International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 5 (2015) pp. 12915-12928

http://www.ripublication.com

Online Monitoring And Counting Of Voting Using Zigbee Protocol And Cloud Computing

[1]S.Karthikeyan, [2]K.Vimala Devi, [2]K.Valarmathi

[1]Department of Electronics and Instrumentation Engineering
M.Kumarasamy College of Engineering,Karur
[2]Department of Computer Science Engineering
[2]Department of Electronics and Communication Engineering
P.S.R. Engineering College,Sivakasi

ABSTRACT

Voting is an important system to determine the opinion of the society people to make their government. The data on voting machine will change due to any technical problem came after voting, in-charge person can misguide and change of data can possibly during the transportation of machines or even may destroy in the place of storing the machine for counting purposes. Due to this above concern government expenses lot of money and employees time for securing the machine up to the counting day. In this proposed Wireless based Electronic Voting Machine (WEVM), the above mentioned problems are avoided and also the counting of votes can be monitored in real time and the result of society people to determine the government can get on that day itself. Here the system matches the vote counting at the time of voting and keep it in the database of election commission through the wireless network. The implemented framework uses cloud computing to store and retrieve the database of election commission and also designed with a security framework. By this method the reliability and security of the result can get with minimum expenses.

KeyWords: ElectronicVoting Machine, ATmega16 Micro Controller, ZigBee, Cloud Computing, Security in private cloud

1. INTRODUCTION

The Electronic Voting Machine was most vitally use in National elections, also in the applications like business, shareholder meeting, student body election, and parliament for passing of legislation This process should be in good efficiency, reliability, easy to use, sooner to get the result with lower cost and also to avoid the manual paper based processes, with this concern the electronic machine was established in the year of

1989, to match up with all the benefits. Even though a wide usage of electronic voting machine is there, but still the problem arising in the security, reliability and transparency in getting results [1-3].

Fig. 1. Conventional Electronic Voting Machine

Basically the electronic voting machine work with a collection of peoples' opinion with less security and not a smart enough to handle the data. However an analysis shown the system used today is critically deficient [4-6]. For evaluation and to compete with more effective after everything the standard set of procedures, performance, and function was developed, but it is not enough to match the problem concern [7-8].

To satisfy this reason by improving the device with high speed of getting results, more reliability, security and efficiency also by reducing the manual data error, misguide of in-charge as well as to avoid expenses and government employees time for protecting EVM storage area and not to wait for result up to counting day [9-11]. The idea of Wireless based EVM was proposed in this paper, here all the EVM's are connected under the single network and collect the voters count on all the EVM's and store it in Election commission database using cloud computing with all the particulars of the parties from a district ward, etc.,. By this method the result can get with above concerned factors and the result can be announced on the day of the election itself.

2. PROPOSED ELECTRONIC VOTING MACHINE

The conventional Electronic Voting Machine diagram was shown in figure. 1 It reduces the time in both casting a vote and declaring the results compared to the old

Paper Ballot System. EVM was manufactured in 1989-90 by The Industrial design (Product Design) It was updated by ECIL, Hyderabad in the year of 1998.

The conventional Electronic voting machine consists of two units, They are Ballot unit and Control unit. The Existing system has lots of negative aspects like Damage of EVM, loss of data,misguidance of EVM and Time taken to get the result. To attain all this needs

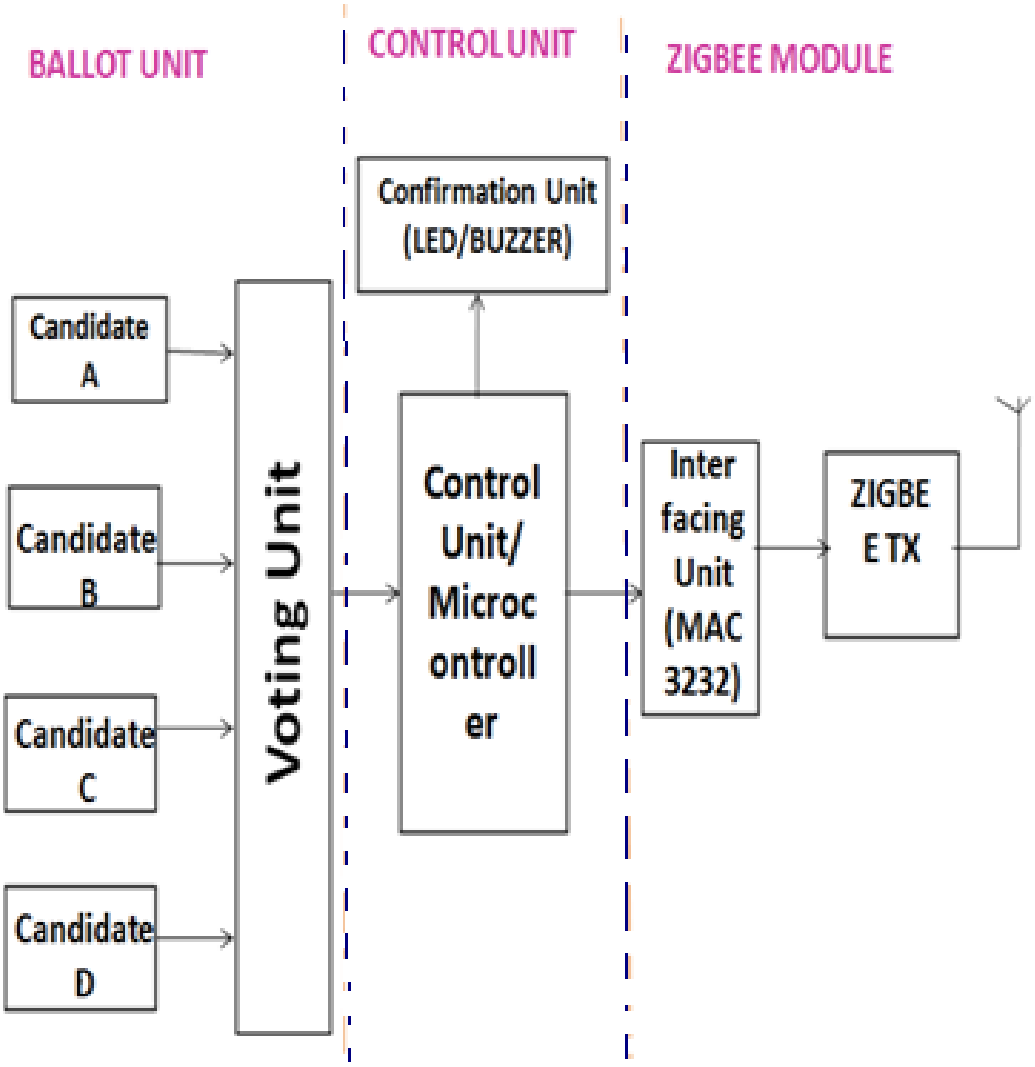

Fig. 2. Proposed Electronic voting Machine Block diagram

the proposed voting machine system was created fig. 2 shows the proposed block diagram of EVM. The proposed EVM method consists of Ballot Unit, Control Unit and ZigBee Module.

2.1 Ballot unit

The ballot unit is a simple device, which displays the list of candidates, party names and symbols are inbuilt. Here the voters need to press the desired switch located next to their interested candidate name and can watch the success of voting by the glowing of confirmation LED and by the beep sound indication. The ballot unit contains sixteen candidate buttons. If any buttons are not used, it is covered with a plastic masking tape. If the candidates are more than sixteen, another ballot unit can be added to a port of the primary ballot unit. Up to four ballot units can be chained together in this way, for a maximum of 64 candidates. These ballot units are joined by a five-meter cable to the control unit.

2.2 Control unit

It is the heart of the machinery that controls its operations such as conduction of polling, display the information like the number of voters polled and the declaration of result. It contains all necessary information needed by the presiding officer and by just pressing a button, The candidate wise result can be obtained and a transmitter unit interfaces with the control unit for transmitting all information parallel to the election commission for analyzing the polling status on all booths in a state, also for monitoring and to get the results quickly.

2.3 ZigBee Module

The growth of network and communication technology plays a vital role in the world. The WSN has put out a lot of difficulties in the engineering field. It has many advantages compared to wired networks, recently many near field wireless communication technology was used, particularly for Bluetooth, Wireless Local Area Network (WLAN), infrared, etc. But, they have a number of disadvantages like complexity, large power consumption, short coverage range, networking in small scale. But the ZigBee wireless/ IEEE 802.15.4 standard will satisfy all this demand, [12].

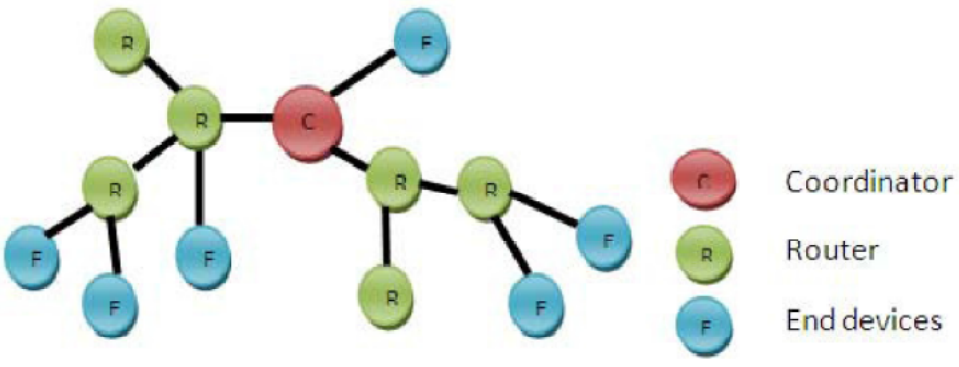

Fig. 3. ZigBee Model Network

ZigBee was launched in August, 2001, it authoritatively named ZigBee 2007. It offers full wireless mesh networking capable of supporting more than 64,000 devices on a single network. ZigBee [13] [14] is a standard protocol designed for low power devices used in wireless monitoring and control systems. The protocol supports star; tree and mesh topologies. In star topology, all devices communicate directly with the coordinator. Tree and mesh topologies allow increasing range of the network by introducing routers that relay the traffic from the end devices (EDs). The ZigBee specification enhances the IEEE 802.15.4 standard by adding network layer and security layer and an application framework.

2.3.1 ZIGBEE INTERFACE WITH EVM

The ZigBee Module network was shown in the figure. 3. It consists of a ZigBee coordinator (ZC), ZigBee Router (ZR) and ZigBee End Device (ZED). ZigBee coordinator is the most important device, the coordinator forms the root of the network tree and link to other networks. Only one ZigBee coordinator was attached in each network since it is the device that starts the network initially. It stores the information about network and also acts as the Trust Center & repository for security keys. ZigBee Router (ZR) runs an application function and it acts as an intermediate router, passing data from one device to other devices. ZigBee End Device (ZED) contains sufficient functionality to talk with the parent node and it cannot transmit data from other devices. It allows the node to be in asleep mode for a major amount of the time, thereby giving long battery life. ZED requires the small amount of memory, and therefore can be less expensive to manufacture than ZR or ZC.

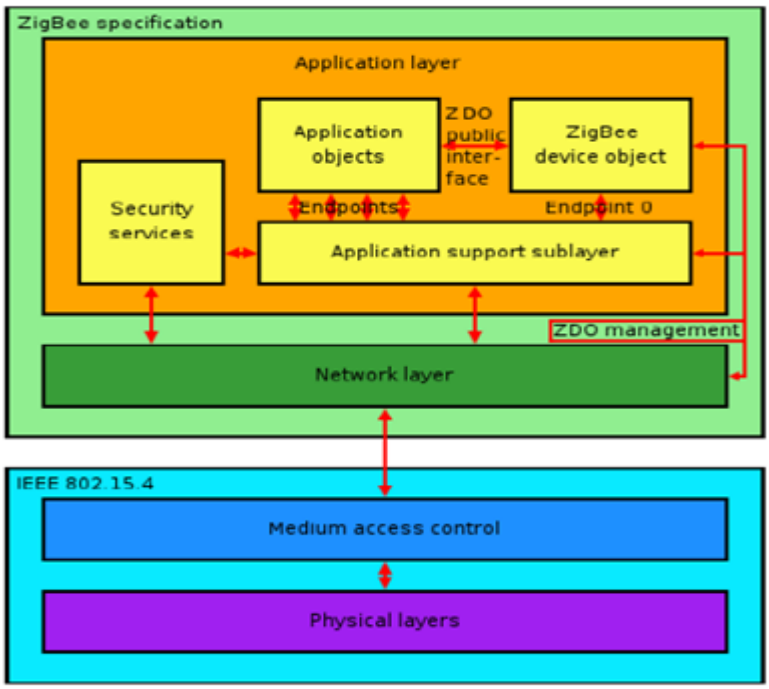

Fig. 4. ZigBee Protocol

2.3.2 ZigBee Protocol Architecture

The protocols uses a recent algorithm to automatically construct a low-speed ad-hoc network of nodes [15]. The majority of network will be a cluster of clusters for large network and furthermore the network forms a mesh or a single cluster. The ZigBee protocols support beacon and non-beacon facilitated networking. In non-beacon-enabled networks, an unspotted CSMA/CA channel access mechanism is exercised. In this type of network, ZigBee Routers normally have their receivers in active, requiring more power supply. On the other hand, this adopts heterogeneous networks in which, some devices receive continuously and others only transmit when an external motivation is detected. The Zigbee protocol was shown in the figure. 4. It consists of a physical layer, MAC layer, Network layer and Application layer.

The physical layer, which control and communicate with the radio transceiver directly. It deals with all tasks related to the ZigBee hardware, which includes initialization, channel selection, link quality estimation, energy detection measurement and clear channel assessment. The MAC Layer provides an interface between physical layer and the network layer. This provides two services they are i) Data services ii) Management services like interfacing to the MAC sub Layer Management Entity (MLME) Service Access Point called (MLME-SAP). Network layer interfaces between the application layer and MAC Layer. This Layer is used for Routing and Network formation also it provides security for network and allows the devices to maximize their battery life. Another important layer is an Application layer which consists of four parts. They are Application Objects [16], ZigBee Device Object [17], Application Support Sub Layers and Security service provider.

3. CIRCUIT DESCRIPTION

The elevated digital voting machine built with ATmega16 Micro controller. In this Micro controller circuit port D was used for LCD display and port C.0 (pin 22) was used giving for voting power to an officer, LED and buzzer output uses Micro controller port C.5 and C.6. The LCD is also connected to port C.7 via a transistor. Initially, once the election commission officer power on the device and seals so that nobody can switch it off again.

After every voting it stores the counting result in Micro controller EEPROM. And also the details will be sent to central election commission data bas, by the ZigBee module interface with port A.0. This module is used for collecting all EVM's voters and counter details in the booth and this data will be sent send to the coordinator node for that district. From the coordinator node the data will move through the cloud network to the central election commission data base.

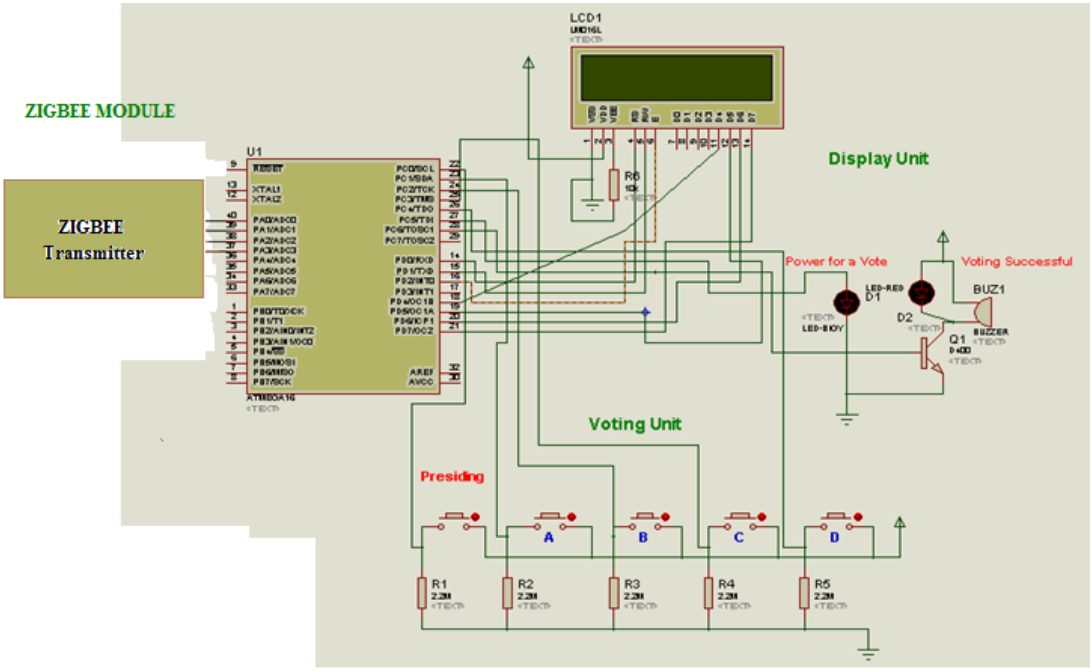

Fig. 5. EVM Circuit Diagram

Next the presiding officer verifies the voter's particulars to avoid the fake voter and press the voting power button, then the Micro controller starts scanning from pin 23 to pin 26 and glows LED until the voter press the candidatebuttons. When the voter presses the button beside his candidate symbol in the voting unit. A beep sound is produced instantly the LED indication is used to confirm the success of the voting process. Then the power goes down to avoid the possibility of voting twice or more.

Here the entire state result as booth wise as well as for all districts wise with the help of cloud computing network the result update in real time and can get the result on that day evening itself without any mentioned problems in early. After data get collected, then it needs to erase recorded data from EEPROM just broken the sealed on the power button and power of the system. Now we can use this system for the next election.

4. CLOUD COMPUTING

The cloud computing concept was introduced in 2007 by Google and IBM [18]. It is possible to realize cloud computing, due to the development of technologies and high-speed internet facilities. Many organizations around the world are providing cloud services, It is an internet- based model for enabling on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) [19]. In internet, cloud computing technology provides four major services such as: i) Software as a Service ii) Data Storage as a Service iii)

Platform as a Service and iv) Infrastructure as a Service [20]. Cloud service activities are upgraded or improved by the cloud service provider based on the customer needs. Our objective is to ensure security in the voting system and in the counting process by using cloud services over insecure internet. There are four types of deployment that a customer can establish such as: Private, Public, Community and Hybrid [21].

Public Cloud: Public cloud describes cloud computing in the traditional mainstream, where resources are equipped, self assessments over the internet via web applications or web services. Thus the cloud available to public through Internet, here the general provider bill with a fine-grained utility by computing basis.

Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns. The community cloud created with a similar group of customers with the same set of resource requirements.

Private Cloud: In private cloud the services and infrastructure are maintained on a private network. These clouds provide the supreme level of security and control, but the company need to purchase and maintain all the software and infrastructure to use it properly.

Hybrid Cloud: A hybrid cloud environment consisting of multiple internal and/or external providers, it will be typical for most enterprises. By Hybrid cloud services users may easily change over to public cloud services by this it possible to avoiding issues such as PCI compliance.

5. IMPLEMENTATION OF PRIVATE CLOUD

The private cloud is used in this proposed system for its benefits like speed and its flexibility. Based on their varying demands the recourses can be assigned for its application. The implementation of a private cloud to the proposed system was shown in the figure. 6. Metering and thus billing of this system is to be availed on a monthly basis or daily basis, even an hourly basis with great precision in the metering and billing cost. But the understanding of private cloud goes away from our virtualization.According to Gartner, a successful implementation of private cloud depends on the following,

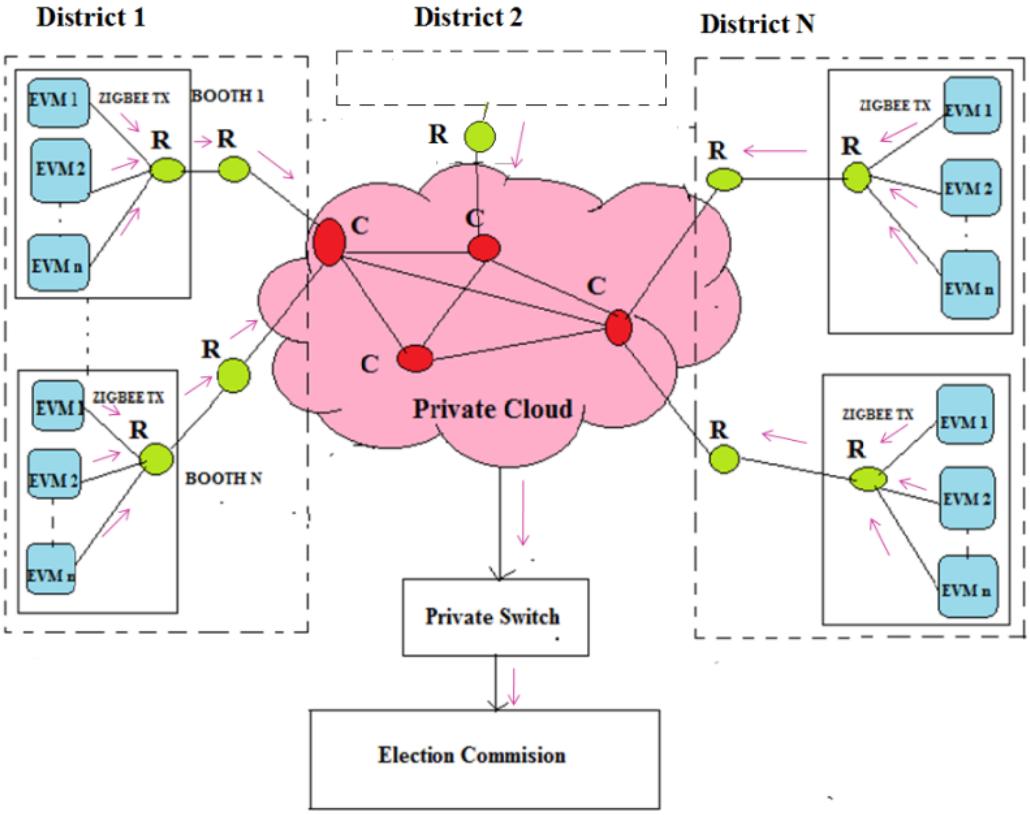

Fig.6.Implementation of EVM with Cloud

Service Management – The key factor of cloud Services which includes Management and automation.In every step, all actions need to be steady, retry-able and documented to keep a reliable platform. Every server needs to be perfect to get the expected results. Without a Service Management solution a cloud cannot offer any work.

Applications – The cloud solution depends on its quality of applications. The Applications must be handier from the cloud's provider management portal, but metering needs to be very flexible. When more resources are required the application also needs to be balanced.

Organization – The organization also need to be geared up for cloud technology similarly your organization will be shifting its emphasis from pure technology to more commerce solutions. Also the people need to adopt with cloud technology, else the technological solutions will fail.

6. SECURITY FRAMEWORK FOR EVM NETWORK

The architecture is designed in which a new security layer is designed for private

cloud. The new security framework is present in between session layer and transport layer such that it is transparent to the application layer and the lower layers, whenever a data is transferred by the EVM, it is first secured by certain authentication protocols and saved at the server end. With this, the data will be stored in a secured way at the server end. Those who want to download the data or view it should have access permission through the same framework to view the data. This is done in application (user) level so that the data will be secured and transferred when there is a need to disturb any lower layers of the network.

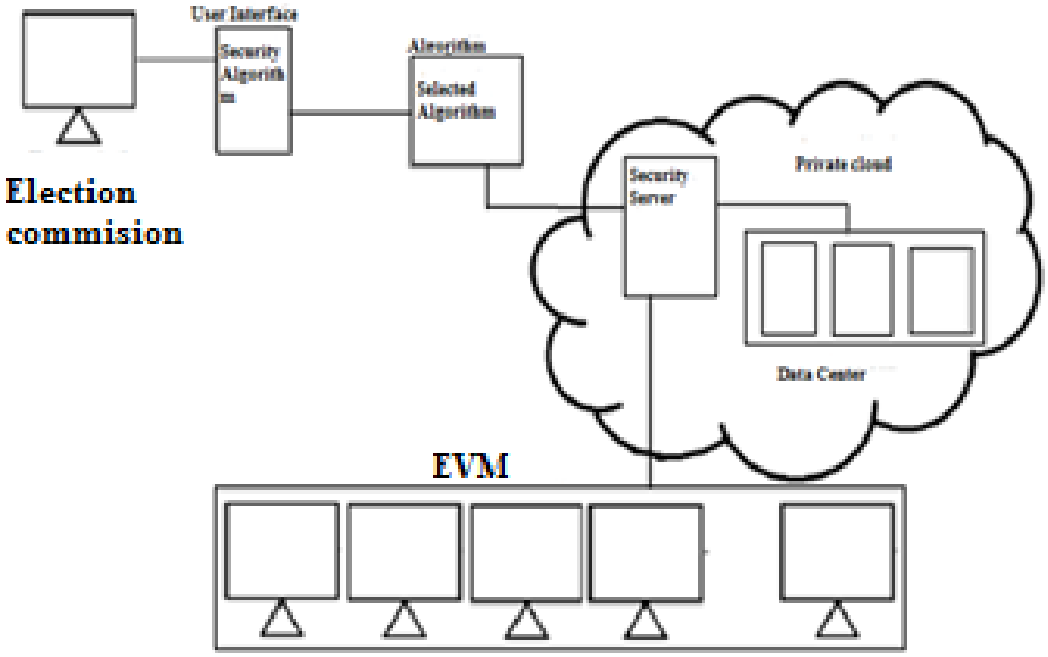

Fig.7. Security Framework model

6.1 Security Framework Model

The detailed design of the framework is in the below diagram figure. 7. The nodes which are linked to server will be connected to the security layer. The security server will secure the data and store it in a database. Here all the EVM's which belong to that network are connected to the same architecture. When the Election commission wishes to get any data from the booth center, it is required to be connected in the same server to get the original information. This helps to increase the security and privacy of the data.

6.2 Process at sender

The data at the EVM end will encrypt the data by selecting the appropriate approach from the interface and sends it to the server end.

As shown in the figure 8. Before sending the data into the server and the data will be encrypted in the socket layer for each byte and the encrypted data is sent. Here

the data is carried by the protocol to process, other commands which happens in a network.

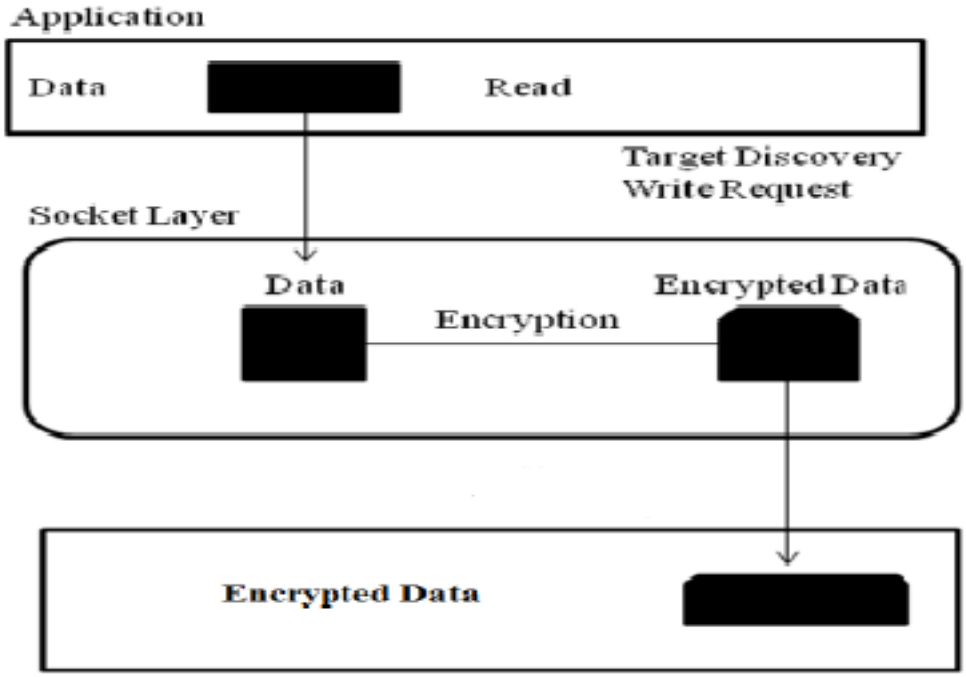

Fig.8. Encryption process at sender

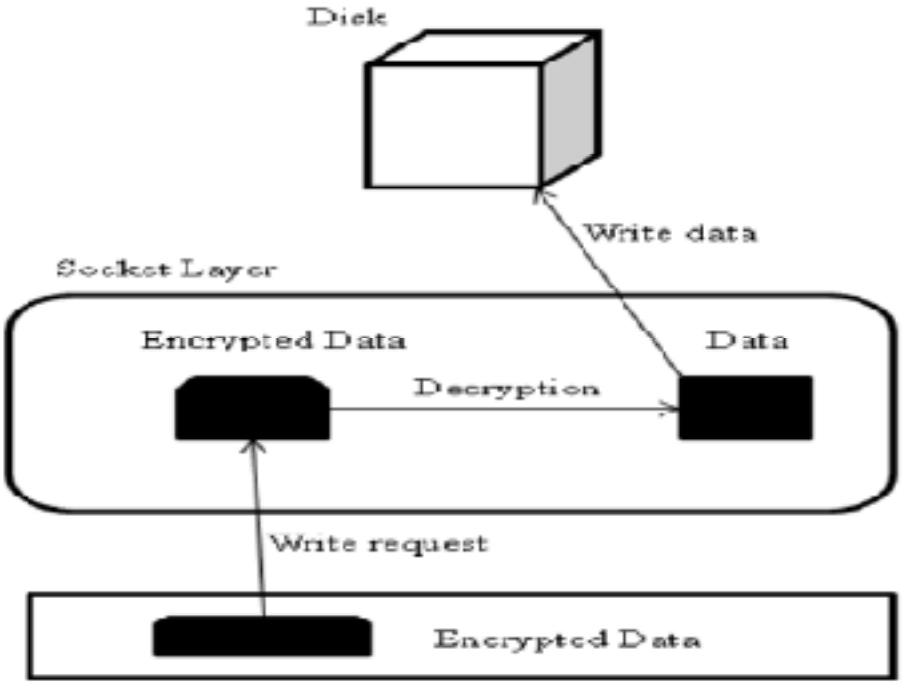

Fig.9. Decryption process at receiver

The data will be secured at the sender end by the security framework which helps secured data transfer.

6.3 Process at receiver end

At the receiver end (Election commission) when the data is received, the data will be decrypted by the security approach used at encryption end and it worked again above to the transport layer just where the packets arrived. As before the write request is given by the protocols, the security framework decrypts the data and saves on to the disk. Once the election commission makes a request for a file from the server the same security process will act as mentioned above. This ensures that the data is maintained confidential over the network and integrity in security checks at the receiver end.

7. CONCLUSION

In this proposed method cloud computing is introduced with the EVM to access the data instantly. The private cloud concept provides a new era in the voting system as the voting process can be monitored continuously without any malpractice and secured storage of data. ZigBee protocol provides an efficient way to interact with the server for transmitting the data. Thus we enter into a new era of voting system using this proposed EVM architecture. This system helps in raising the security, reliability and transparency, also to obtain the result within a short time and hence minimizes the expenses of the government.

REFERENCE

3. Wagner.Y. D, M. Bishop, T. Baker, B. D. Medeiros, G. Tyson, M. Shamos, and M. Burmester, 2007. “Software Review and Security Analysis of the ES&S I Votronic 8.0.1.2 Voting Machine Firmware,” Technical report, Security and Assurance in Information Technology Laboratory,
4. Kohno.T, A. Stubblefield, A. Rubin, and D. Wallach, 2004 “Analysis of an Electronic Voting System,” in Proc. of IEEE Symp. Security and Privacy, pp. 27-40.
5. Proebstel.E, S.Riddle, F.Hsu, J.Cummins, F. Oakley, T. Stanionis, and M. Bishop,2007 “An Analysis of the Hart Intercivic DAU eSlate,” in Proc. of Usenix/Accurate Electronic Voting Technology Workshop.
6. Molnar.D, T.Kohno, N. Sastry, and D.Wagner, 2006.“Tamper-Evident, History Independent, Subliminal -Free Data Structures on PROM Storage-or-

How to Store Ballots on a Voting Machine (Extended Abstract)," in Proc. of IEEE Symp. Security and Privacy, pp. 365-370.

7. Bethencourt.J, D. Boneh, and B. Waters,2007. "Cryptographic Methods for Storing Ballots on a Voting Machine," in Proc. of Network and Distributed System Security Symp.
8. Garera.S and A. Rubin, 2007. "An Independent Audit Framework for Software Dependent Voting Systems," in Proc. of ACM conf. Computer and Comm. Security, pp. 256-265.
9. J. Hall, "Improving the Security, Transparency and Efficiency of California's 1 Percent Manual Tally Procedures," in Proc. of Usenix/ Accurate Electronic Voting Technology Workshop, 2008.
10. K. Weldemariam and A. Villafiorita,2008 "Modeling and Analysis of Procedural Security in (e) Voting: The Trentino's Approach and Experiences," in Proc. of Usenix/Accurate Electronic Voting Technology Workshop.
11. R. Hite, 2007, "All Levels of Government are needed to Address Electronic Voting System Challenges," Technical report, GAO.
12. M. Gondree, P. Wheeler, and D. D. Figueiredo,2005 "A Critique of the 2002 FEC VSPT E-Voting Standards," Technical report, Univ. of California.
13. R. Mercuri. Voting System Guidelines Comments. [Online].2005 Available:http://www.wheresthepaper.org/VVSGComment.pdf.
14. Nisha Ashok Somani and Yask Patel May 2012 "Zigbee: A Low Power Wireless Technology For Industrial Applications" International Journal of Control Theory and Computer Modelling (IJCTCM) Vol.2, No.3, DOI : 10.5121/ijctcm.2012.2303 27
15. ZigBee Standards Organization, ZigBee Specification, January 2008. Document 053474r17.
16. D.Gislason, 2008, ZigBee Wireless Networking, Newnes.
17. Zhou Yiming, Yang Xianglong, Guo Xishan, Zhou Mingang, Wang Liren,2007." A Design of Greenhouse Monitoring & Control System Based on ZigBee Wireless Sensor Network",IEEE journa1-4244-1312- 5/07 2007
18. Dunfan Ye, Daoli Gong, Wei Wang.2009. "Application of Wireless Sensor Networks in Environmental Monitoring"2nd International Conference on Power Electronics and Intelligent Transportation System IEEE2009 pg 2563-2567
19. Xiuping Zhang; Guangjie Han; Changping Zhu; Yan Dou; Jianfeng Tao,2009." Research of Wireless Sensor Networks based on ZigBee for Miner Position", [J] International Symposium on Computer, Communication, Control and Automation, IEEE. 29 July 2010Pg1 – 5
20. Center Bo Wang, HongYu Xing, 2011. "The Application of Cloud Computing in Education Informatization, Modern Educational Tech..." Computer Science and Service System (CSSS), 2011 International Conference on IEEE, 27-29 June 2011, 978-1-4244-9762-1, pp 2673 – 2676.

21. NIST Definition http ://www.au. af.mil/au/awc/ awcgate /nist/cloud-def-v15.doc

22. Cloud Computing services & comparison http://www.thbs.com/pdfs/Comparison%20of%20Cloud%20computing%20services.pdf

23. Safiriyu Eludiora1, Olatunde Abiona2, Ayodeji Oluwatope1, Adeniran Oluwaranti1, Clement Onime3 and Lawrence Kehinde apered in Int. J. Communications, 2011. A User Identity Management Protocol for Cloud Computing Paradigm Network and System Sciences, 2011, 4, 152-163