SAFE, CLEAN AND UNBIASED ELECTIONS WITH ENCRYPTED QR CODE VOTER CARDS

Cheman Shaik

VISH Consulting Services Inc, 6242 N Hoyne Avenue, Chicago IL 60659, USA
cheman_shaik@rediffmail.com

ABSTRACT

The aim of this paper is to propose a novel approach to conducting safe, clean and unbiased elections by issuing Voter Cards with encrypted QR codes and including a new device called Voter Card Processor (VCAP) for verifying the issued voter cards at polling stations during elections. Detailed descriptions are provided of how to generate encrypted QR code voter cards, and how the VCAP functions in detecting fraudulent voter cards and repeat voters. This approach enables polling officers to automatically verify forgery of voter cards, identify and stop repeat voters, and also prevent rigging and compromised voting that could be possible due to corruption, bribery, intimidation and muscle power.

KEYWORDS

Cryptography, Encryption, Decryption, encrypted QR Code, Mobile App, EVM, Control Unit, Ballot Unit, VVPAT, Voter Card Processor,

1. INTRODUCTION

Democracy is a system of government practiced by more than half of the world countries today. In democracy government is elected by people through elections for a tenure decided by their constitution. Free and fair elections are the foundation of any successful and healthy democracy.

Every democratic government spends millions to billions of Dollars on elections depending on the country's population size. Such a high-priced democracy is really worth only if the election is conducted in a safe, clean and unbiased environment. The electoral process is slowly evolving from ballot box to EVMs (Electronic Voting Machines). Presently, twenty countries of the world are using EVMs for elections, India being one of them doing it since 2014 for their *Lok Sabha* elections.

The replacement of ballot box by EVM has saved ample of time in counting votes and tons of paper wasted in printing paper ballots. Moreover, EVM has prevented many malpractices booth capturing with muscle power. Despite these advantages the credibility of EVMs is questioned and criticized on grounds of hacking and tampering, though none of the allegations were proved technically [1].

As the election commission claims, EVMs may not be vulnerable to hacks and tamper. However, they are not resistant to compromised voting because ballot issuance to voters is in the control of the polling officer. Any bias or favoritism of the officer towards a particular political party or contesting candidate may result in compromised voting, thereby altering the poll result. Other reasons for compromised voting could be bribery, pressure, intimidation and muscle power.

Much more research needs to be conducted to improve the electronic voting machinery and the embedded software of the machinery. Also new security methods need to be developed and implemented in the machinery to rule out he chances of compromised voting.

Paper Outline: Section 2 explores the existing literature and cites related work done in the past. Section 3 explains the basics of public key cryptography, its application in secure communication and how it works. Section 4 discusses QR codes, types of data that they can encode and their various purposes. Section 5 discusses the existing EVM setup currently deployed in polling stations during elections in India. Section 6 explains in detail how cryptography and QR codes can be applied on voter cards to facilitate clean, safe and unbiased elections. Section 7 discusses how forged voter cards can be detected using encrypted QR code voter cards and VCAP device. Section 8 discusses how repeat voters can be identified by verifying voter details in VCAP memory. Section 9 discusses how voter information can be encrypted and encodes in QR code. Section 10 discusses how voter information can be decrypted and decoded from QR code. Section 11 discusses cross verification of voter with an OTP from election commissions OTP service. Section 12 compares QR code and blockchain technologies and recommends QR code due to their simplicity and ease of implementation. Section 12 provides conclusion of this research paper.

2. LITERATURE SURVEY

Many democratic countries of the world are using electronic voting machinery in their elections to record and count votes. The voting equipment includes different components such as Optical/Digital Scanner, Direct-Recording Electronic (DRE) Voting Machine and Ballot Marking Device (BMD) [2].

Though there were no reports of compromised elections due to the use of DREs, several research studies demonstrated that at least in theory DREs are vulnerable as they rely purely on a computer for casting and recording votes in a single machine through its software. A hidden malicious code or malware installed on the computer can record a different vote from the one a voter casts and sees in the VVPAT connected to the voting machine, finally altering the poll result [3].

In 2007, Feldman et al conducted a security analysis of certain voting machines uncovering several ways that malicious code could compromise election security [4], following which several states in the US conducted individual security evaluation of their election technology.

In India, the election commission uses three electronic components, a EVM control unit, a ballot unit and a VVPAT to facilitate their voting process. The control unit allows the polling officer to release a ballot to the voter to cast his vote while the ballot unit allows voters to cast their votes. The VVPAT component provides a physical evidence to the voter that his vote was cast to his desired electoral candidate [5].

In 2010, Scott et al conducted a security analysis of India's EVMs and disclosed that the machines are vulnerable to hardware tampering attacks by replacing some of their parts with malicious look-alike components. They also clarified that the attacks were possible due to the lack of cryptographic protection of the vote data stored in the machines [6].

In 2016, Soumyajit et al proposed a Biometric Voting System (BVS) which will access the data stored in the database of Aadhar card, an identity issued by the Government of India, while casting their votes. Integrated with a biometric fingerprint machine, the BVS collects voter's

fingerprints and compares them with the ones stored in the Aadhar card database voter authentication. This approach to voter authentication sounds good, however, it requires internet connection in polling stations to connect the Aadhar Card database and may hamper or completely stop the polling process if the net connection is slow or down [7].

In 2019, Krishna et al proposed a method of storing the vote data in a decentralized network and securing the data using a security mechanism derived from the blockchain framework. The vote data is shared among all the devices in the network and peer to peer verification is done to verify the authenticity of the vote data [8].

In 2020, Akhil Shah et al proposed a blockchain based online voting system wherein voter can register themselves and cast their vote. Security is provided through authentication and authorization. The online voting web application counts votes and percentage of votes cast for each contestant [9]. However, blockchain is a too complicate and costly a technology to deploy in polling stations for voter verification. It also hampers voting process as it requires internet connections that may not be sufficient and stable during elections.

3. PUBLIC KEY CRYPTOGRAPHY

Public key cryptography depends on two keys, a public key and a private key, to secure communication over an unsecured channel. The plaintext information that needs to be communicated is encrypted using the public key to generate a ciphertext which is communicated to the intended receiver. The receiver will decrypt the ciphertext using the private key, which is always kept secret, to derive the plaintext information.

The two keys are generated by performing certain rigorous computations subject to an equation underlying the cryptographic algorithm used. RSA and ECC are the two well known and tested public key cryptosystems in the industry. Both the cryptosystems use discrete mathematics for key computation, encryption and decryption. While RSA uses exponential modular arithmetic operations, ECC uses discrete point additions on an elliptic curve for encryption and decryption.

Information encrypted by one key can be decrypted only by the other key, without which decryption is nearly impossible with today's processing power of computers. Compromise of the private key will expose communication to hackers and eavesdroppers intercepting the messages in the middle.

4. QR CODES

QR code is a two-dimensional matrix of black modules placed over a white background. It can encode much more data compared to the one-dimensional barcodes that we see on products we shop in our daily life. It can encode different types of data such as byte, numeric, alphanumeric, Chinese, Japanese and Korean characters. The amount of data that can be encoded depends on the type of characters.

In the last few years QR codes have become more and more popular and are used for different purposes such as encoding business cards, product details, connecting a viewer to a website or social media profile, sharing a location on Google Maps and so on. Another interesting capability of QR code is it is tolerant to partial damage and can be read even when a part of it is torn or damaged.

A thick white border surrounding the QR code differentiates it from the surrounding background images. Every QR code consists of three position markers placed at the top left, top right and bottom left corners to guide the scanning camera to locate the data modules and identify the scanning direction.

5. EXISTING EVM SETUP DEPLOYED IN CURRENT ELECTIONS

The electronic machinery used today in India for elections includes a main EVM control unit, a ballot unit and a Voter Verified Paper Audit Trial (VVPAT) unit as shown in figure 1. The control unit is connected to the VVPAT unit with a five-meter chord.

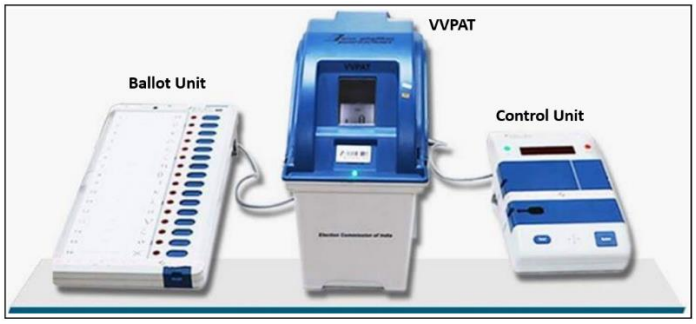


Figure 1. An electronic voting machinery setup in a polling station

The ballot unit is used by voters to cast their votes while the VVPAT generates printed paper records of voter ballots to ensure the voter that his vote was cast properly to his desired candidate. During voting the control unit is operated by one of the polling officers to release a ballot for each voter by pressing the Ballot button.

As the ballot issuance to voters is in the control of prolling officer, miscreants can take control of the control unit by overpowering the polling station, or there could be a possibility of compromised voting through bribery or favoritism towards a particular political party or electoral candidate.

6. APPLYING CRYPTOGRAPHY AND QR CODES ON VOTER CARDS

In this section we present a novel method of verifying voters at a polling station and allowing them to vote for their chosen party. Implementation of the method requires that the election commission obtain a cryptographic key pair of any public key cryptosystem and securely save their private key. Further, the election commission is required to create a special QR code scanning mobile app and place it on their website for download by voters. The election commission's public key should be stored in the scanning app memory.

The election commission also needs to include an additional device called Voter Card Processor (VCAP) in their EVM setup of polling stations. The VCAP device should store the election commission's public key in its memory. The purpose of the VCAP device is to scan the QR code on voter card, decrypt the ciphertext encoded in the QR code and display the voter details on the monitor connected to the device. The VCAP device also stores the voter card information in its memory.

When the same voter attempts to cast his vote second time at the polling station with a fake/prosthetic finger hiding the indelible ink mark made during his first vote, the VCAP will

raise an alert as his details are already stored in its memory. The same alert is raised when a different person with similar facial appearance presents the same voter card at the polling station.

The VCAP device is also connected to the EVM control unit and sends a signal to it to release a ballot to enable the voter to cast his vote, without requiring the polling officer to press the Ballot button. So compromised voting to cast duplicate or redundant votes is not possible even if the pooling officers and party agents join hands. It also prevents unlawful vote casting by taking control of the poll station through intimidation or muscle power. Figure 2 below shows a VCAP connected to the control unit.

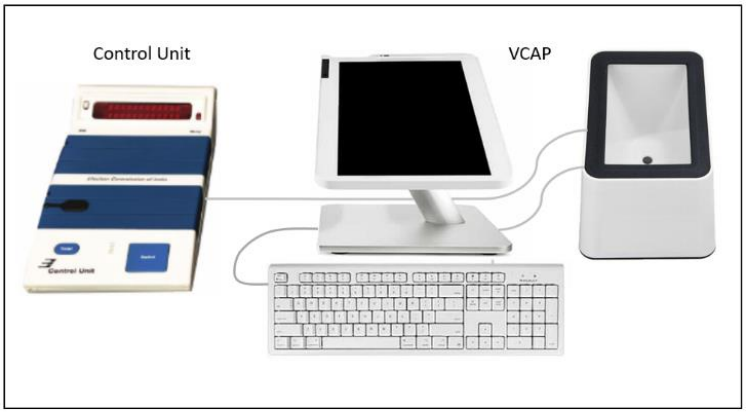
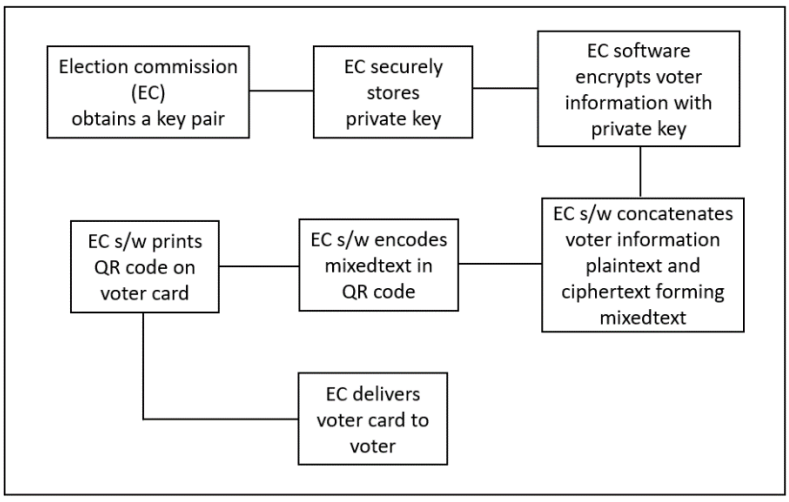


Figure 2. A VCAP integrated with EVM control unit

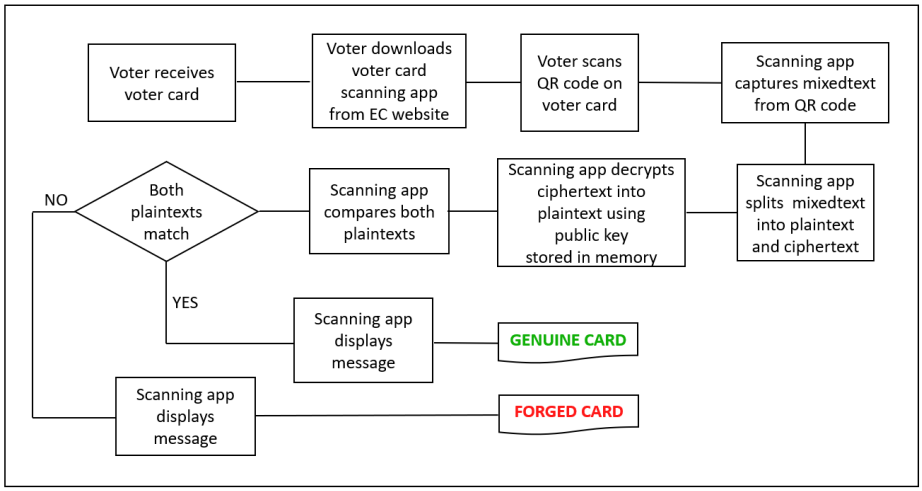
The election commission's voter card generation and printing software application should be enhanced to incorporate a QR code on voter cards. When the election commission issues a voter card, the software application should encrypt the voter information such as the voter card id, name, father's name, sex and date of birth using the private key and generate a ciphertext. A mixedtext should be formed by appending the ciphertext to the plaintext followed by a separator string such as '**' or '##' in order to differentiate the ciphertext from plaintext. A QR code should be generated encoding the mixedtext and printed on the voter card to be issued. Flowchart 1 below describes the process of voter card printing by election commission.



Flowchart 1. Voter card printing by election commission

When a voter receives his voter card, he or she can download the QR code scan app from the election commission's website on their mobile phone and scan the QR code, which will retrieve

the election commission's public key from its memory, capture the mixedtext from the QR code, extract the ciphertext from it, decrypt it and compare it with the plaintext. If there is a mismatch of any field, the app will display an alert message 'FORGED CARD'. If all the fields match exactly, the app will display a message "GENUINE CARD' along with the details of the voter. This confirms that no forging was attempted on the QR code. The voter also needs to verify the displayed information with the actual information printed on the voter card. A perfect match with all the fields printed on the voter card indicates that no forging was attempted on the printed information on the voter card. Flowchart 2 below describes the process of voter card verification by voter.



Flowchart 2. Voter card verification by voter using election commission's scanning app

Similarly, when a voter reaches a polling station and presents his voter card to the polling officer, the polling officer will place it on the Voter Card Processor (VCAP) scanning screen. Figure 3 below shows a polling officer's desk and the polling booth wherein the control unit on the officer's desk is connected to the VVPAT in the polling booth.

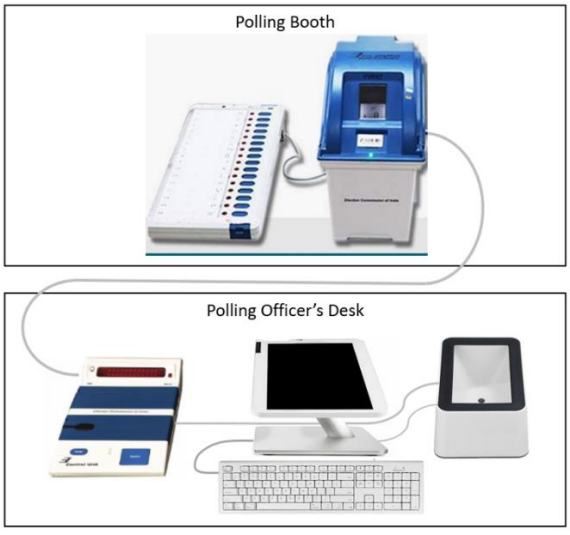


Figure 3. A control unit connected to VCAP and VVPAT

Figure 4 below shows a voter card issued by the election commission which the voter needs to present at the polling station he is referred to vote at. One of the polling officers checks the voter details in the electoral roll after which he will mark the voter's forefinger with indelible ink to

prevent him from repeat voting. Subsequently, the polling officer in-charge of the control unit will press the ballot button on it to release a ballot so the voter can cast his vote in the polling booth by pressing the button on the ballot unit against his contesting candidate's name.

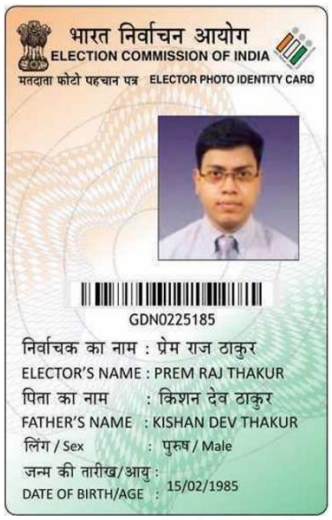


Figure 4. An original voter card

The proposed EMV setup includes the additional VCAP system which is connected to the control unit on the polling officers desk. The VCAP unit consists of a scanner device with a QR code scanning software loaded and sufficient memory to store voter details. It also stores public key of the election commission in its memory.

Figure 5 shows a voter card issued consisting a QR code encoding the voter's plaintext information plus the ciphertext generated by encrypting the plainetx information with the election commission's private key.

Figure 5. An original voter card with encrypted QR code

When the polling officer places the voter card on the VCAP scanner as shown in figure 6, its software will scan the QR code, capture the mixedtext encoded in it, separate it into the plaintext

and ciphertext. Further, the software will decrypt the ciphertext using the election commission's public key stored in memory and compare the plaintext with the plaintext in the QR code. If both values match exactly, it will display a message 'GENUINE CARD' on the monitor. This conifrms that no forgery is attemped on the QR code. When the polling officer presses the page down arrow key on the keyboard, it will display the information in the plaintext captured from the QR code. The officer should the check this information with that printed on the voter card. Any mismatch is a clear indication of forgery of the printed information on the card and the polling officer should prevent the voter from casting vote.

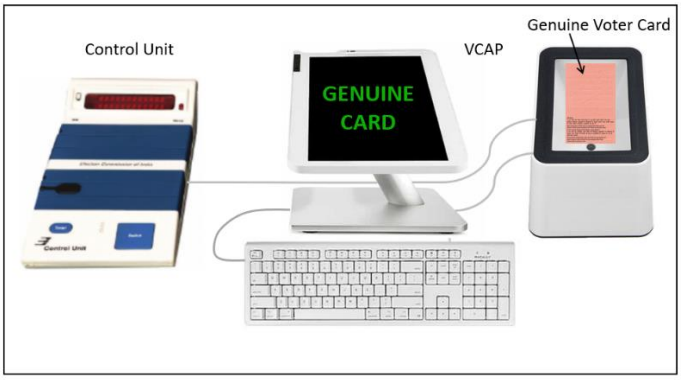


Figure 6. An original voter card scan and process result seen on VCAP monitor

On the other hand, if both informations match, the polling officer will press the ENTER key to proceed further which will send a signal to the VCAP device software. Subsequently, the software will store the voter card details in VCAP memory and send a signal to the control unit to release ballot so the voter can get into the polling booth and cast his vote, without requiring the officer to press the Ballot button. In the new control units that will be connected to the VCAP device, the Ballot button will have no funtion and it will be either disabled or removed completely.

Table 1 below shows the voter information obtained on decrypting the ciphertext in the QR code and the plaintext voter information encoded in the same QR code. As the QR code is not forged both the texts are identical.

Table 1. Voter information encoded in plaintext and ciphertext of QR code

Voter Information Obtained on Decrypting Ciphertext in QR Code	**Plaintext Voter Information Encoded in QR Code**
GDN0225185, PREM RAJ THAKUR, KISHAN DEV THAKUR, Male, 15/02/1985	GDN0225185, PREM RAJ THAKUR, KISHAN DEV THAKUR, Male, 15/02/1985

7. FORGED VOTER CARD DETECTION

Figure 7 below shows the same voter card shown in figure 5 forged to change the voter name. The forger also changed the name in the plaintext encoded in the QR code on the voter card. When the fraudulent voter presents the voter card to a polling officer, he will place the card on the VACP device scan surface following which the VCAP software will capture the mixedtext encoded in in the QR code, split it into the plaintext and ciphertext. It further decrypts the ciphertext with the public key of the election commission already stored in memory and compares it with the plaintext. As the plaintext in the QR code mismatches with the plaintext resulting from the decryption of ciphertext, the software will display the 'FORGED CARD'

message on the monitor. Consequently, it will not issue any signal to the control unit to issue Ballot even after pressing the *Enter* key. Even the polling officer or the fraudulent voter can not override this control, thereby preventing compromised voting.

Figure 7. An forged voter card with encrypted QR code

Table 1 below shows the voter information obtained on decrypting the ciphertext in the QR code and the plaintext voter information encoded in the same QR code. As the QR code is foreged to modify the voter's first name the plaintext information differs from the one obtained on decrypting the ciphertext. Consequently, VACP software will display the alert message 'FORGED CARD' as shown in figure 8, and no signal will be sent to the control unit to issue ballot for the fradulent voter.

Table 2. Voter information encoded in plaintext and ciphertext of QR code

Voter Information Derived on Decrypting Ciphertext in QR Code	**Plaintext Voter Information Encoded in QR Code**
GDN0225185, **PREM** RAJ THAKUR, KISHAN DEV THAKUR, Male, 15/02/1985	GDN0225185, **GIRI** RAJ THAKUR, KISHAN DEV THAKUR, Male, 15/02/1985

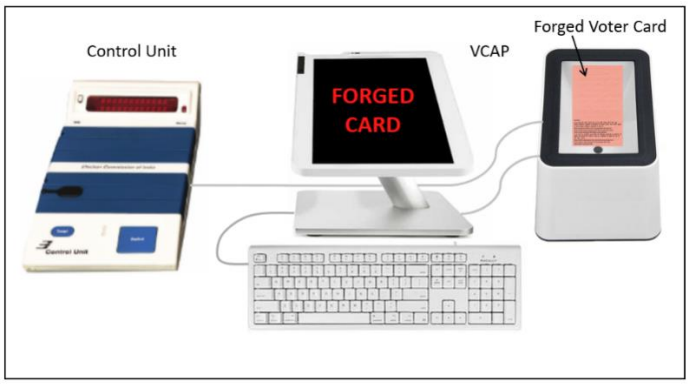


Figure 8. A forged voter card scan and process result seen on terminal

In order to modify the ciphertext in the QR code to exactly match the forged text, the forger needs to have the private key of the election commission which is not possible as it is stored securely by them with stringent security measures. Alternatively, if the forger encrypts the forged

information with his own private key, its decryption by the VCAP software will produce junk text totally mismatching the forged information because the forger's private key and the election commission's public key stored in the VACP memory are not mathematically related to produce the desired decryption for the forger. This will again alert the polling officer with the message 'FORGED CARD' as shown in figure 8.

8. REPEAT VOTER DETECTION

When a voter appears for the second time at the polling station with erased indelible ink or prosthetic cap on his fore finger and presents his voter card to the polling officer, he will place it on the VCAP scanner surface which will make the software scan the QR code, extract the ciphertext encoded in it, decrypt it with the public key stored in memory and derives the plaintext voter information. The software will further check the VCAP memory for the voter information. As it is already stored during his first voting session, it will display the alert message 'REPEAT VOTER' on the polling officer's VACP monitor as shown in figure 9.

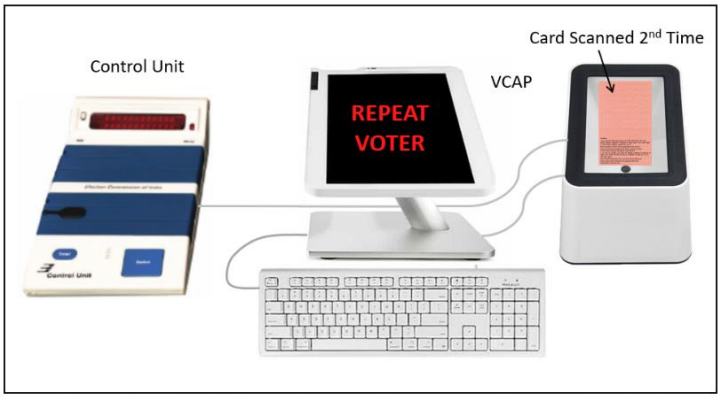
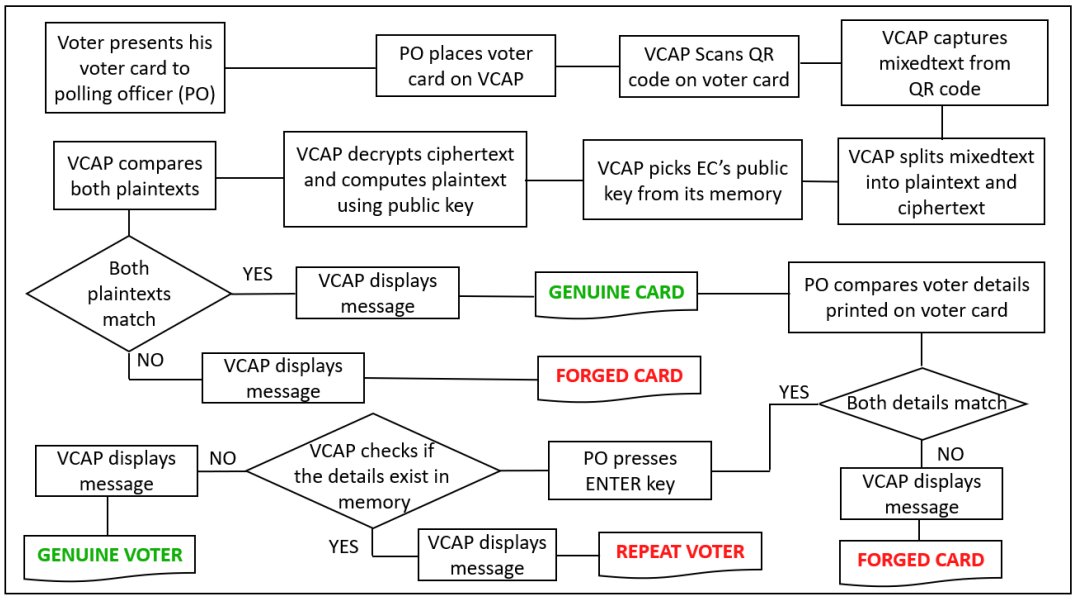


Figure 9. A forged voter card scan and process result seen on terminal

Flowchart 3 below describes the process of voter card verification by polling officer before a voter is allowed to vote.



Flowchart 3. Voter card verification by polling officer using VCAP at polling station

9. VOTER INFORMATION ENCODING IN QR CODE

Voter information can be encrypted using any tested, industry standard public key cryptosystem such as RSA and ECC. The current standard key length of RSA key is 2048 bits.

Assuming the following notions for the plaintext and ciphertext voter information and cryptographic key of the election commission,

M = Voter information in plaintext
C = Encrypted voter information (ciphertext)
X = Mixed string of plaintext M and ciphertext C
e = RSA private key exponent of the election commission. Must be kept secret.
d = RSA public key exponent of the election commission
n = RSA key modulus which is common on both sides

The election commission's voter card software application will compute the ciphertext C and form the mixed string X as follows:

$C = M^e \bmod n$
X = M##C where ## is the separator string to differentiate M and C

The software application will encode X in a QR code and prints the QR code on the voter card.

10. VOTER INFORMATION DECODING FROM QR CODE

When the QR code on the voter card is scanned by the voter using the election commission's mobile app or by the polling officer's VCAP unit software, the following steps will take place:

- The software of the mobile app or VACP extracts X from the QR code
- Splits X into M and C
- Decrypts C into M_d using the relation $M_d = C^d \bmod n$
- Compares M and M_d.
- If M == M_d, the software displays the message 'GENUINE CARD' on VCAP monitor or voter's mobile phone
  Else it displays the message 'FORGED CARD' on VCAP monitor or voter's mobile phone

11. CROSS VERIFICATION WITH OTP

Cross verification with a One-Time Password (OTP) can also be added as an additional step of the voter card verification process. However, it should be made only an optional requirement as it can hamper the voter card verification process if the voter's cellular network is down or jammed.

The election commission need to have an OTP service deployed with a dedicated number where the scanning application on the voter's mobile phone will send a text message to which the OTP service will send an OTP. The voter needs to share the OTP with the polling officer which will be stored in the VCAP device memory.

12. ENCRYPTED QR CODES VS BLOCKCHAIN

Blockchain technology will not be suitable for voter information verification during polling as it needs internet connection to connect to the blockchain. Network bandwidth issues and failure of the internet connection during polling will seriously hamper or completely stop the polling process. On the other hand, encrypted QR codes work quickly and facilitate continuous progress of the polling process.

13. CONCLUSION

Clean and fair elections conducted in very unbiased environment is a paramount requirement for the function of a healthy and successful democracy. The advent of EVM has made the counting process faster. However, even with EVMs compromised voting is still possible due to reasons such as corruption, bribery, intimidation and biased favoritism of polling officers towards any political party.

In this paper we presented a novel method of preventing compromised voting by issuing voter cards with encrypted QR codes and including a new device called Voter Card Processor (VCAP) in the electronic machinery setup of polling stations. The method requires that the election commission obtain a cryptographic key pair and store the private key securely and use it in their voter card printing software application. The application should encrypt the voter card information with the private key, encode both the plaintext and ciphertext in a QR code and print the QR code on the voter card to be issued.

Further, the election commission should develop and publish their voter card scanning application on their website for download by voters on their mobile phones. The application should also be deployed on the VCAP device. The election commission's public key should be stored in the VCAP device memory.

When a voter receives his voter card, he can download the scanning app from the election commission's website and scan the QR code on his voter card, which will capture the text encoded in it, separate the plaintext and ciphertext, decrypt the ciphertext with the public key stored in the app memory and compare the result with the plaintext. Any mismatch between the two will raise an alert message that the card is forged. The method can also detect repeat voters by storing the voter information in the VCAP memory and checking the memory when a voter card is presented to the polling officer.

The proposed method prevents compromised voting by removing the ballot issuing control from the polling officer and vesting it technically in the VCAP device.

DISCLAIMER

The voter card shown in this paper is not a real one but obtained from Google search and used only for the purpose of illustration.

REFERENCES

[1] Mbauniverse.com, "EVMs Vs Paper Ballots: Which one is Better to Use?", https://www.mbauniverse.com/group-discussion/topic/current-affairs/evms-vs-paper-ballots

[2] NCSL, "Voting Equipment", https://www.ncsl.org/research/elections-and-campaigns/voting-equipment.aspx

[3] EvA. J. Feldman, J. A. Halderman, and E. W. Felten. Security analysis of the Diebold AccuVote-TS voting machine. In Proc. EVT, Boston, MA, Aug. 2007

[5 ceodelhi.gov.in/, "Electronic Voting Machines and VVPAT", http://ceodelhi.gov.in/eLearningv2/admin/HindiPDF/EVM.pdfScott Wolchok et al, "Security analysis of India's electronic voting machines", CCS '10: 17th ACM Conference on Computer and Communications Security 2010 Chicago Illinois USA October, 2010

[6] Soumyajit Chakraborty, Siddhartha Mukherjee, Bhaswati Sadhukhan and Kazi Tanvi Yasmin, "Biometric Voting System using Adhar Card in India", International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 4, April 2016

[7] S. B, R. T. V, N. Krishna M P, B. R. J, S. Arvindh M and D. M. Alagappan, "Secured Electronic Voting System Using the Concepts of Blockchain," 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2019.

[8] Akhil Shah, Nishita Sodhia, Shruti Saha, Soumi Banerjee and Madhuri Chavan, "Blockchain Enabled Online-Voting System", ITM Web of Conferences 32, 03018 ICACC-2020

AUTHOR

Cheman Shaik is a Research & Development professional in Computer Science and Information Technology for the last twenty years. He has been an inventor in these areas of technology with eight U.S Patents for his inventions in Cryptography, Password Security, Codeless Dynamic Websites, Text Generation in Foreign Languages, Anti-phishing Techniques and 3D Mouse for Computers. He is the pioneer of the Absolute Public Key Cryptography in 1999. He is well known for his Password Self Encryption Method which has earned him three U.S Patents. He has published research papers in the international journals – IJCSEA, IJCIS, IJNSA, ACIJ, CSEIJ and the proceedings of EC2ND 2006 and CSC 2008.