iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** X **Month of publication:** October 2017

DOI: http://doi.org/10.22214/ijraset.2017.10283

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue X, October 2017- Available at www.ijraset.com

E-Voting For Large Scale Elections Using Simple Network Management Protocol

Anil Pandit[1], R. C. Gangwar[2]
[1]*Research Scholar, I.K.G. Punjab Technical University, Kapurthala, Punjab, India*
[2]*Associate Prof.Dept. of Computer Sc. & Engg. BCET, Gurdaspur, Punjab, India.*

Abstract: ***Democratic process world-over is a very important referendum, which elects or removes governments. Elections are held in countries where large number of voters vote to elect their favourite candidate. This paper proposes an E-Voting through Internet, which uses Simple Network Management Protocol (SNMP) for large-scale elections to be held on decentralised servers. The proposal of using Simple Network Management Protocol is a unique one because SNMP based NMS (Network Management System) could be implemented during voting, which manages, monitors and get the accurate data of voters ballots from the decentralised servers in regular intervals for compilation of data at a centralised server that can be much accurate, authenticated, authorized and coercion free. SNMP operating server can be easily managed as wecan compile data for the number of voters from a particular region or state who had voted on the voting day, and the results or data cannot be tampered with. Devices being used in casting ballots on election day can also be managed well. Numerous advantages could be achieved if SNMP implemented systems are being implemented by the election commission in the online e-voting system. Main objective of this paper is to propose a solution to monitor and manage the large-scale elections with secrecy,and curtail coercion, which is necessary to get hundred-per-cent accurate results for effective democracy.***
Keyword: EVM, Coercion, MIB, SNMP, UDP, NMS.

I. INTRODUCTION

To provide additional channel for voting apart from conventional is necessary to augment voter count for a fair democracy.To use the existing infrastructure more efficiently, Election identity cards enable secure online-authentication and the use of digital channels is steadily widening. It is time consuming to change voters' practices and approaches and to increase the voter turnout. Internet voting that is also known as e-voting brings people closer to the information society. Integrated functioning of public sector IT systems raises the cost-efficiency. Internet voting is there to stay. On the voting day, e-voter votes through any electronic device e.g. Mobile device, Laptop etc… with a valid identity number given to him/her by the election commission.

This paper proposes the use of Simple Network Management Protocol (SNMP) in e-voting infrastructure / architecture, which will help to keep track of devices e.g. election servers, databases containing ballots and how they function during election-day.Dealing with problems and emergencies in the network (router stops routing, server loses power, machines are being tampered with, mobile devices, systems etc.). E-Voting can be through any device e.g. any voter who votes through any mobile device can cast her/his vote and the ballot is stored in the nearest local server of the election commission. These local servers are managed and guarded by the Centralized servers which can be done by loading SNMP based Network Management System (NMS) in all the managed systems. If the electronic devices are so intelligent, then why to bother with the network management protocol? Devices don't then to have an analysis of an entire network, but SNMP do. Managing devices using SNMP is called a Network Management System (NMS). In this paper we show how SNMP helps to solve the problem of coercion and security in E-Voting. NMS enables fast access to faults. The functional areas where SNMP could be useful in e-voting are as follows,

A. Fault Management
B. detection, isolation and correction of abnormal operations by the electronic devices
C. Configuration Management
D. identify managed resources and their connectivity, discovery
E. Accounting Management
F. keep track of usage for charging if any
G. Performance Management
H. monitor and evaluate the behavior of managed resources
I. Security Management

J. allow only authorized e-voters access and control

II. LITERATURE REVIEW

SNMP could be useful when implemented meticulously in e-voting system. J. Alex Haldermanet. al. in[1], has clearly shown that how easy is to reach and change the secret ballot and election officials are not able to detect the culprits. It is now becoming the need for a secure democracy.

Hari K. Prasad, et. al.[2] discuss the important flaws in the electronic voting machines used in one of the largest democracies in the world. This paper also elaborates as how much loss and dependence the government shows while reaching to every voter to cast his/her vote. Atsushi Fujioktaet.al.in [3], Jonker et. alin [4] explained the very fundamental definitions that the voting is secure only when all the following properties of E-Voting exists a) Completeness b) Soundness c) Privacy d) Eligibility e) Fairness f) Un-reusability f) Verifiability. "CORE BANKING SOLUTION: Evaluation of Security and Controls" titled by Sriram, M. Revathy in[5] elaborateshow core banking solutions are being managed by Simple Network Management Protocol. It is well known to each of us, how much comfortable life has been made by introducing Internet banking solutions.

LisandroZambenedetti Granville et. al. in [6] Evaluated the performance of SNMP and web services notifications. Internet http services against SNMP notification messages have been described. Evaluation of the performance of the proposed solution in order to redraw the current conclusions about http services against Network Management Protocol is also elaborated. Ronald L. Rivest et al. in [7], proposed Scratch & Vote, a cryptographic voting system that can be implemented with today's technology, at very low cost and minimized complexity. EVM's used in many countries including India and the process followed by the Election Commission officials have many flaws as explained by GVL NarshimhaRoain [8], K.N.Bhar in [9], Shubina et al.in [10] and Wolchok et al. in [1] . These literatures were the base line for organising this paper into a new fresh need for the future of E-Voting in respect to security and coercion.

III. E-VOTING ARCHITECTURE AND PROPOSED IMPLEMENTATION OF SNMP

A. Simple Network Management Protocol in NMS

NMS is an acronym for Network Management System. NMS uses Simple Network Management Protocol. In real world almost every organization has a good technology infrastructure such as Electronic-mail solutions, central database systems, web servers, developer environments, test environments, employee workstations, for its success. All these assets are running in the server of the organization's network. Since web is animportantcommercial aspect of any group, it is very important to monitor thenetwork.

A network consists of manyvaried, multivendor composite, interrelating hardware and software possessions. The resources comprise physical devices such as routers, bridges, hosts, terminal servers, modems, links, interfaces, apart from many protocols that controls and coordinates these devices. When hundreds or thousands of such components are interfaced together by an organization to form a network, day by day network operation management and strategic network growth planning became extremely difficult due to the following facts.

1) Increased complexity of network topologies &technologies;
2) Deployment of a large number of incompatibletechnologies; and
3) Election Network often located in remotesites, rural areas

Hence avital need arises to monitor a network and to have an expert system of control. To cater this need Network Management System emerged. The branch of science which refersto the activities related with running and governing a network, along with the technology required to support those activities is called network management. Election Network can be managed easily.

B. Architecture of E-Voting Protocol using SNMP

Though SNMP protocol is having its own architecture, a general or basic model of E-Voting network architecture is designed with the following key elements.

1) Managementstation (Election Monitoring NMS)
2) Management agents (Election servers)
3) Management informationbase (NMS Database)
4) Network managementprotocol (SNMP)
5) Authentication Servers

C. FCAPS for E-Voting

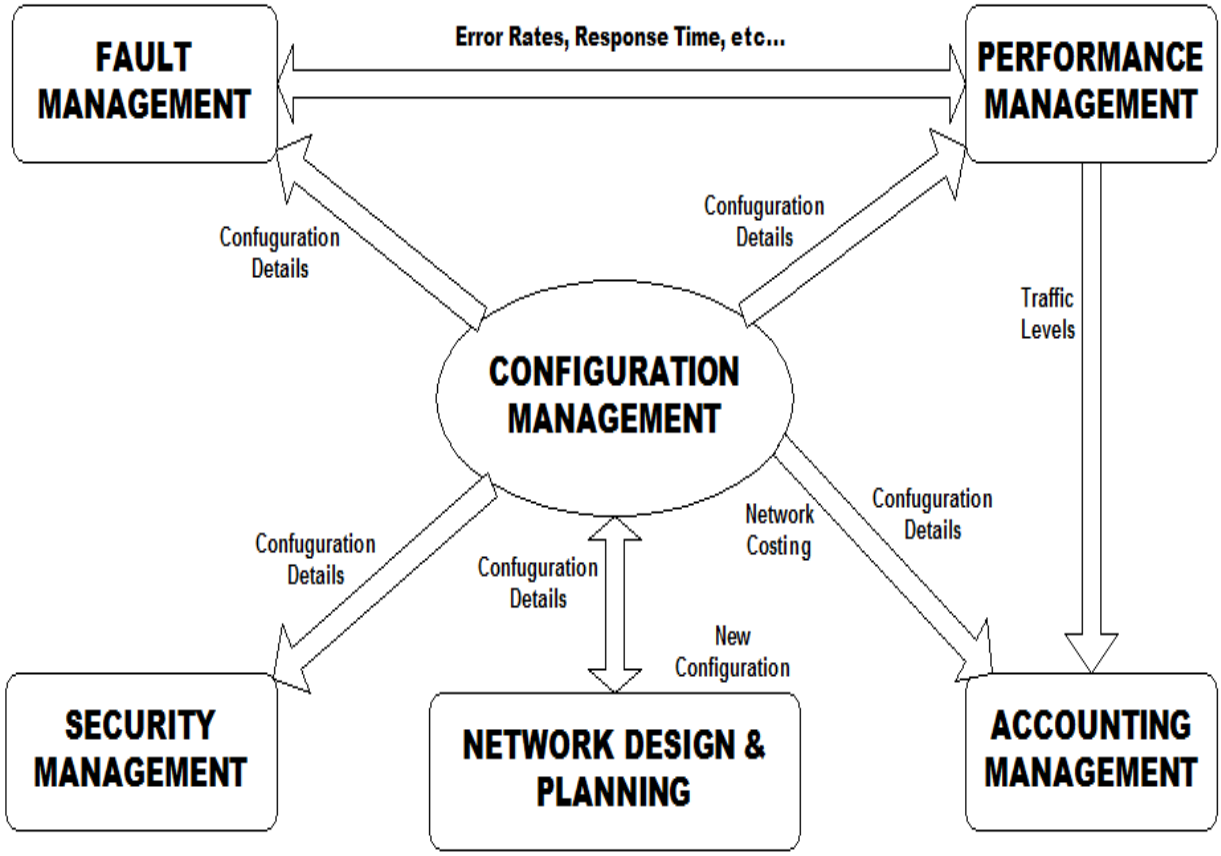


Figure 1: FCAPS for Internet Voting

D. Fault Management

Fault Management Utility manages network problems during election to keep the network of election commission running reliably and efficiently.Fault management process does the following thing:

1) Detecting the problem symptoms. Isolating the problem.
2) Rectifying the problem routinely (if possible) or manually.
3) Logging the detection and resolution of the problem if any voter cannot figure it out or the problem is from the decentralized server of election authority.

E. Configuration Management

Configuration Management utility monitors e-voting network and system configuration information and stores it in a configuration management database e.g. MIB (Management Information Base). The maintenance of this database allows e-voting network administrators to track hardware (election server, election proxy servers), software, and other e-voting network resources during the election process.Each e-voting network device has a variety of information associated with it.Software version information for the election operating system, voting protocol software, or voting management software.Hardware version information for the interfaces or hardware controllers used in conventional Electronic Voting Machines (EVM's). Election officials contact information indicating who to contact if problems with the device arise. Location and information indicating the physical location of the device of the e-voting app device.

F. Accounting Management

Accounting Management utility measures e-voting network parameters in order to regulate individual and group uses of the network.

Minimizes network problems and maximizes fairness of e-voter user access to the network because network resources can be portioned based on network capacity and e-voter user needs.

G. Performance Management

Performance Management utility maintains e-voter internetwork performance at acceptable levels by measuring and managing various network performance variables. Performance variables include network throughput during the election-day, user response times, line utilization, and others. Performance management involves three basic steps:

1) Gathering election data relating to key performance variables;
2) Analyzing election data to determine the normal (baseline) performance levels; and
3) Determining appropriate performance thresholds for each variable so that exceeding these thresholds indicates a network problem, which needs proper attention.

H. Security Management

Access control utility controls access to e-voter network resources, and prevents network sabotage (intentional or unintentional) and unauthorized access to sensitive information. Aids election officials / administrators in creating a secure election network environment. This includes, partitioning network resources into authorized and unauthorized mapping groups of users to those areas which are divided according to the e-voter user density, andmonitoring, policing, and logging user access to resources in the areas likeElection Security monitoring, Election Security event collection,ElectionEvent analysis, correlation and alert generation and alert handling .

I. E-Voting Model

Organization of E-Voting prototype describes the components of network management such as a manager, agent and so on, and their relationships. The implementation of these components leads to different type of architectures.The Two-Tier Model, Three-Tier Model, Manager of Managers and Peer NMS. A network object called as network elements consists of hosts, hubs, bridges, routers, e-voter devices etc. Network objects are classified as managed and unmanaged elements or objects. The managed objects have a management process running in them called agent. Unmanaged objects do not have agent running in them. The manager communicates with the agent in the managed object. The functions of manager, agent and managed object are given below.

J. Manager

1) Sends requests toagents;
2) Monitorsalarms;
3) Housesapplications for E-Voter; and
4) Provides userinterface for E-Voter;

K. Agent

1) Gathers information e.g. Ballots fromobjects;
2) Configures parameters ofobjects;
3) Responds to managers'requests; and
4) Generates alarms and sends them tomangers;

L. Managed object

1) Network element that ismanaged;
2) Houses managementagent; and
3) All objects are not managed /manageable

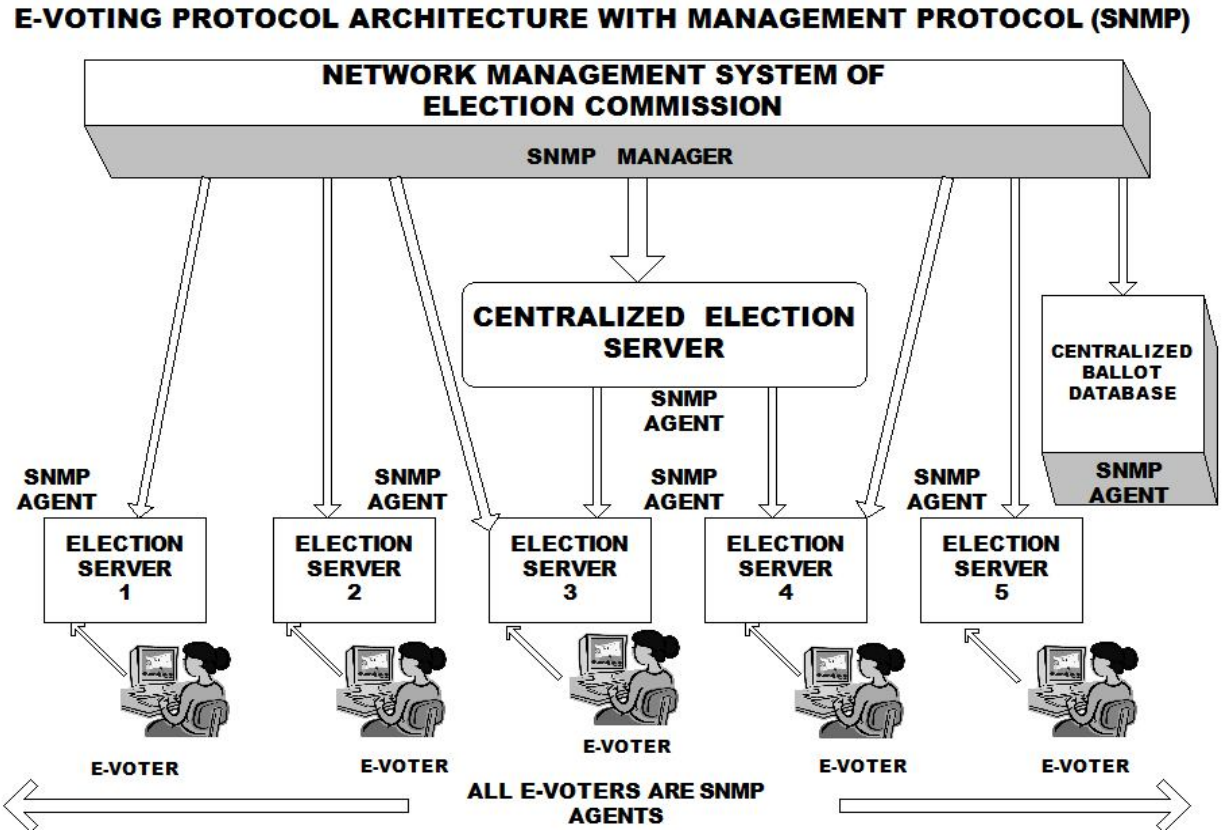


Figure 2: E-Voting Architecture Managed by Network Management System

M. Working of the E-Voting MODEL

There are two types of devices, first, unmanaged and secondly managed devices. Those that are confidential as unmanaged devices do not have the ability of being analyzed by a network management protocol or application. In the figure 2, each agent is manageable by the manager. Agents are E-Voting devices, election servers etc… On the other hand, a managed device allows a network administrator or information technology professional in the election commission to manage the device. Each managed network device such as a router, gateway, or an election server, e-voter mobile device, centralized database of ballots stored has a collector called an agent. The agent gathers information about the device, and stores that information in a database called the management information base (MIB). If voters are at remote locations and voting through mobile devices using an e-voter application on any device, which are manageable, then it is very meticulously controlled by the NMS (Network Management System) of Election Commission. Sometimes thisisreferredtoasamanagermanagingamanageabledevice,andin this manager is a database that contains the information collected by an agent and then processed. The manager is typically a server (NMS) with network management software on it that sends requests to the agents, which are located on the manageable networkdevices.

Regarding coercion, if a voter votes through any device and if any coercer coerces him then he can vote again without any hesitation to show the coercer that vote has been casted by him/her through the managed device. But only his/her first vote casted will be counted, which will be locked by the NMS at the first instance. Later on, if any e-voter wants to change his/her casted vote then he/she can vote again to please the coercer but this vote will not be counted by the voting server. And NMS will automatically reject his vote internally by sending a message to the e-voter that his vote has been accepted, this message will be a lookalike as voted for the first time and sending a unique acknowledgement number which will be the same sent earlier at casting ballot, which will remain the same always as a unique number to each individual voter throughout the country.

NMS uses SNMP and a UDP (User Datagram Protocol) to send a receive messages between the manager and the agent. Because SNMP uses User Datagram Protocol, this brands the data transmission less reliable due to the absence of replies of appeals and conveyance of data. In its place, a network manager can set a timeout on the manager to send another appealto the agent if there is no response. Managers either poll the agent orobtain traps from an agent. During the process of voting, the manager queries the agent to retrieve data about that device. This webevidence is usually referred to as a protocol data unit (PDU),which an object that

has variables, data types, and values. This information is sent back to the manager and stored in the database. In a process of a trap, the agent sends information to the manager without a request. An example of this could be a UPS (uninterruptible power supply) that has a SNMP agent sending information about the battery running out of power in any side of the country where voting process is going on. As Simple Network Management Protocol there are no acknowledgments with sending and receiving of protocol data units, traps that are sent from agents can be lost and the agent will not be notified of the lost data. This may lead toproblems, so it is up to the infrastructure we design before starting this process of e-voting. SNMP can be a very powerful tool in E-Voting. It allows for the continual analysis of the network owning manageable devices. This consistent flow of analysis can help network managers detect for potential problems. For example SNMP can be used to monitor performance on a router, tell what speed a connection is on the network, and even monitors the temperature of a switch used for sending the election data in and out.
And, to securethe ballots, voters and election network infrastructure, SNMP has advanced version i.e. SNMPv3 which has a security model and is developed to protect the following security threats:
Modification of information: Contents modified by unauthorized e-voter.
Masquerade :Change of originating address by unauthorized e-voter user
MessageStreamAlteration: Re-ordering, delayreplay of messages.
Discovery of messages:Eavesdropping.
SNMPv3 provides important security features:
Message Integrity to ensure that a packet has not been tampered with intransit.
Authentication to confirm that the message is from a legalsource.
Encryption of packets to stop snooping by an illegalperson.

N. Usm&Vasm

SNMP has an important version that has an architecture introduced as a User-based Security Model (USM) in SNMPv3 for message security and the View-based Access Control Model (VACM) for access control. USM uses the notion of a user for which security arguments (levels of safety, verification and privacy protocols, and keys) are configured at both the agent and the manager. Messages sent using USM are better protected than messages sent with community- based security, where passwords are sent in the clear and can be displayed in traces. With USM, messages exchanged between the manager and the agent have data integrity checking and data origin authentication.

O. User-based Security Model(USM)

It was planned in RFC 2274 and it describes the User-based Security Model for SNMPv3. It defines the Elements of Procedure for providing SNMP message-level security. The USM protects the user against four threats, which are as follows:

1) Alteration ofinformation / messages / data;
2) Masquerade;
3) Message streammodification; and
4) Disclosure(optionally).

The USM uses MD5 algorithm (Message Digest Algorithm) and the Secure Hash Algorithm to provide data reliability, to directly guard against data alteration attacks / threats, to indirectly provide data origin verification, and to defend against masquerade attacks / threats. It also uses Data Encryption Standard (DES) to protect against expose.

P. View-based Access Control Model(VACM)

It was projected in RFC 2275 and it defines the View-based Access Control Model for SNMPv3. It defines the Elements of Procedure for controlling access to management information. The VACM can simultaneously be associated in a single engine Implementation with multiple Message Processing Prototypes and multiple Security Prototypes. The document also includes a MIB for remotely managing the configuration parameters for the View-based Access ControlModel.

Q. SNMPArchitecture

SNMP entity

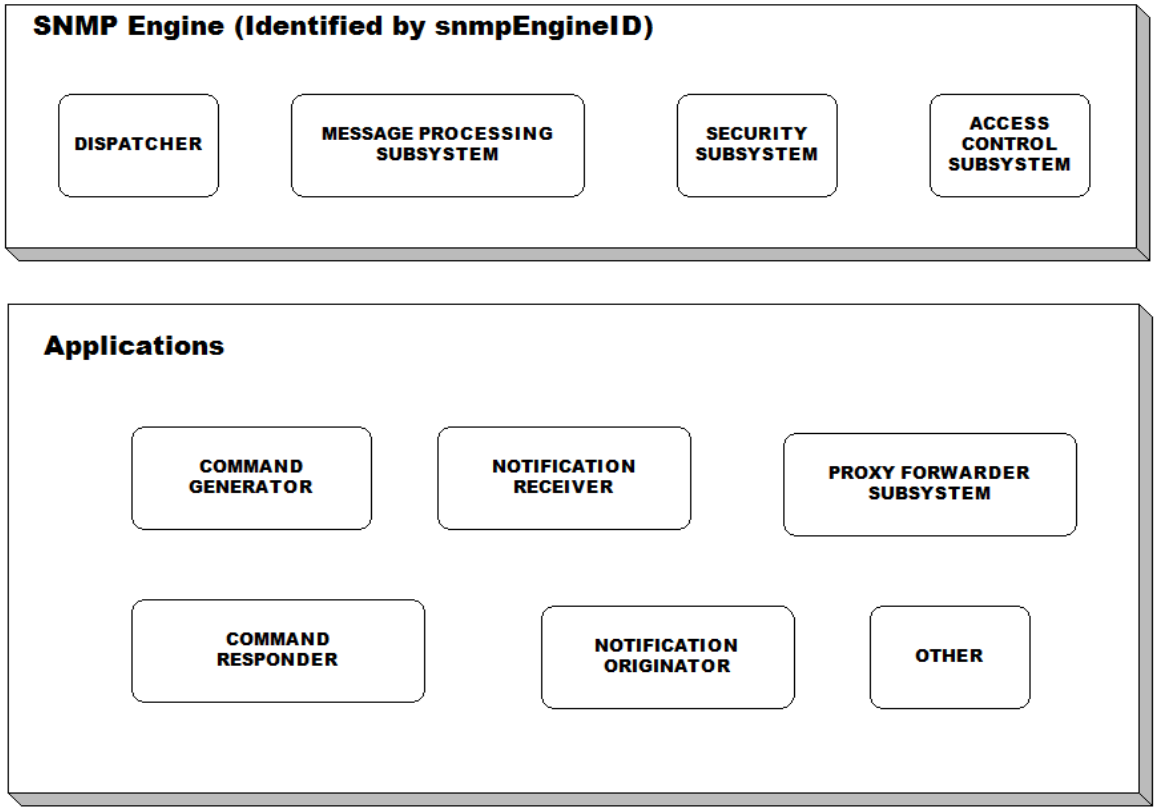


Figure 3: SNMPv3 Architecture

Fig. 3 depictsto understand SNMP V3 architecture. An SNMPv3 in the above figure has an engine which offers services for sending and receiving messages, validating and encoding messages, and controlling access to managed objects. There is a one-to one relationship between an SNMPv3 engine and the SNMPv3 entity which contains it. Within amanagerialarea, ansnmpEngineID is the unique and unequivocal identifier of an SNMP engine. Since there is a one-to-one association between SNMP engines and SNMP entities, it also uniquely and unequivocally identifies the SNMP entity within that administrative domain. Note that it is possible for SNMP entities in different administrative domains to have the same value for snmpEngineID. The SNMPv3 engine comprises (a) a Dispatcher (b) a Message Processing Subsystem (c) a Security Subsystem, and (d) an Access Control Subsystem. There is only one Dispatcher in an SNMPv3 engine. It allowsforconcurrentsupportofmultipleversionsofSNMPmessagesin the SNMP engine. The Message Processing Subsystem is responsible for preparing messages for sending, and extracting data from received messages. The Message Processing Subsystem can potentially covers multiple Message Processing Models, for example one for processing SNMPv1 messages and another for SNMPv2c and yet another for SNMPv3. The Security Subsystem provides security services such as the authentication and privacy of messages and potentially contains multiple Security Models. The Access Control Subsystem provides authorization services by means of one or more of Access Control Models.

Applications contain command generators, which monitor and manipulate management data, command responders, who provide access to management data, notification originators, which initiate asynchronous messages, notification receivers, which process asynchronous messages, and proxy forwarders, which forward messages between entities. These applications make use of the services provided by the SNMP engine. An SNMP entity containing one or more command generator and/or notification receiver applications (along with their associated SNMP engine) has traditionally been called an SNMPmanager.

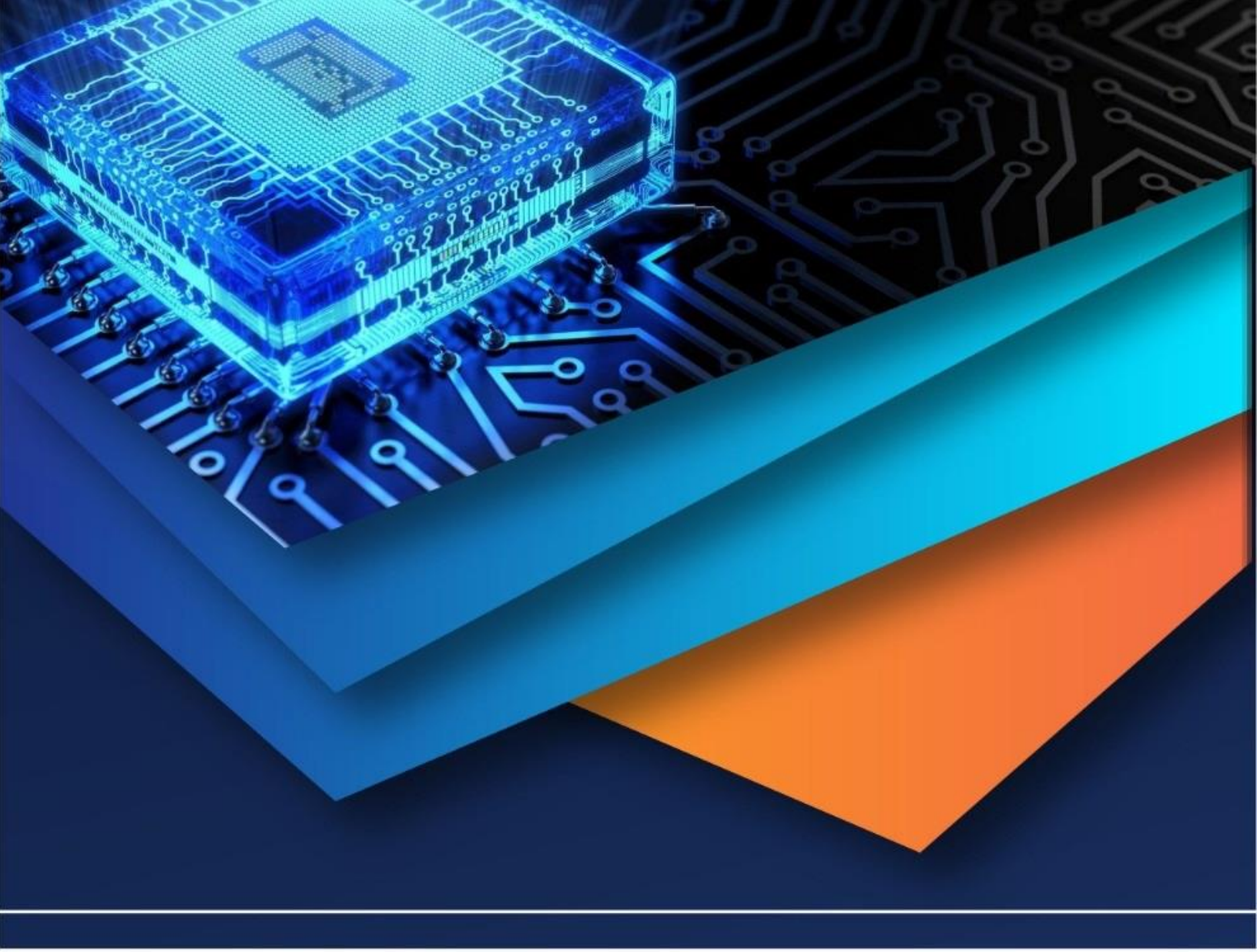
IV. CONCLUSIONS

Globally successful democracies are thus, that employ secure technologies, which create confidence inproposed work, whichcould bring a major change to the mind-set of those who ignore e-voting through internet as a network due to several doubts / misconceptions. This paper explained methods to resist Coercion and Security threats,that SNMP protocol will definitely change the digitisation of the Voting process.

Simple Network Management Protocol for managing each and every device. This can help Election officials to easily check whether the voter has voted or not or voter has any type of online difficulty in voting. Election devices could be easily managed from a centre point. Coercion can be removed by implementing a solution of locking the first time voter's vote and giving the choice to dodge a coercer by voting again to show that we are voting in front of him. Several other advantages can also be fixed using this E-Voting working model in practical e-voting system by halting the electronic voting machines (EVM) or any paper trial method using manual force. Security can be enhanced by User-based Security Model (USM) and View based access control Model (VASM).

REFERENCES

[1] Wolchok, Scott, Eric Wustrow, Dawn Isabel, and J. Alex Halderman. "Attacking the Washington, DC Internet voting system." In International Conference on Financial Cryptography and Data Security, pp. 114-128. Springer, Berlin, Heidelberg, 2012.
[2] Wolchok, Scott, Eric Wustrow, J. Alex Halderman, Hari K. Prasad, ArunKankipati, Sai Krishna Sakhamuri, VasavyaYagati, and RopGonggrijp. "Security analysis of India's electronic voting machines." In Proceedings of the 17th ACM conference on Computer and communications security, pp. 1-14. ACM, 2010
[3] Fujioka, Atsushi, Tatsuaki Okamoto, and Kazuo Ohta. "A practical secret voting scheme for large scale elections." In International Workshop on the Theory and Application of Cryptographic Techniques, Springer Berlin Heidelberg, pp. 244-251.1992
[4] Jonker, Hugo,SjoukeMauw, and Jun Pang. "Privacy and verifiability in voting systems: Methods, developments and trends." Computer Science Review 10, pp. 1-30.2013
[5] Sriram, M. Revathy. CORE BANKING SOLUTION: Evaluation of Security and Controls. PHI Learning Pvt. Ltd., 2013.
[6] de Lima, W. Queiroz, Rodrigo Sanger Alves, Ricardo LemosVianna, Maria JanilceBosquiroli Almeida, Liane Margarida RockenbachTarouco, and LisandroZambenedetti Granville. "Evaluating the performance of SNMP and web services notifications." In Network Operations and Management Symposium, 2006. NOMS 2006. 10th IEEE/IFIP, pp. 546-556. IEEE, 2006.
[7] Adida, Ben, and Ronald L. Rivest."Scratch & Vote: self-contained paper-based cryptographic voting." In Proceedings of the 5th ACM workshop on Privacy in electronic society, pp. 29-40.2006
[8] GVL NarshimhaRoa, "Democracy at Risk" in Title of His Published Book, Ist ed. New Delhi, India, Sharp Prints,2010
[9] K.N.Bhar, Letter No. 51/8/16/4/2007 PLN-IV Dated: 12th October,. [Online] Available:www.eci.nic.in, 2007
[10] Shubina, Anna M., and Sean W. Smith. "Design and prototype of a coercion-resistant, voter verifiable electronic voting system." In Proc. of Conference on Privacy, Security and Trust, pp. 29-39, 2004.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY