Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 4– No.3, January 2016 – www.caeaccess.org

Implementation of Advance Encryption Standard (AES) in Biometric Electronic Voting Software

M. O. Yinyeh
University for Development Studies
Faculty of Mathematical Sciences
Department of Computer Science

David Sanka Laar
University for Development Studies
Faculty of Mathematical Sciences
Department of Computer Science

ABSTRACT
This paper describes the development and implementation of a Voting software that makes use of the Advance Encryption Standard (AES), to encrypt all votes cast in a biometric verifiable election system. The software allows votes that are cast to be sent and tallied safely. The software allows the voter to cast their ballot by clicking or selecting few buttons, making voting seamlessly.

The software is composed of a two applications, the Server application and the Client application, the Client application basically encrypts the votes cast by the voter whiles the Sever application decrypts the encrypted votes, tally votes and manages Election related data and procedures. The biometric identification module enrolls qualified voters and verifiers them on Election Day reducing or eliminating the possibility of multiple registration and voting. The AES module prevents the possibility of manipulating a voter's intent and thwarting malicious people from tampering of the elections results. The software was developed using C# .Net for the front end of the software and Microsoft SQL Server 2012 database at the back end. The software can be used for all public elections for choosing leaders and to inform decision making process.

Keywords
Biometric, Electronic Voting, AES, Encryption, Software and Secure.

1. INTRODUCTION
Voting to select leaders in a country and indeed any organization or group is the ultimate measure of how democratic such an organization or country is. Traditionally, elections serve as an official mechanism for citizens of a geographical area or members of an organization to express their views or more importantly choose a new leader.

The traditional voting system is paper based, that is, the voting process requires the voter to mark his candidate of choice with his thumb print (or other means) on a ballot paper which is then dropped in a ballot box. After the voting process the ballot box is then opened, the ballot papers sorted, counted and the victor is announced after wards. This simple method of voting however has many challenges like error during counting, unregistered voting, over voting, multiple voting and many more. It's then necessary to ensure that elections are accurate and reflect the true views of the voter.

Even though there have been recent electronic and software approaches to solving the problems associated with the Traditional Voting system, Ghana and most African countries still make use of the traditional voting system. This system has often led to court cases and disputes, a good example being the 2012 Ghanaian Presidential and Parliamentary Election. Reuters in a news article stated this about the election "Ghana's electoral authorities said on Sunday incumbent front-runner, John Dramani Mahama won a new term as president of Ghana, in the West African state in an election the opposition claimed was marred by tinkering." [12], as a result the New Patriotic Party (NPP) petitioned the Ghanaian Supreme Court, the case was however dismissed by the Supreme Court.

With the advent of modern cryptosystems and advancement in computer power and networks, the proposed system combines the speed, stability and security the modern computer system provides. The Voting software will provide dynamic capabilities that will make voting easy and fast as well as accurate by implementing procedures or algorithms that allow fast processing of information.

2. RELATED LITERATURE
2.1 Introduction
Advancement in Computer hardware and software has brought many important changes in the lives of people. As a result there exits new technologies in software and networking industry that can be merged together to form a voting software that is fast, robust and more importantly secure.

2.2 Electronic Voting
Wikipedia defines Electronic voting (also known as e-voting) as voting using electronic systems to aid casting and counting votes [2].

There is a wide range of Electronic voting technologies some of which include punched cards, optical scan voting systems, and specialized voting kiosks. Some of these systems have modules which handle transmission of ballots and votes using Computer software via telephones, secluded computer networks/systems, or the Internet. Electronic Voting system do not make use of only computer systems, there are also mixed systems that include an electronic ballot marking device or other assistive technology to print a voter verified paper audit trail which the uses a separate machine for electronic tabulation.

Electronic voting however can be generalized or categorized into two groups;

i. Electronic voting which is physically supervised by either governmental or independent electoral authorities (voting occurs at dedicated polling stations).

ii. Electronic voting which is performed without supervision, this is done remotely within the voter's

sole influence, and is not physically supervised by representatives of governmental authorities or independent electoral authorities (voting occurs on one's personal computer, mobile phone, television via the internet).

Electronic voting systems have been in use since the 1960, however its first official use was in the form of a lever type voting machine, known then as the "Myers Automatic Booth," which occurred in Lockport, New York in 1892. Four years later, they were used on a large scale in the city of Rochester, New York. By 1930, these lever machines had been installed in virtually every major city in the United States, and by the 1960's well more than half of the country's votes were being cast on these machines.

Conventionally five different types of voting systems may be identified. These are:

- **Paper-based electronic voting system**

These systems record, count, and produce a well-organized form of the vote count from votes that are cast on paper cards or sheets. Now these systems allow voters to make their selections by means of electronic input devices like touch screens. Voter selections are, however, not independently recorded, stored or tabulated by such input devices. [4].

- **Direct-recording electronic (DRE) voting system**

They record votes by means of a ballot display provided with mechanical or electronic optical components which could be triggered by the voter. Such equipment's record voting data and ballot images in computer memory components. Also, data computation and organization is achieved by the use of computer programs. [4].

- **Public network DRE voting system**

These systems are similar to the DRE voting systems, however they transmit vote data from the polling stations to other locations through a secure public network. The votes may be transmitted as individual ballots as they are cast, or occasionally as batches of ballots, or as one single batch, at the end of polls [4].

- **Precinct count voting systems (PCVS):**

They put the ballots in a tabular form at a particular place, say, a polling station. They offer mechanisms that accumulate and store vote count electronically and transmit the results to a central location over public network [4].

- **Central count voting systems (CCVS):**

They collate and tabulate ballots from multiple precincts or voting centers at a central location. Voted ballots are safely stored temporarily at the polling center. These ballots are then transported or transmitted to a central counting location and produce printed reports on the vote count [4].

Brazil successfully implemented Electronic voting systems in the form of DRE voting systems in May 1996, where over 400 electronic voting machines were distributed across the country, enabling citizens from more than 50 different municipalities to participate in Brazil's first computerized elections, which were held in October that year. In 2005, the Brazilian Electoral Justice added the digital identification project, which aimed at improving computerized elections. The project was further enhanced and implemented by the various administrations that followed [11].

2.3 General Features of an Electronic Voting Machine

Generally, electronic voting systems have many complex internal functions, some including encryption, randomization, communication and security systems. However for a general view of the features of Electronic Voting systems it is necessary to consider the following list of some of the functionalities that such systems can provide to both voters and election officials. Generally, electronic voting systems includes one of more of the features listed below.

1. It should have an Electronic list of voters and candidates, hence providing a means of authenticating legible votes and also record valid votes.
2. It should include Poll worker interfaces. These interfaces allow special functionalities that are only available to electoral workers, for example, resetting the vote count at the opening of the polling station, closing voting, printing and transmission of results.
3. It should have an interface for casting votes. These include touch screens, optical mark recognition (OMR) ballot papers that are fed into a scanner, touch-sensitive tablets, push buttons, online pages or special voting software for Internet voting.
4. Inclusion of special interfaces for handicapped voters. These include Braille ballot or audio input ballot devices for the blind, easier access for voters with physical disabilities, and simpler interfaces for illiterate voters.
5. Interfaces for the results output. This is often a printer or digital display. Once voting is closed this interface can be used to display or print the results that were recorded by the voting machine.
6. Result transmission system. Here voting machines can transmit results to central counting systems, this can be done via the Internet, telephone, mobile phone or satellite connection or through a dedicated Network. However in the absence of communication links, the results can also be transported physically, using electronic storage media such as memory cards.
7. Result tabulation systems, these systems receive electronic results from polling stations and automatically tabulate the results for the various districts or polling centers.
8. Result publication systems. Initial and final results can be circulated in many different ways including but not limited to websites, CDs, and geographic visualization structures and if possible on all levels of detail down to every polling stations. The more detailed the published results are, the more transparent the election.
9. Confirmation code systems. Some e-voting solutions allow for verification codes that allow voters to verify each vote by the relevant voter (International IDEA, 2011).

2.4 Cryptographic Elements

Security is paramount when dealing with electronic voting systems, hence when one thinks about security, data encryption and decryption comes to mind. In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. It must be noted that Encryption does not of itself prevent interception, it however denies the message content to the interceptor. In an encryption scheme, the message or information, referred to as plaintext, is encoded using an encryption algorithm, generating cipher text that can only be read if decrypted. Encryption schemes usually uses a pseudo-random encryption key generated by an algorithm. An authorized person can easily decrypt the cipher text with the key provided by the creator of the cipher text recipients, so an unauthorized person cannot be able to decrypt the cipher text unless he or she employs a large computational resource or skill.

2.4.1 Symmetric Key Encryption

Symmetric algorithm use same key for encrypting and decrypting any data, thus communicating partners or individuals or group must have the same key before they can achieve secret communication. The keys may be identical or there may be a modest transformation to go among the two keys. In practice, the keys usually represent a shared secret between two or more persons that can be used to maintain a private information link between two individuals or group [1]. However, this requires that both parties and groups have access to the secret key is one of the main weaknesses of symmetric key encryption, in contrast to public-key encryption [8]. Popular symmetric algorithms include Twofish, Serpent, AES (Rinjdael), Blowfish, CAST5, RC4, 3DES, Skipjack, Safer+/++ (Bluetooth).

Generally Symmetric Encryption algorithms use either Stream cyphers or Block cyphers, with Stream cyphers encrypt the digits (typically bytes) of a message one at a time, whiles Block cyphers take a number of bits and encrypt them as a single unit, padding the plaintext so that it is a manifold of the block size. Blocks of 64 bits have been commonly used however the Advanced Encryption Standard (AES) algorithm sanctioned by National Institute of Standards and Technology (NIST) in December 2001 uses 128-bit blocks [10].

2.4.2 Asymmetric Key or Public key Encryption

In simple terms, Asymmetric Encryption uses two types of key for encryption and decryption. This relies on algorithms that use a public keys for encryption and a private keys for decryption. Although different, the two parts of this key pair are mathematically linked. So for instance the public key would be used to encrypt plaintext or to verify a digital signature; whereas the private key is used in this examples to decrypt ciphertext or to create a digital signature. The term "asymmetric" twigs from the use of dissimilar keys to perform these opposite functions, in divergence with conventional "symmetric" cryptography which relies on the same key to perform both encryption and decryption.

As previously stated, Public-key are related to their corresponding Private keys by certain mathematical functions usually integer factorization, discrete logarithm, and elliptic curve relationships.

Even though, it is computationally easy for a user to generate their own public and private key-pair and to use them for encryption and decryption. The strength of Asymmetric encryption algorithms lies in it being almost computationally infeasible for a properly generated private key to be determined from its corresponding public key. Hence the public keys may be published without actually, compromising security, whereas the private key must not be disclosed to anyone not sanctioned to read messages or execute digital signatures. Examples of Asymmetric Encryption algorithms are the Diffie–Hellman key exchange protocol, DSS (Digital Signature Standard), ElGamal, RSA encryption algorithm (PKCS#1), Cramer–Shoup cryptosystem, YAK authenticated key agreement protocol.

2.5 Advance Encryption Standard (AES)

The Advanced Encryption Standard (AES), also referenced as Rijndael (its original name), is a requirement for the encryption of electronic data established by the United States National Institute of Standards and Technology (NIST) in 2001. The algorithm is based on the Rijndael cipher which was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process [10].

Since then, AES has been adopted by the U.S. government [9] and is now used worldwide. It surpasses the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

2.5.1 Brief History AES

September 12, 1997, the NIST publicly calls for nominees for the new AES, this call is made due to limitations of DES (small key of 56-bit key and block sizes of 64-bit). NIST started an open process to select a new block cipher. The first AES conference was held on 20th August, 1998 where 15 algorithms where chosen as candidates for becoming AES [10].

These algorithms underwent Public Reviews and from 22th to 23rd March 1999 a second AES conference was held where the algorithms were presentat, analysed and tested. Five finalist were then announced in 9th August, 1999 (MARS, RC6, RINJDAEL, SERPENT, and TWOFISH).

At the third AES conference (13th to 14th April, 2000) these five finalist algorithms were subjected to further tests and analysis and on 2nd October 2000, RIJNDAEL was chosen as AES. A publication of a draft by Federal Information Processing Standard (FIPS) was released on 28th February, 2001 which was exposed to public appraisal for 90 days, after series of other publications it was released finally on November 26, 2001 [10].

Rijndael is a family of ciphers with different key and block sizes however for AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits [3].

2.5.2 Description of the Cipher

AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is quicker in both software and hardware. As previously stated the AES specification is a variant of

Rijndael and has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. The Rijndael specification, in contrast, was specified with block and key sizes that may be any multiple of 32 bits with a minimum of 128 and a maximum of 256 bits. In AES the key size used for encryption specifies the number of repetitions of transformation circles that convert the Plaintext (input) into the cipher text (output encrypted data).Below is a table that specifies the number of cycles of repetition required for a particular key length.

Table 1. Number of Rounds Required for a particular key length

Key Length	Number of Rounds or Cycles
128 Bits	10 Cycles
192 Bits	12 Cycles
256 Bits	14 Cycles

Unlike its predecessor DES which made use a Feistel network (the Feistel notion involves the dividing the input block into two halves, processing each half separately, and then exchanging the two halves.), AES works in parallel over the whole input block.

2.5.3 High-Level Description of AES

Internally, the AES algorithm's operations are performed on a two-dimensional array of bytes called the State, with 4 rows, each containing N_b bytes and N_b columns, constituted by 32-bit words. For explanatory purposes let $S_{r,c}$ denote the byte in row *r* and column *c*.

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

Figure 1: State Matrix

1. Initially the array of bytes in input is copied in the State matrix and the cipher Key undergoes a process called Key where round keys are derived from the cipher key using Rijndael's key schedule.
2. Initial Round, each byte of the state is combined with a block of the round key using bitwise XOR this process is called the Add Round Key step.
3. The resulting Matrix or array is then subjected to the following steps:
   i. A non-linear substitution step where each byte is replaced with another according to a lookup table, this step is known as the SubBytes or Bit substitutions Step.
   ii. A transposition step where the last three rows of the state are shifted cyclically a certain number of steps (Shift Rows step).
   iii. A mixing operation which works on the columns of the state, merging the four bytes in each column (Mix Columns).
   iv. Afterwards the Add Round Key step is executed once more
4. Step three is repeated until the final round is reached, At the final round all the processes in step three (3) is executed except the Mix Columns step, that is;
   i. SubBytes
   ii. ShiftRows
   iii. AddRoundKey.
5. The resulting State Matrix is output as the cipher text

2.6 The SubBytes Step

In the SubBytes step, each byte $S_{r,c}$ in the state matrix is replaced with a SubByte $S'_{r,c}$ using an 8-bit substitution box called the Rijndael S-box. This operation provides the non-linearity in the cipher.

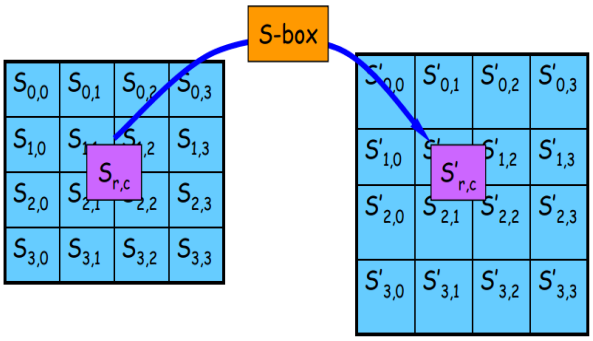

Figure 2: SubBits Step

The S-box is represented as a 16x16 array, with its rows and columns indexed by hexadecimal bits as seen below;

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 4– No.3, January 2016 – www.caeaccess.org

Table 2. 16 by 16 array representation of S-Box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	3	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

The first 4 bits in the byte that is the first hexadecimal value is becomes the row, whiles the last 4 bits becomes the column, hence for example hex 65 is replaced with hex 4D and so on.

2.6.1 The Shift Rows Step

This involves, more or less, the Circular Left Shift of a number of bytes equal to the row number For AES, the first row is left untouched and each byte of the second row is shifted one to the left. In the same way, the third and fourth rows are shifted by offsets of two and three respectively. This is done to prevent the columns in the State Matrix form becoming linearly independent.

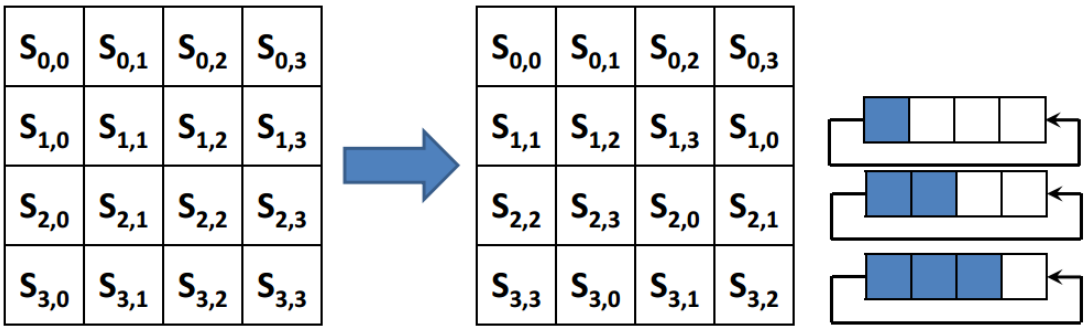

Figure 3: Diagrammatic representation of Shift Rows step

2.6.2 The MixColumns step

Here each column is interpreted as a vector of length four (4) and each column of State is replaced by another column obtained by multiplying that column with a matrix in a particular field (Galois Field). During this stage this operation, each column is multiplied by a fixed matrix below.

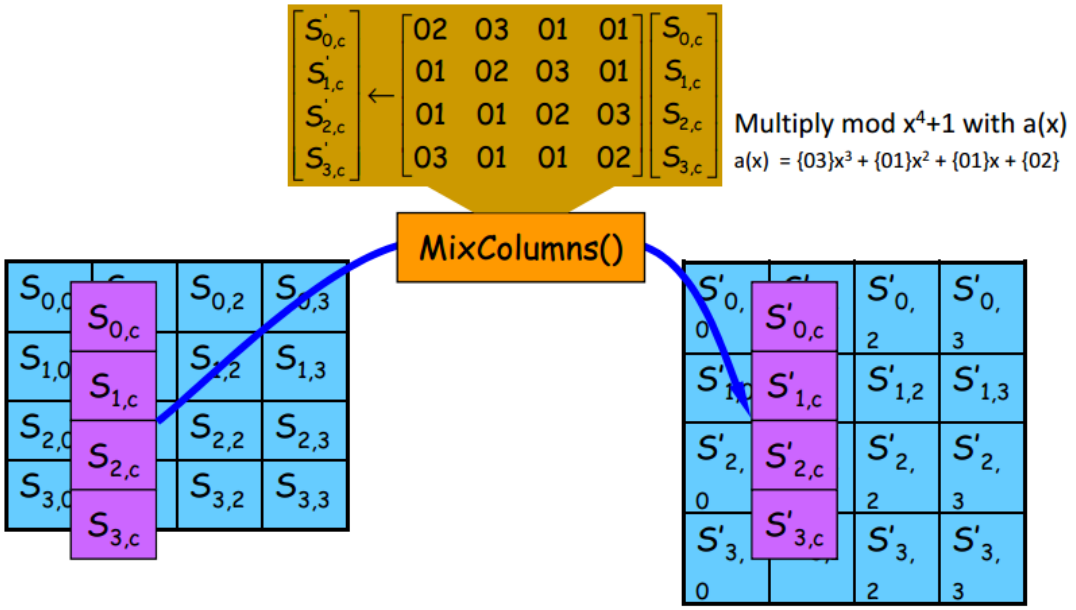

Figure 4: Diagrammatic representation of Mix Columns Step

2.6.3 Decryption in AES

The decryption algorithm is not identical with the encryption algorithm, but uses the same key schedule. During decryption the following four steps:

1. Inverse shift rows
2. Inverse substitute bytes
3. Add round key,
4. Inverse mix columns.

In the third step, the output of the previous two steps are XORed with four words from the key schedule. The final round for decryption does not include the "Inverse mix columns" step

2.7 Some Related Works

Over the last few years, there have been attempts to improve the traditional system through software development. Below are a description of some of them;

2.7.1 The EVOX Voting System

This was implemented by [6], Massachusetts Institute of Technology (M.I.T.) as part of his Master's thesis. It was based on the paper, "A practical secret voting scheme for large scale elections", by Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta (AUSCRYPT '92, 1993). EVOX's interface was built using HTML which linked with a Java applet, it used the JDK 1.1 because of its cryptographic class and functions. This software made use of the RSA encryption method [6]. Since RSA works on the bases of multiplication of two prime numbers, number factorization is a serious threat to the security of systems that use RSA [5].

2.7.2 Electronic Voting System

It was designed by [7], as a thesis submitted a degree in Bachelor of Science in Computer Science and Engineering of the BRAC University, Dhaka, Bangladesh [7].

Their prototype used java as their front end and an SQL database as their back end and made use of Data Encryption Standard (DES) as it encryption method. This encryption standard has been replaced by AES, due to its small key size of 56-bit key and block sizes of 64-bit.

2.8 The Proposed System

2.8.1 Introduction

The Voting software is composed of two applications, which is the Sever application and Client application, with the former handling registration of voters and tally of votes while the latter handles the casting of votes. Both applications would run Microsoft's Windows Seven (7) Operating System, however they would also work perfect with earlier versions of Microsoft's Operating System. Its user interface is built with Microsoft Visual studio 2012 using Visual C-Sharp(C#) as programming language. The whole system makes use of a centralized database using Microsoft SQL Server 2012 as its Relational Database Management System. To ensure security the system made use AES to encrypt all votes that are cast and biometric identification for verifying voters.

2.8.2 Application of AES on System

AES is an iterative, symmetric-key block cipher that can use keys of 128, 192, and 256 bits, and encrypts and decrypts data in blocks of 128 bits (16 bytes). Unlike public-key ciphers, which use a pair of keys, symmetric-key ciphers use the same key to encrypt and decrypt data. Encrypted data returned by block ciphers have the same number of bits that the input data had. Iterative encryptions use a loop structure that repeatedly

performs permutations and substitutions of the input data. The diagram below represents the AES algorithm in an activity diagram.

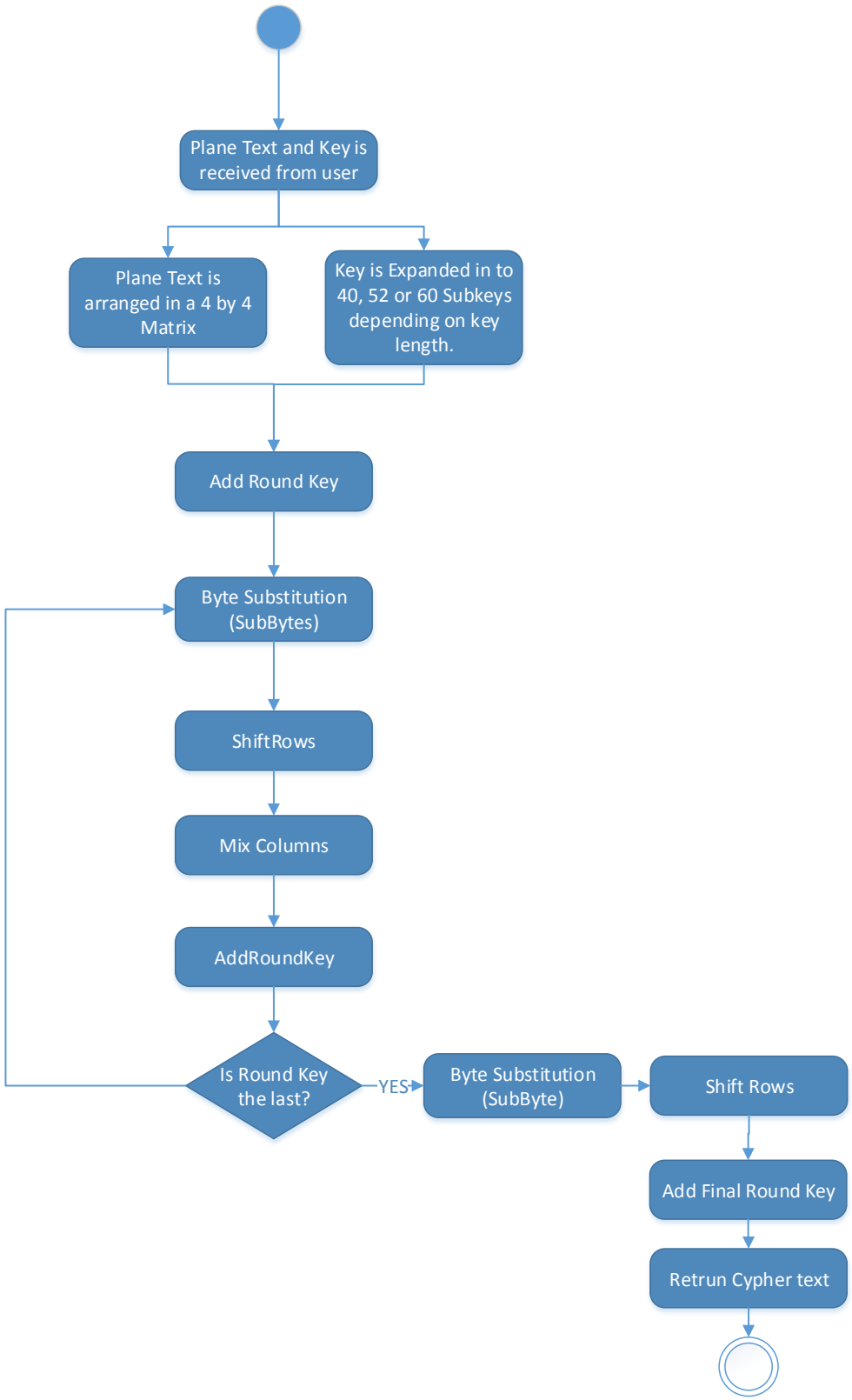

Figure 5: Activity diagram for AES algorithm

This encryption algorithm was put to good use during the implementation of the software, it was specifically used to encrypt the voters vote before it was sent to the server application via a network, where the server application would also decrypt and tall the votes cast. The diagram below give a general idea of how the encryption was applied to the voting process.

Figure 6: How AES is applied to Voting system

3. USERS OF THE SYSTEM

The system has four types of users, Electoral Commissioner (EC), The Registration Officer, Polling Agent and finally the Voter. Each user is expected to provide their corresponding user name, password before they can log in successfully. The table below shows the various user's rank and their hierarchy.

Table 3. Users of the system.

User	Functions
Electoral Commissioner (EC),	Start, Stop Elections and View Voting Statistics
Registration Officer	Register Voters, Candidate and Political Parties
Verification Officer	Check Voter Validity and generate password for Voter
Voter	Cast Vote

3.1 Usage Scenario Representation

Here the user interaction with the software is described using Use Cases and Activity Diagrams. A use case is a methodology used in software analysis to identify, clarify, and organize system requirements. Use case diagrams are employed in UML (Unified Modeling Language), a standard scheme for the modeling of real-world objects and systems.

The system generally has four actors or users and the subsequent Use Case diagrams shows how the users interacts with the various forms and sub forms of the system.

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 4– No.3, January 2016 – www.caeaccess.org

3.1.1 Use Case Description of the System

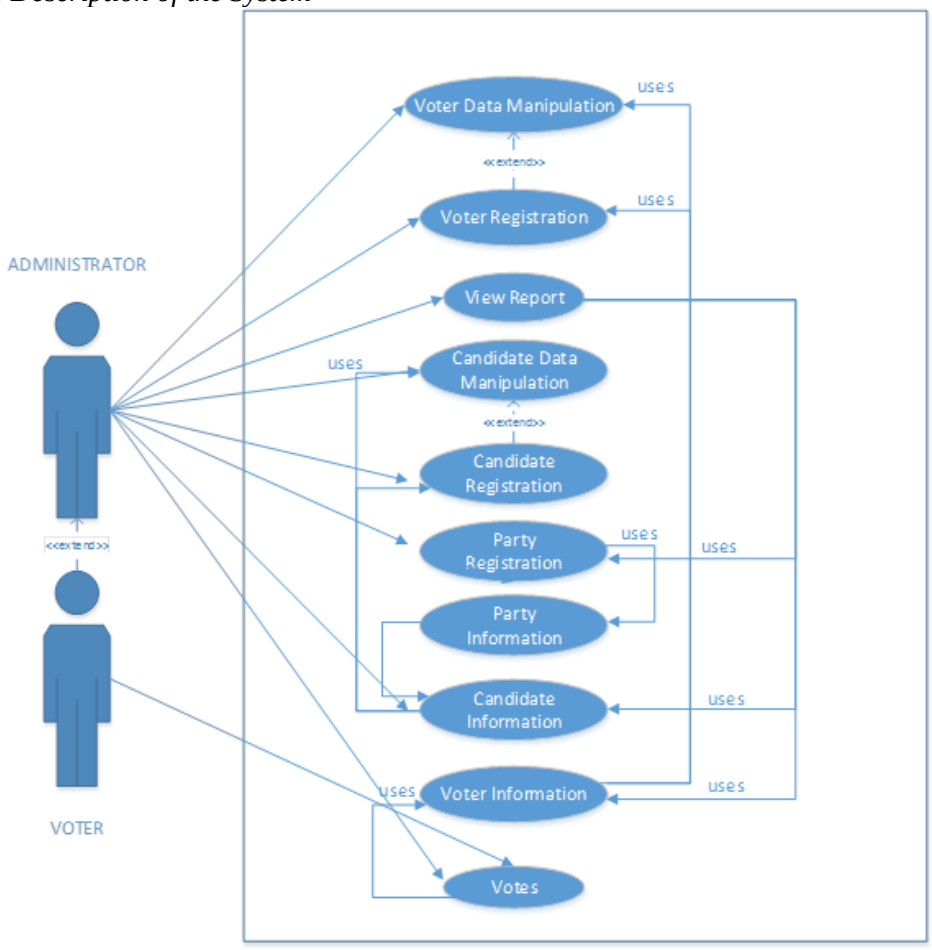

Figure 7: General Use case diagram for the System

3.1.2 3.1.2 Use case of the Electoral Commissioner (EC)

The diagram below shows how the EC interacts with the system

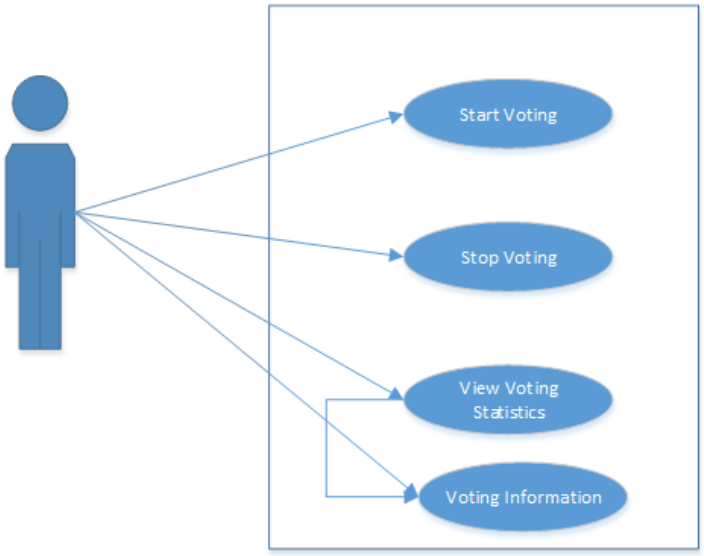

Figure 8: Use Case of the EC's Session

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 4– No.3, January 2016 – www.caeaccess.org

3.1.3 Use case of the Registration Officer

The diagram below shows how the Registration Officer interacts with the system.

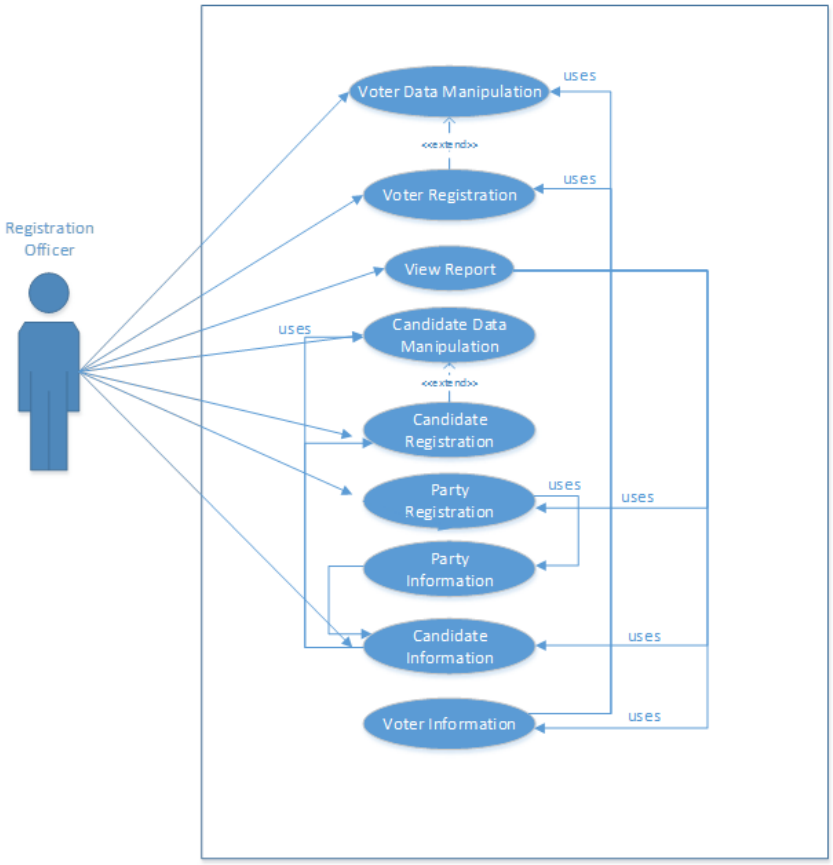

Figure 9: Use case of the Registration Officer's Session

3.1.4 Use case of the Verification Officer

The diagram below shows how the Registration Officer interacts with the system.

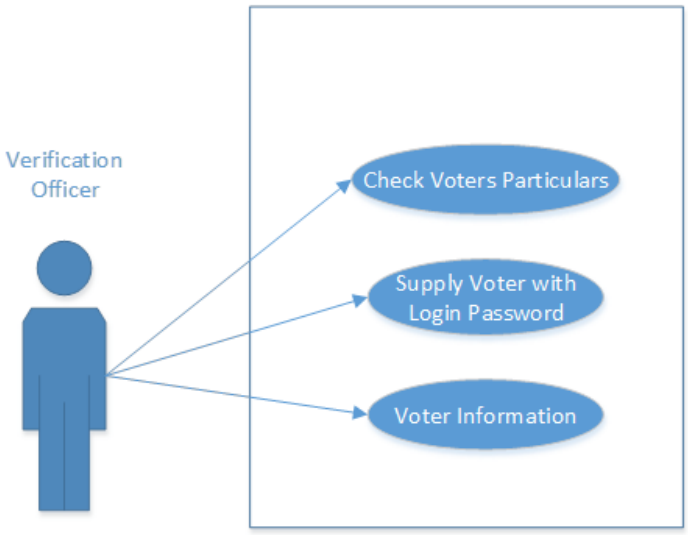

Figure 10: Use case of the Verification Officer's Session

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 4– No.3, January 2016 – www.caeaccess.org

4. ACTIVITY DIAGRAM OF THE SOFTWARE

In Unified Modeling Language (UML), an activity diagram refers to the graphical representation of the execution of activities or procedures in relation to a given system. Activity diagram describes parallel and conditional activities, use cases and system functions at a detailed level. The state of an activity relates to the performance of each workflow step. (Janssen, 2015).

The following figures of activity diagrams shows some of the selected actions that occur in some of the sessions of the system.

4.1.1 Sever System login Activity Diagram

Figure 4.5 shows the steps taken as user logs on to the system. Access is only granted if the correct User ID and password combination is entered

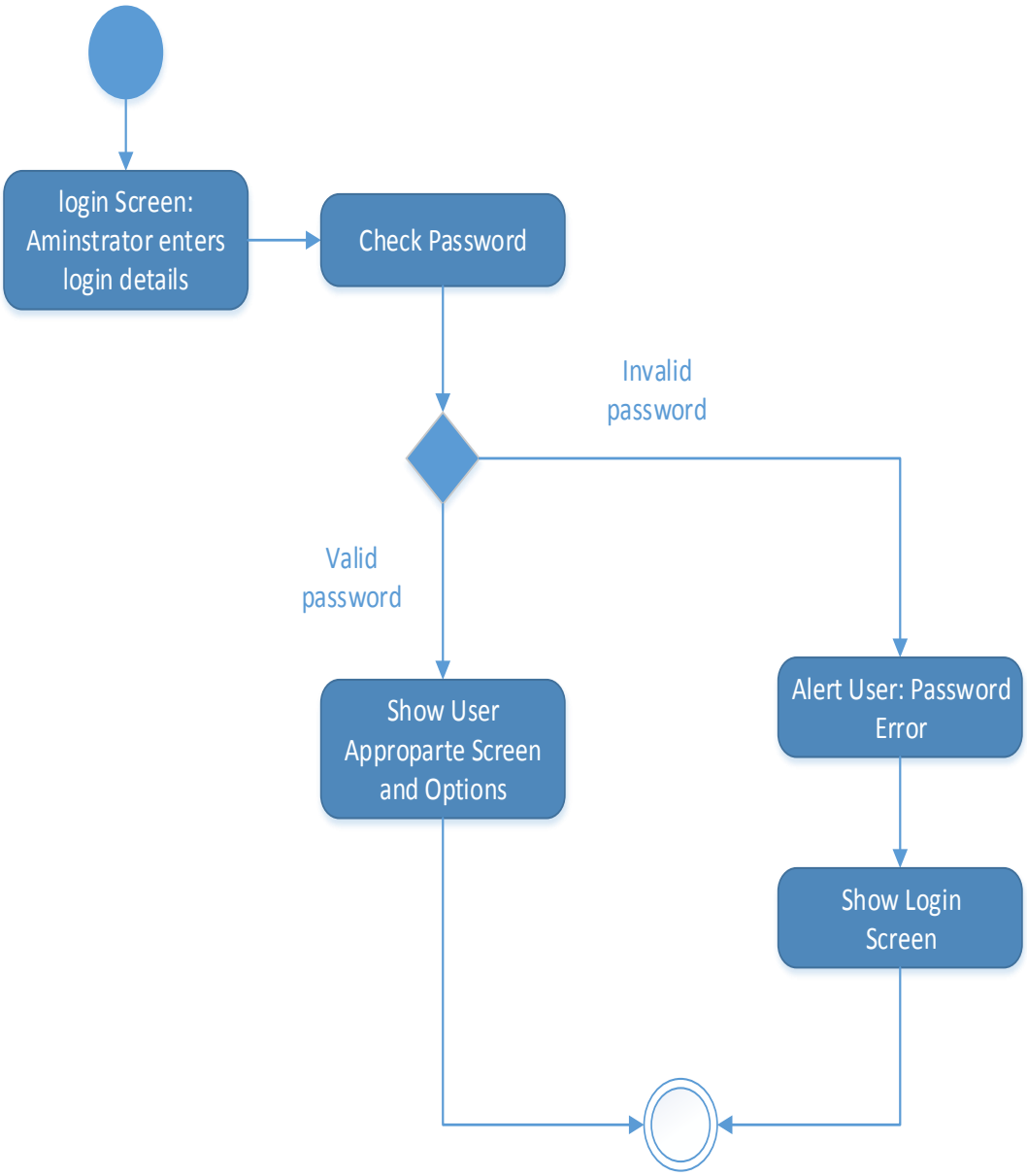

Figure 11: System's login

4.1.2 Client system (Voting) Activity Diagram

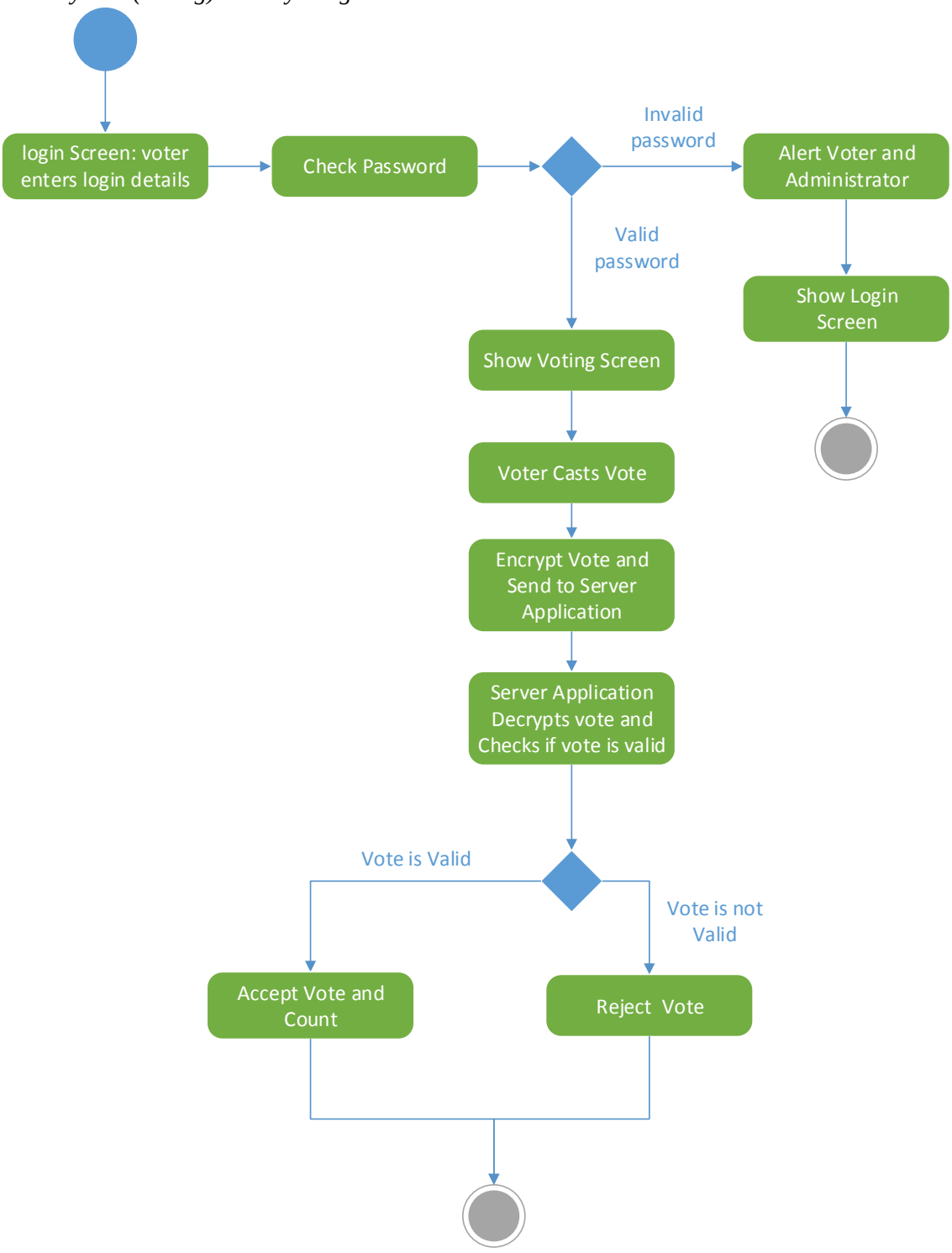

Figure 12: Client system (Voting) Activity Diagram

5. CONCLUSION

Elections are prerequisite for every democratic country. Conducting free, fair and credible elections to select leaders to govern these countries have become paramount for every electoral commission. To achieve this task, a biometric enabled identification software using AES encryption have been developed for public elections to improve security and reliability of the voter intent. The confidence of the voter is much higher if the voter is sure that, their votes are tallied for the right candidate during the voting process. In future this system could be improved to include multiple biometrics and a web based application.

6. REFERENCES

[1] Delfs, Hans & Knebl, Helmut (2007). "Symmetric-key encryption". Introduction to cryptography: principles and applications. Springer. ISBN 9783540492436

[2] Electronic Voting, Wikipedia, April 2015. Retrieved fromwebsite:http://en.wikipedia.org/wiki/Electronic_voting

[3] Federal Information Processing Standards (FIPS) (November 26, 2001) "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", Publication 197

[4] G.O. Ofori-Dwumfuo and E. Paatey, 2011. "The Design of an Electronic Voting System". Research Journal of Information Technology 3(2): 91-98, 2011 International Institute for Democracy and Electoral Assistance (International IDEA) (December 2011). "Introducing Electronic Voting: Essential Considerations". PolicyPaper. ISBN 978-91-86565-21-3

[5] Majid Bakhtiari & Mohd Aizaini Maarof, (2012),"Serious Security Weakness in RSA Cryptosystem". IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3, January 2012

[6] Mark A. Herschberg, 1997. "Secure Electronic Voting Over the World Wide Web", Massachusetts Institute of Technology.

[7] Mostafizur, R., Sharfuddin B., & Rajibul, H., Electronic Voting System, (2007) BRAC University, Dhaka, Bangladesh.

[8] Mullen, Gary & Mummert, Carl (2007). Finite fields and applications. American Mathematical Society. p. 112. ISBN 9780821844182.

[9] National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information - CNSS Policy No. 15, Fact Sheet No. 1, June 2003 Retrieved from Website: http://niatec.info/viewpage.aspx?id=244

[10] NIST.gov, 2001. "NIST FIPS 197 - Advanced Encryption Standard (AES)". Retrived for the Website: http://www.nist.org/nist_plugins/content/content.php?content.39

[11] Superior Electoral Court, 2014. "The history of Brazilian voting machines". Retrieved from website: http://english.tse.jus.br/noticias-tse-en/2014/Fevereiro/justice-carlos-velloso-the-history-of-brazilian-voting-machines

[12] Reuters "Ghana's Mahama wins election, opposition cries foul". 9 December 2012. Retrieved form website : http://uk.reuters.com/article/2012/12/09/uk-ghana-election-idUKBRE8B809120121209

.