IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

AES Based Online Voting System

Lalit Kumar Gupta[1*], Utkarsh Tiwari[2], Ajay Kumar[3], Saumya Jaiswal[4]

[1,2,3,4] Department of Computer Science Engineering, IET, Bundelkhand University, Jhansi, India

*Corresponding Author: dr.lalitgupta.bu@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i3.915918 | Available online at: www.ijcseonline.org

Accepted: 26/Mar/2019, Published: 31/Mar/2019

***Abstract*—** In this time of technological advancement everything is online and so is the voting. The online voting is time saving, efficient, reliable and fast. The online voting requires safety for the communication setup between client and server so for that purpose Kerberos protocol is used in the voting process for the authentication purpose which uses DES cryptography but DES is not secure enough to handle highly valuable data used in voting so in order to make it more secure we need to replace DES with some other cryptography technique. Kerberos uses DES by default, but it easy to decrypt so to enhance its security we need to replace it with AES cryptography. So here in this paper, we will discuss AES cryptography as the replacement of DES and its implementation with Kerberos. As AES is mathematically more efficient than DES other than that it allows choosing a 128-bit, 192-bit or 256-bit key as compared to the 56-bit key of DES thus making it exponentially stronger.

***Keywords*—** DES, AES, NIST, IDEA, BDB, HMAC, CBC

I. INTRODUCTION

Voting is a method by which collective decision is taken. It plays a vital role in the decision-making process when more than one individual or parties are involved in the decision-making process.

In this fast-moving world, no one wants to waste their time and for that, there are plenty of enhancements have been bought to our day to day life one of which is the internet. Nowadays everything is online so why not the voting be online as it will save the time and is in many ways better than the traditional voting like in traditional voting the polling booths are set up and people have to reach to the polling booth and have to stand in long queues that waste lot of time other than time wasting for casting vote it takes a lot of time in traditional method to count the votes not only this there is possibility of fake votes as user identity cannot be authenticated and also the people who are physically unfit or are out of the city cannot cast their vote or may find it hard to cast vote.

Online voting is a solution to all these problems as firstly people do not have to stand in queue to wait for their turn to cast votes they can cast vote from home or from anywhere from where they can get access to internet-enabled computer system, the counting process is also fast and authentication of voters can be done using biometric authentication thus making voting fast fair and reliable. This to be kept in mind that voting is not necessarily only concerned with voting for election any type of voting where decision making is required the online voting can be used there.

The authentication protocol to be used in online voting is Kerberos [1], Kerberos protocol can work with both symmetric and asymmetric cryptography, the Kerberos protocol when using symmetric cryptography it by default uses the Data Encryption Standard (DES) for encryption but in case of online voting the data transferred between client (here voter) and server is very sensitive and DES cannot provide enough security to his data so there is need of replacement and DES can be replaced by Advanced Encryption Standard (AES) which is much more secure and can handle the sophisticated voter data with much more security thus making online voting much more reliable and secure process.

In this paper, we are discussing how to improve the security of the online voting system by replacing DES cryptography with AES cryptography. We will focus on working of AES cryptography, how it is more secure than DES cryptography and what are its advantages. Also how it will be implemented in an online voting system.

II. LITERATURE

Overview of Online Voting: Voting is the process of collection of choices to make a decision which can be achieved through various methods like Ballot paper voting, machine voting, and postal voting. Online voting is the most advanced version of voting which has the same purpose as

other voting methods but in this method, voting is carried out online where people can cast vote from their personal computer system or provided polling kiosk and need not go anywhere. This method is quick, smart, and most reliable as compared to other types of voting. The online voting system reduces the time consumed in the counting of votes as compared to tie taken by ballot based voting method [2-4].

Cryptography: It is the art of protecting information by converting it into an unreadable format, called ciphertext. It can only be converted back into plain readable text by those who have the secret key.
As with the use of the internet is increasing day by day for electronic communication, electronic security is becoming increasingly important. Cryptography is used to protect important information which is not supposed to be shared with everyone, information like e-mail messages, credit card information and corporate data.
Cryptography system is classified into types:
1. Symmetric-key system: It is a system that uses a single key that both the sender and recipient have
2. Asymmetric-key system: It is a system that uses two keys, a public key which is known to everyone and a private key that is known and can be used only by the recipient of messages [5].

Kerberos: Kerberos is an authentication protocol. In this protocol, the secret key cryptography is used for secure communication and authentication in client/server applications [1,6]. It provides security when there is an exchange of information it also deals with security issues like confidentiality, integrity, authentication, etc.

Data Encryption Standard: The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standard and Technology (NIST) [7].
In this, the data is encrypted in a block of 64 bits. It produces 64-bit cipher text. The key length is 56 bits. Initially, the key is consisting of 64 bits. The following bit position discarded from the key length is 8, 16, 24, 32,40,48,56 and 64. The two fundamental aspects of cryptography on which DES is basically established are Substitution and transposition. DES consists of 16 steps, each of which are also termed as Round [6].
International Data Encryption Algorithm: The International Data Encryption Algorithm (IDEA), it was originally called Improved Proposed Encryption Standard (IPES). It is a block cipher algorithm. Xuejia Lai and James L. Massey of ETH-Zurich designed this algorithm and they described it first in 1991. This algorithm was made as a replacement for the Data Encryption Standard (DES).
IDEA consists of a series of 8 identical transformations and an output transformation. Operating on 64-bit blocks using a 128-bit key the processes for encryption and decryption are quite similar in this algorithm. The security is derived mostly by alternating between operations from different groups. The groups are modular addition and multiplication, and bitwise exclusive-OR (XOR) – which are algebraically incompatible in some sense.

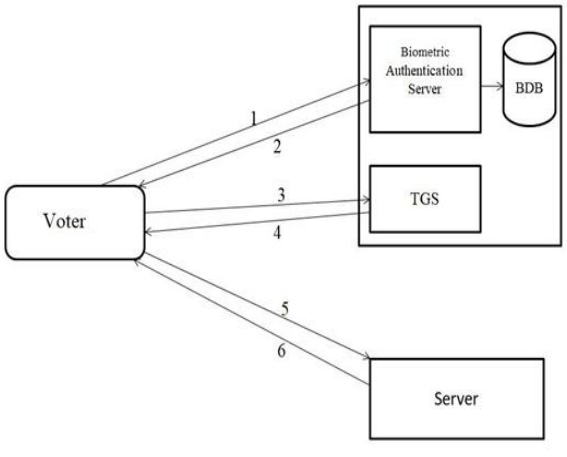
Advanced Encryption Standard: The Advanced Encryption Standard (AES) is a symmetric block cipher whose development was started by National Institute of Standards and Technology (NIST) in 1997 when there was need of successor algorithm for Data Encryption Standard.
It is implemented in hardware and software to encrypt sensitive data it is also chosen by the U.S. government to protect classified information.
It is the most popular algorithm used in symmetric key cryptography. It is more secure and is also support faster encryption and decryption as compared to its predecessors i.e. DES.

III. ONLINE VOTING SYSTEM WITH AES CRYPTOGRAPHY

• Online Voting System:

As security and privacy are the most important aspect of voting, so Kerberos based online voting system is the most secure and advanced option of the present time. It is the most secure system in comparison to all the other options available for voting. Being biometric-enabled this system provides the highest level of privacy. As it works online so not only the process of voting is fast, but the generation of results is also quick and accurate. Online voting is allowed in some countries. Estonia was the first country to use online voting. It was used for local elections in 2005 [8].

• Design and Implementation:



Security Model

The Authentication process involved in online voting is as follows [10]:

1. The voter will go to the kiosk and entered registration number in the voting machine which will send the details to biometric authenticator then biometric authenticator will ask for the fingerprint scan then it will authenticate the voter and will generate a ticket

2. The AS sends back a ticket which is encrypted with the secret key of the voter and the voter decrypts the ticket and this ticket will be sent to the voting machine.

3. The voting machine will send this ticket to the token granting server than token granting server will raise a token with details of the voter which are the area that can be accessed by the voter.

4. Then this token will be sent to a voting machine which will be sent to the server.

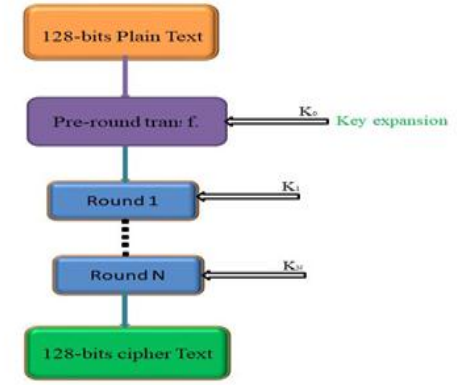
5. The server will verify the details in the token and will redirect the voter to a page containing choices with details of each choice. Each choice will have a vote button in front of it the voter will opt the choice he wants to opt by clicking on the vote and pressing the submit button.

6. After the vote is cast successfully the server will send the confirmation message on the screen of the voting machine.

Here in all above steps, the data is sent from voter to the server and in the meantime, while it is in midway between voter and server it can be stolen or can be altered by some attacker/hacker so in order to save this data from going to wrong hand AES cryptography plays its role.

IV. ADVANCED ENCRYPTION STANDARD (AES) CRYPTOGRAPHY

AES is a symmetric key block cipher. It is an advanced version of DES and stronger and faster than DES. The block cipher AES operates with 128-bit plaintext and cipher text blocks and is controlled by a 128-bit key with 10 number of the round in encryption. Plane text divided into 16-byte sub-blocks and this encryption key are used in many forms i.e. I) 10 No. Of the round in encryption and 128 bits key used. II) 12 No. Of the round in encryption and 192 bits key used. III) 14 No. Of the round in encryption and 256 bits key used.



AES Block Diagram

Following are the steps of AES –
Encryption Process

1) At a time it takes a plain text and divides it into sub-blocks, these sub-blocks are the inputs for the first round of the algorithm. If the size of plain text is 128 bits, it will be divided into 16 bytes sub-block.

2) For 128 bits key the encryption process is executed in 10 rounds.

3) The 16 Byte sub-block are substituted by a fixed table (S-box). The result comes out in a matrix of four rows and four columns.

4) In this stage Shift Rows phases of AES, each row of the 128-bit internal state of the cipher is shifted. The rows in this stage refer to the standard representation of the internal state in AES, which is a 4x4 matrix and cell contains a byte. Bytes of the internal state are placed in the matrix across rows from left to right and down columns. In the Shift Rows operation, each of these rows is shifted to the left by a set amount. Their row number starting with zero. The top row is not shifted at all; the next row is shifted by one and so on. The result is a new matrix consisting of the same 16 Bytes.

5) The Mix Columns stage provides diffusion by mixing the input around. A mathematical function is using transform each column of four bytes. This function takes as input the four Byte of one column and outputs four completely new bytes, which replace the original column. The result is a new matrix consisting of the same 16 new Bytes. These rounds perform the 10 times and output produced is ciphertext consisting of 128 bits.

6) The Roundkey stage, The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Decryption Process

The decryption process is the same as the reverse order of the encryption process. It's every round consider four process reverse order of the encryption process.

- Round key
- Mix columns
- Shift rows
- Byte substitution

Above mention, sub-process is reverse order of the encryption process and its process converted cipher text to plain text.

V. COMPARATIVE STUDY OF SECURITY

Cipher algorithm	Cipher mode	Key length	HMAC	Strength
DES	CBC	56-bits	CRC 32-bits	Weakest
3DES	CBC	168-bits	SHA-1 96-bits	Weak
IDEA	CBC	128-bits	SHA-1 96-bits	Strong
AES	CBC	128-bits	SHA-1 96-bits	Strongest

VI. CONCLUSION

We can conclude that online security is a very pressing issue in this time of advanced technology. So in the online voting system also, the security system must be reliable. Though the implementation of the online voting system will make things easy, fast and smart, this system should also be very much secure. AES is an advanced version of DES and stronger and faster than DES. The Kerberos uses DES cryptography to protect voter and server communication. This communication can be made more secure through the use of AES. AES cryptography improves Kerberos security and stability and eliminates its limitation.

REFERENCES

[1] Kerberos Overview- An Authentication Service for Open Network Systems, Document ID:16087

[2] S. P. Everett, M. D. Byrne, and K. K. Greene, "Measuring the usability of paper ballots: Efficiency, effectiveness, and satisfaction", Proceedings of the Human Factors and Ergonomics Society 50th Annual Meeting, (2006) October 16-20; Santa Monica, USA

[3] S. P. Everett, K. K. Greene, M. D. Byrne, D. S. Wallach, K. Derr, D. Sandler, and T. Torous, "Electronic Voting Machines versus Traditional Methods: Improved Preference, Similar Performance", CHI Proceedings: Measuring, Business, and Voting, (2008) April 5-10; Florence, Italy.

[4] M. Patil, V. Pimplodkar, A. R. Zade, V. Vibhute and R. Ghadge, "A Survey on Voting System Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 1, (2013).

[5] Diffie, Whitfield; Hellman, Martin (8 June 1976). "Multi-user cryptographic techniques". AFIPS Proceedings. 45: 109–112

[6] Jindal, S., & Sharma, M. (2016). Design and Implementation of Kerberos using DES Algorithm, 92–95.

[7] Robert Sugarman (editor) (July 1979). "On foiling computer crime". IEEE Spectrum

[8] Voting methods in Estonia: Statistics about Internet Voting in Estonia VVK.

[9] Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.

[10] Lalit Kumar Gupta, Utkarsh Tiwari, Manoj Kumar Chaudhary, Kuldeep Kasaudhan, "Secure Voting Using Bio-metric Authentication", International Journal of Computer Sciences and Engineering, Vol.7, Issue.2, pp.731-735, 2019.

Authors Profile

Mr. Lalit Kumar Gupta pursed Bachelor of Technology from Purvanchal University, Jaunpur in 2001 and Ph.D. from Bundelkhand University in year 2016. He is currently working as Assistant Professor in Department of Computer Science & Engineering, Institute of Engineering & Technology, Bundelkhand University, Jhansi since 2006. He is a member of various computer societies. He has published more than 10 research papers in reputed international journals. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Grid Computing, IoT and Computational Intelligence based education. He has 13 years of teaching experience.

