter along with the confirming receipt. The voter then checks that the two codes match, thus the voter can confirm that the integrity of the votes has not been compromised. The digital hash is a fixed-length value computed based on the encrypted ballot that makes it impossible for either the contents or length of the encrypted ballot to be recovered by the attacker.

©IJRASET 2015: All Rights are Reserved

J. Ensuring Votes Verifiability

To ensure variability of the votes, we introduce two mechanisms: Auditing by independent bodies and a possibility for voters to verify using independent channel that votes are recorded as casted. Through independent auditing we can ensure that every step of the election is working accordingly. Generally, all the processes of the system have to be audited. The voter can also verify that his ballot was included in the counting process. This can be done using vote verification code. The verification codes are computed by receipt generator. The verification codes are sent directly to the voters, After receiving this feedback the voters can compare between their choice of options and receipt code. If the receipt code matches the selected options, the voter can conclude that the vote is recorded as intended.

K. 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.

L. 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

M. 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.

III. LITERATURE SURVEY

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 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 TalabDepartment of Information Technology, University of Neelain, Sudan

©IJRASET 2015: All Rights are Reserved

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.

Web based secure e-voting system with fingerprint authentication Adem Alpaslan ALTUN and Metin B Selcuk University, Technical Education Faculty, 42031, Konya, Turkey. Selcuk University, Natural and Applied Sciences Institutes 42031, Konya, Turkey.

The elections that are made by using traditional methods are no longer preferred because of the long period of preparation, fake voting, faulty voting, mistakes made in counting the votes, long period of counting and high cost of voting process. In order to avoid these disadvantages affecting directly the economy and policy of the country, it is obligatory to carry the available voting system to an electronic system. In this study, an electronic voting system, E-voting for a general election is developed and fingerprint authentication based e-voting system is applied. As a result, security of the voting system is greatly improved by using biometric authentication system.

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 usetoday, 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 Forsythe 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 mixnet 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 were 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 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.

IV. EXISTING & PROPOSED MODEL

System and participating parties: the proposed model consists of the following components.

A. 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

B. 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.

1) 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.

2) 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.

3) 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

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

C. 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.

D. 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

E. Auditing Module

This component is an application which solves disputes and complaints using logged information from the central voting system

F. Population Register

This component is a database for citizens' personal data. It is maintained by National Identity Authority

G. Voters and candidate registers

This is a database for eligible voters and candidates. The database is maintained by National Election Commission

H. Digital Certificate Validation Server

This server checks the validity of digital certificates of e-card holders. The server should be operated by independent entity. If the voter decides to vote via Internet, the processes are as follows;

1) The voter launches the client application and inserts her ID card and enters the first PIN number to establish Secure Socket Layer(SSL) connection. The client verifies the server's identity using a hard-coded certificate.

2) Once a secure connection between a client and VRS is established, the client sends a message with its credentials (second pin number and fingerprint) digitally signed with its private key corresponding to the public key in voter's digital certificate.

3) VRS then validates the digital certificate of the voter

4) VRS checks if the voter is eligible using the data from the population register maintained by National Identity Authority. If the voter is not eligible, a corresponding message is delivered. If the voter is eligible, VRS performs a query from the VSS whether such voter has already voted. If this is the case, the voter is informed about it.

5) The voter receives electronic ballot and select a candidate

6) VFS asks the user to confirm the choice.

7) When issued a choice of candidate and political party the voter clicks to submit the vote.

8) e_VCA encrypts voter's choice and a random number with the public key of the VSS. The voter signs the entire package (as a double envelope scheme) with private key that belongs to him

9) E_VCA transmits the digitally signed envelope to the VRS which verifies the formal correctness of the received material.

©IJRASET 2015: All Rights are Reserved

10) The entire envelope is then sent to VSS.

11) In case of successful vote the VSS sends the VRS a confirmation that the vote has been received. The voter receives an SMS containing the receipt code corresponding to the vote he issues, and can verify this code is correct against the codes on his voting card. By this mean the voter can for instance detect if a malicious program on his computer has changed the ballot. The receipt code can also be used for the voter to verify his vote is present in the latter e-counting process.

12) An entry about receiving of the vote is recorded in the log-file

13) Finally VSS separates inner envelopes from outer envelopes and readies them for the Vote
Counting Application (VCS) .If the voter decides to vote through mobile phones, the voting processes are the same as for Internet voting except that the voter uses a mobile phone and authentication is done through the mobile authentication module instead of the vote relying server. The proposed GSM mobile voting scheme is part of the central voting system and thus voters can choose to vote through the Internet or the GSM network. If voters want to vote through GSM, they have to be registered and obtain a special SIM card with the embedded cryptographic algorithm and national identity. SIM cards should be registered by mobile phone operators in collaboration with National Election Commission. There exists a Local Area Network System During the Election time having at least 40 work stations nodes connected to the LAN Server. The topology followed is Bus

I. Disadvantages of Existing System

The existing systems suffer fromt the following problems

1) Poor Hardware Infrastructure
2) Very Low Virtual Memory
3) Very Low Hard disk Capacity
4) Slow Processors
5) Virus infected Systems often created problems
6) No Intrusion Protection Mechanism

V. 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 cod 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 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.

A. Advantages Of Proposed System

1) Advanced Hardware architecture
2) L1,L2 Cache Technology
3) Very High Storage Capacity of Hard disk drives
4) High Speed Processors
5) Fully Protected From Virus
6) Intrusion Protected

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=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.

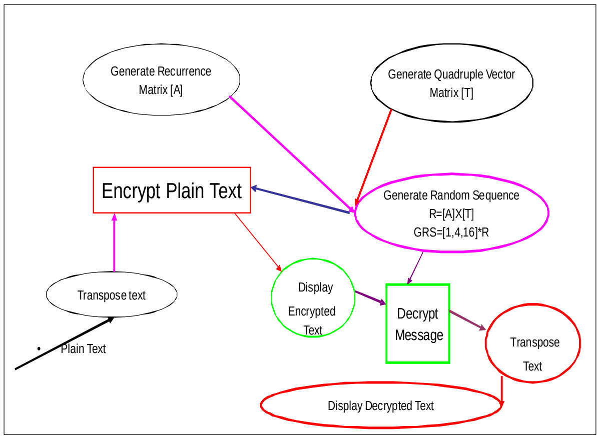
Step 1 : First we set up a four – cell table with its cells clearly marked using letters from A to D

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

©IJRASET 2015: All Rights are Reserved

B. Architecture

ARCHITECTURE


Generate Recurrence Matrix [A]
Generate Quadruple Vector Matrix [T]
Encrypt Plain Text
Generate Random Sequence R=[A]X[T] GRS=[1,4,16]*R
Transpose text
Display Encrypted Text
Decrypt Message
Transpose Text
Plain Text
Display Decrypted Text

C. Implementation

Following Quadruple vector Algorithm is used for Implementing the process

1) A recurrence matriz used is as a key.Let it be A..
2) Generate a "quadruple vector" T for 44 values,i.efrom 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
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=AD-BC/AD+BC=(270*240)-(260*230)/(270*230)+(260*230)
=5000/121900=0.041

VI. 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.

VII. FUTURE ENCHANCEMENT

We strongly recommend that remote electronic voting should not be implemented prior thorough testing and therefore we emphasize the need for the government to initiate a number of pilot and test projects. Properly planned pilot projects and systematic

©IJRASET 2015: All Rights are Reserved

evaluation should be done as soon as possible, with the aim of testing various technical solutions and enhancing the voters' confidence in remote electronic voting.

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

[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] Msyani, C. M. "The Current Status of Energy Sector in Tanzania". Retrieved on 14th September 2012 from the website http://www.usea.org/sites/default/files/event-/Tanzania%20Power%20Sector.pdf, 2012.

[17] The National Democratic Institute (NDI). "Report on the 2005 Zanzibar Elections". Retrieved on 23rd January 2014 from the website https://www.ndi.org, 2005.

[18] Schwartz, J. "Online Voting Canceled for Americans Overseas". Retrieved on 3rd April 2012 from the website http://www.nytimes.com, 2004.

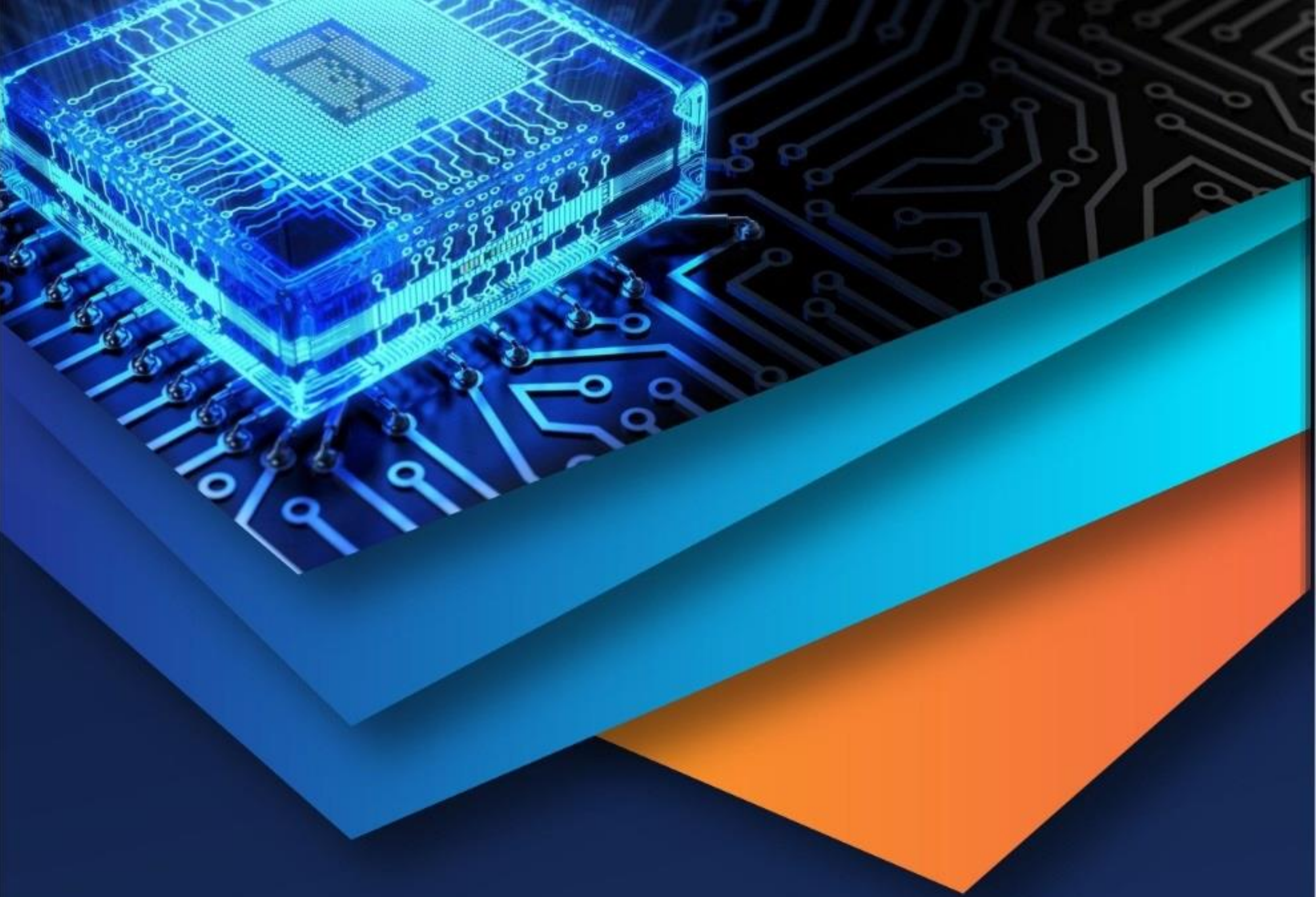
[19] Seyondeka, E. "Obstacles in Bridging the Digital Divide in Tanzania". International Journal of Computing and ICT Research, Vol. 6, Issue 1,pp 60, 2012

[20] Tanzania Communication Regulatory Authority (TCRA)."Quarterly Telecommunications Statistics". Retrieved on 29th November 2013 from the website www.tcra.go.tz, 2010.

[21] Tanzania National Identity Authority (NIDA). "National identity Cards Registration – Progress Report". Retrieved on 5th October 2013 from the website www.nida.go.tz, 2010.

[22] Qiuel,.Y, and Zhu, H. "Somewhat Secure Mobile Electronic-Voting Systems Based on the Cut-and-Choose Mechanism". Retrieved on 10th September 2013 from the website http://www.computer.org/csdl/, 2009

©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR: 7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)