JPPIPA 9(9) (2023)

Jurnal Penelitian Pendidikan IPA

*Journal of Research in Science Education*

http://jppipa.unram.ac.id/index.php/jppipa/index

# Implementation of AES-256 Algorithm in Android-Based E-Voting Data Security

Faiz Nazhir Amrulloh[1*], Yuli Asriningtias[1]

[1] Faculty of Science and Technology, Universitas teknologi Yogyakarta, Yogyakarta, Indonesia.

Received: July 5, 2023
Revised: September 6, 2023
Accepted: September 25, 2023
Published: September 30, 2023

Corresponding Author:
Faiz Nazhir Amrulloh
faizn890@gmail.com

DOI: 10.29303/jppipa.v9i9.4543



**Abstract**: E-voting is a method of voting and vote counting in general elections using digital devices. There are still many errors and fraud that occur during village head elections in Indonesia. Then the idea was created to carry out village head elections by utilizing existing technological developments, especially Android-based smartphone technology. The data source used in this study is secondary data which uses population data of citizens who will exercise their right to vote, vote data for citizens' voting rights, and data from the results of vote acquisition during the village head election process. In this study, a number of important data were needed in the village head election process which was carried out using documentation techniques. This research produced an Android-based application system for securing e-voting data for village head elections using the AES-256 cryptographic algorithm called Vodes. The application produced in this study was built using the Kotlin programming language on the Android frontend side by utilizing the Android Studio IDE as a tool in the development process. While on the backend side it uses the Javascript programming language using the Node js framework. The database used in the Vodes application uses MySQL. Based on the results of this study, it can be concluded that an e-voting data security application for village head elections has been created using the AES-256 cryptographic algorithm. The application produced in this study has succeeded in properly securing all aspects of the data in the village head election process.

**Keywords:** AES-256; Cryptography; Data security; E-voting; Village head

## Introduction

The development of communication technology in Indonesia, especially Android smartphones, is very rapid (Simsir et al., 2022; Wijayanti et al., 2022). Reporting from the Ministry of Communication and Information (Kominfo) states that in 2021 as many as 167 million people or 89% of the total population of Indonesia use smartphones (Nugroho et al., 2019; Said et al., 2018). The majority of Indonesia's population uses Android type smartphones. This has become a trigger for changing every existing bureaucratic system in society into a digital system (Pan et al., 2020). One of them is changing the conventional general election bureaucracy system to an electronic voting system (e-voting). E-voting is a method of voting and counting votes in general elections using digital devices (Petitpas et al., 2021; Risnanto et al., 2022; Verma et al., 2022; Yi, 2019).

The bureaucratic system in general elections in Indonesia is still carried out manually, including village head elections. Citizens who have the right to vote are required to come to the polls on Election Day. Residents who come will then vote on the ballot paper and then put it in the ballot box. After the voting process is complete, then the vote counting process will be carried out. The conventional election bureaucratic system for villages has several weaknesses. Some of the weaknesses of the conventional process include (Eka Putri et al., 2021).

In Indonesia, it takes up to several weeks for the vote counting process and it is difficult to re-count the votes if there is distrust of the vote count results. Inaccurate vote count results. There is often debate about

**How to Cite:**
Amrulloh, F. N., & Asriningtias, Y. (2023). Implementation of AES-256 Algorithm in Android-Based E-Voting Data Security. *Jurnal Penelitian Pendidikan IPA*, *9*(9), 7757–7766. https://doi.org/10.29303/jppipa.v9i9.4543

whether ballot papers are valid or invalid, making the results of the vote count less accurate. Residents who will vote sometimes do not know who the candidate for village head will be elected because of the lack of information provided. Errors often occur, such as voters voting for more than one candidate, voters not voting, and voters wrongly marking the ballot paper (Djuyandi et al., 2019; Yi, 2019).

Based on research conducted states that there are still many errors and fraud that occur during village head elections in Indonesia. Supported by this research and the many problems above, especially regarding data security issues, an idea was created to carry out village head elections by utilizing existing technological developments, especially Android-based smartphone technology. This is also supported by the increasingly widespread and even distribution of internet networks and cheaper internet costs. With e-voting focused on data security and the use of Android-based technology, it is expected to be a solution. In this writing, the researcher explores information from several previous studies as a comparison material, both regarding the shortcomings or advantages that already exist. The results made for comparison are inseparable from the research topic, namely the security of village head election e-voting data using the AES-256 method (Fitriani et al., 2020; Hao et al., 2019; Zhao et al., 2017).

This research regarding the development of the Pilkades e-voting mobile application, where system design uses the Waterfall method. The result of this research is the creation of an android application which functionally runs smoothly with the black-box testing method and is compatible with various versions of Android, at least the Jelly Bean version and above (Guntur, 2020; Prasetyawan et al., 2018; Rachawati et al., 2022).

E-voting system by implementing blockchain to secure election voting results (Anjarsari et al., 2020; Oprea et al., 2023). The blockchain technology used is able to help store voting results data that is transparent and accessible to the public. The technology also helps maintain the confidentiality of voters (Pratama et al., 2021; Yulianton et al., 2018). The result of this research is to create an e-voting application that helps the voting process to be easier in terms of managing related parties, voting, to vote counting as well as helping in terms of data security (Hu et al., 2019; Noor, 2020).

Research regarding securing data transfers on the API for e-voting applications using the RSA algorithm, where the research method uses the waterfall model. The result of this research is to design and create an E-Voting application that focuses on how to ensure that a voter is a valid voter according to applicable rules and ensures that data transfers when voters elect one of the candidates cannot be interrupted or tampered with by anyone who irresponsible by randomizing the results of voter choices using RSA Encryption (Siswanto, 2020).

E-voting design system for village head elections for information transparency in Lueng Bata District, Banda Ache City. The research method used is the observation method. Observations were made to obtain the data needed in making the design of the e-voting application. This observation method is in the form of collecting data from sources related to the application to be designed, namely the village head election application. The results of the system design are to obtain data quickly and accurately, so it is hoped that the selection of geuchik online can be carried out in a transparent, efficient and professional manner. Elections by e-voting can also be carried out quickly and at a lower cost compared to conventional elections (Fischhoff, 2019).

Research on the e-voting application for village head elections was also carried out designing a web-based e-voting application using the implementation of the classical Caesarean cryptographic algorithm. The results of this study are creating applications using the Caesar Classical Cryptographic Algorithm for securing data and voting results so that the system that is run runs according to the corridor and there is no repetition or abuse of the identity of vote users who choose potential partners in a school organization where the system that is running produces the expected output and there is no vote fraud (Hidayat, 2020; Pandit et al., 2014). Based on some of the literature reviews, researchers want to make an application for securing village head election e-voting data as a cryptographic algorithm. This e-voting data security system is intended to assist the voting process to make it easier in terms of managing related parties, voting, to vote counting as well as assisting in terms of data security and transparency. Judging from the 6 reference sources, the difference between the six references with titles raised by researchers lies in the method used, namely the use of Advanced Encryption Standard Analitycal (AES) 256 as a cryptographic method to improve the security of e-voting data for village head elections in Indonesia (Cahyo et al., 2022; Hasibuan et al., 2022; Indapwar, 2020).

The purpose of this research is to build an android-based village head election application by utilizing AES-256 as a cryptographic method in order to minimize the occurrence of fraud in the village head election process. While the benefits of developing this application are that it makes it easier to carry out the process of voting and counting village head elections and reducing problems or fraud during the voting and counting process for village head elections. Based on the background of the problem, the formulation of the problem is obtained on how to build an android application to conduct village head elections which are expected to reduce the problems that have occurred during conventional village head elections.

## Method

Primary data that has been further processed and presented either by primary data collectors or by other parties, for example in the form of tables or diagrams. The data source used in this study is secondary data. The secondary data is population data for citizens who will exercise their right to vote, data on prospective candidates, vote data for citizens' voting rights, and data on the results of the calculation of vote acquisition during the village head election process. Secondary data in the form of citizen population data consists of resident Identification Number (NIK), name, place of birth, date of birth, gender, and complete address consisting of RT/RW, village/kelurahan, sub-district, district/city, province, and phone number. Secondary data in the form of village head candidate data consists of name, place of birth, date of birth, gender, complete address consisting of RT/RW, village/kelurahan, sub-district, district/city, province, photo or image of the candidate's partner, vision and mission of the prospective candidate pair and work.

In this study, a number of important data were needed in the village head election process which was carried out using documentation techniques. Documentation is done by collecting documents in the form of photos and digital files. Henceforth it can be used to interpret, strengthen, and test the validation of the system to be built. In this study a number of data were needed which were obtained using several methods, including:

*Observation*

Observations were made to collect information about the needs of researchers in collecting data by means of observations related to the process of selecting village heads conventionally or using an electronic system or what is commonly called e-voting.

*Library Studies*

Data collection by reading books and other literature that can be used as a reference related to research to develop new systems, both reading conventional books and ebooks. The time for data collection in this study can be seen in Figure 1. The time the researchers used for this research was carried out from 10 to 18 October 2022 which was divided into 3 sessions. In the first session on October 10-13, secondary data was collected in the form of citizen population data and data on candidates for Pilkaded candidates. Then on October 15, the process of making citizens' voting rights data was carried out. The last session on October 18 carried out the preparation of secondary data in the form of data on the results of vote acquisition. The business rules for conventional village head elections can be seen in Figure 1. The process begins with voting by residents who have the right to vote. Followed by the vote counting process, signing the minutes of the vote counting results, and ending with the announcement of the village head election results.

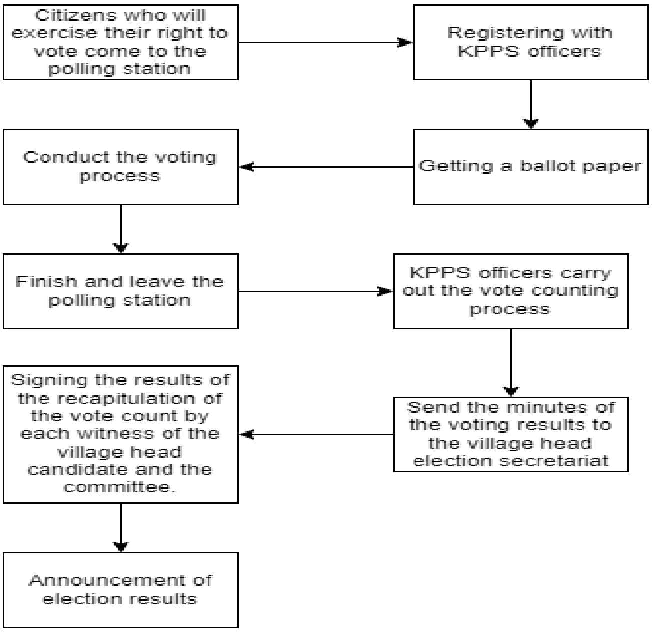



**Figure 1.** Model architecture

The stages of this research describe how the initial conditions differ when this application does not yet exist with the conditions when this application was proposed, as well as with the final conditions when this application can already be used. The following below is Figure 2 which is the framework of this study. This is done so that research can be more easily understood because later in the research report the distribution can be consistent.

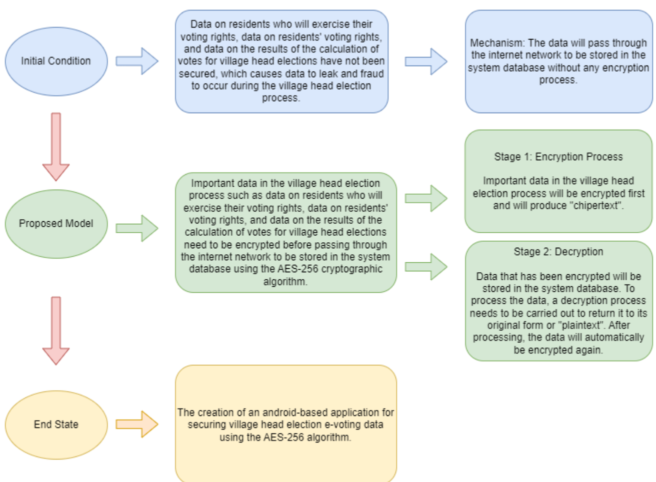



**Figure 2.** Research framework

## Result and Discussion

### *Results*

*Running System Analysis*

System analysis that runs on the village head election system in Indonesia is still running conventionally, although there are several technological developments that can improve the election process to be more efficient and transparent. Currently, village head elections in Indonesia are generally carried out using the direct voting method at the polling stations (TPS). This conventional system involves several stages, such as compiling voter lists, updating voter data, nominating candidates for village heads, campaigning, to carrying out physical elections at TPS. However, there are several obstacles in this system that affect the continuity and trust of the community in the village head election process. One of the main obstacles is the accuracy of voter data. The process of compiling and updating voter data is still done manually, so it is prone to errors in recording and verifying voter data. This can result in problems such as multiple voters or voters who are not legally registered. However, there have been efforts to improve the village head election system in Indonesia. The government and various parties have started to apply information and communication technology to increase efficiency and transparency in the election process. One example is the use of an electronic voter information system (e-voting) or an electronic voting system (e-voting) which can replace the manual voting process at TPS. The application of technology in the village head election system can help speed up the process of updating voter data, improve data accuracy, and reduce the risk of fraud. In addition, technology can also enable voters to vote electronically through secure and encrypted platforms, thereby reducing the hassle and costs associated with manual voting at polling stations.

*Proposed System Analysis*

The analysis of the system proposed in this study can be seen in Figure 3. It can be seen that there are 3 entities, namely general users, in this case the voters, the village head election committee, and an independent institution, namely the Village Consultative Body (BPD). The three entities use an Android-based application system that is connected to the Application Programming Interface (API) as a bridge between the user entity and the server which contains program code, storage space, and system database.

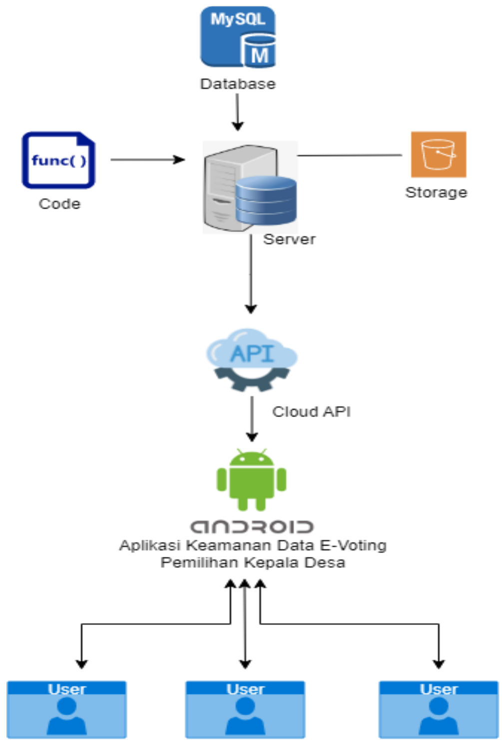



**Figure 3.** Model architecture

*Functional Analysis*

Functional requirements are all the processes carried out by the system and show the facilities needed in the system. Functional requirements also contain information that must exist and be generated by the system. The following are some of the functional requirements of the application that will be implemented as follows: The following is an analysis of input requirements for research:

**Table 1.** Input Needs Analysis

| User | Input Requirements |
|---|---|
| Independent Institution | - Independent institutions input email and password data to perform the login process. |
| | - Independent institutions input data on citizens who will exercise their voting rights by importing csv/xlsx extension files. |
| | - Independent institutions input email and password data for the committee login process. |
| | - Independent institutions input data on village head candidates. |
| | - Independent institutions input election data for the village head election process. |
| Election Committee | - The committee inputs email and password data to perform the login process. |
| Voters | - Voters input NIK and password data to perform the login process. |
| | - Voters input voting data to determine their voting rights in the village head election process. |
| | - Voters input PIN code data for verification when going through the election process. |

The following is an analysis of output requirements in this study:

**Table 2.** Output Needs Analysis

| User | Output Requirements |
|---|---|
| Independent Institution | - An independent organization reports on the results of the village head election. |
| Election Committee | - The committee prints the village head election result report. |
| Voters | - Voters view the village head election result report. |

The following is an analysis of the process requirements in this study:

**Table 3.** Analysis of User Needs

| User | Process Requirements |
|---|---|
| Independent Institution | - Independent institutions can perform the login process.<br>- Independent institutions can schedule the village head election process.<br>- Independent institutions can enter data on citizens who will exercise their voting rights.<br>- Independent institutions can enter data on village head candidates.<br>- Independent institutions can create a committee account.<br>- Independent institutions can view voter data.<br>- Independent institutions can view vote results. |
| Election Committee | - The committee can perform the login process.<br>- The committee can generate a QR code.<br>- The committee can view the vision and mission profile of the village head candidate<br>- The committee can perform the decryption process to view the vote result report.<br>- The committee can view voter citizen data. |
| Voters | - Voters can perform the login process.<br>- Voters can view citizen voter data.<br>- Voters can perform the process of selecting candidates.<br>- Voters can enter a PIN code for verification when going through the election process.<br>- Voters can view village head candidate data.<br>- Voters can view the vote results. |

*Non Functional Analysis*

Non-functional requirements are requirements that describe how the system will work in the future. In determining non-functional requirements is not easy, because you have to understand the characteristics and limitations of the system. Requirements specification involves hardware and software analysis as follows. The software needed in making this system is as follows android studio, visual studio codes, xampp, microsoftWord 2010, figma, mySql. The hardware needed in making this system is as follows and computer/laptop.

The computer specifications used are as follows intel(R) Core(TM) i5 CPU M350 @2.27GHz, 2.27GHz, random Access Memory (RAM): 4 GB, HDD : 500GB, VGA Intel(R) HD Graphics, screen resolution: 1280 x 800, android device. The required Android device specifications are as follows OS is Android 5.0 Lollipop, processor: isQualcomm MSM7225 chipset and Memory 64 GB ROM, 4 GB RAM.

*Logic Design*

UML or Unified Modeling Language is a visual modeling method that functions as a means of designing object-oriented systems. UML can also be said as a development, a modeling language in the field of software engineering which is intended to provide a standard way to visualize the design of a system. At this stage, the application begins to be designed using the UML (Unified Modeling Language) model which describes the existing structure of the application by considering the performance of the application built by the researcher. The following (Figure 4) is a display of use case diagrams in this study.


**Figure 4.** Vodes Use Case Diagram

*Discussion*

*Implementation*

The following is an implementation of the village head election e-voting data security application system using the AES-256 algorithm. The hardware used to operate the village head election e-voting data security application system using the AES-256 algorithm is laptop Acer Predator PH315-54, 11th Gen Intel(R) Core(TM) i7-11800H @ 2.30GHz (16 CPUs), ~2.3GHz, RAM 16GB, SSD 512GB, NVIDIA GeForce 3070. The software used in building the village head election e-voting data security application system using the AES-256 algorithm is android Studio Flamengo, visual Studio Code and XAMPP

*Backend Implementation*

Connection.js is a file that contains program syntax for configuring and establishing connections with databases. It implements a common approach that separates connection-related logic from the core logic of the application, allowing the management of connections to databases to be more centralized and structured.

In particular, it plays an important role in handling aspects of connecting and interacting with databases using MySQL. Through the use of MySQL, applications can store, retrieve, and manipulate data efficiently. However, by separating the connection logic into the Connection.js file, the application becomes more organized and easier to manage.

This principle is particularly useful in software development, as separating database connections from the main application logic helps avoid unnecessary code repetition and facilitates necessary connection fixes or changes throughout the application. With this file in place, managing access to the database can be done cohesively, and if at any point the database is replaced or reconfigured, only the Connection.js file needs to be modified without having to break the integrity of the entire application code.

The system is designed to operate using a JavaScript runtime based on Node.js. The app.js file acts as the main file used as the gateway to the system. In this file, you'll find a collection of code that manages the server, routes requests, applies middleware, and formulates the core logic of the system. When it comes to communication between the client and the server, an HTTP protocol connection is used.

However, more than that, the app.js file also takes on the responsibility of connecting various central functions in the system. This involves calling various modules or components that are necessary in carrying out the main functionality of the system. Hence, it acts as a control center that integrates and coordinates the various aspects required to run the application seamlessly.

With this structure, your application becomes more structured, manageable, and easy to organize. The separation between the main code in app.js and other functions in separate files makes it easier to develop, maintain, and fix bugs in the long run. The app.js configuration file can be seen in Figure 5.

```
const express = require('express')
const app = express()
const http = require('http').createServer(app)
const auth = require('./router/auth')
const daerah = require('./router/daerah')
const admin = require('./router/admin')
const panitia = require('./router/panitia')
const pemilih = require('./router/pemilih')
const deleteFile = require('./function/deletefiles')
//middleware
app.use(express.json({limit:'50mb'}))
app.use(express.urlencoded({extended:true}))
app.use('/public',express.static('./files'))
//router
app.get('/', (req, res)=>{
  res.json({
    status : 'connected',
    message : 'Vodes'
  })
})


app.use('/auth', auth)
app.use('/daerah', daerah)
app.use('/admin', admin)
app.use('/panitia', panitia)
app.use('/pemilih', pemilih)
require('./function/batasWaktu');
setInterval(() => {
  deleteFile.deleteFilesInput();
  deleteFile.deleteFilesQR();
 }, 60000);
http.listen(5000, ()=>{
  console.log('Server berjalan pada port 5000')
})
```

**Figure 5.** The app.js connection script

Encryption.js is a file that plays an important role in configuring the execution of each encryption and decryption process in the system. The module relied upon to carry out both processes is the AES-256-CBC crypto module. Aside from the encryption and decryption processes that utilize AES-256, extra steps are also involved in the form of encoding and decoding using base64. This encoding technique ensures that the encrypted data can be safely represented in a text format that can be transmitted over various communication channels.

The Encryption.js file also plays a role in providing the settings and parameters needed to configure the encryption algorithm, such as the secret key used to secure the data. With centralized configuration, the system becomes more organized and easier to keep secure.

In this context, the use of the AES-256-CBC crypto module and encoding and decoding using base64 form a solid security foundation. The encryption process protects the confidentiality of data by transforming it into a form that cannot be read directly, while the decryption process allows the data to be restored to its original form. The combination of strong encryption algorithms and careful encoding techniques is essential for maintaining the confidentiality and integrity of the information transmitted and stored in the system. The encryption.js file can be seen in Figure 6.

```
const crypto = require('crypto');
const fs = require('fs')


exports.decrypt = async (encryptedData)=> {
  try {
    const secretKey = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ123456'
    const iv = secretKey.toString().substring(0, 16);
    const decipher = crypto.createDecipheriv('aes-256-cbc',
secretKey, iv);
    let decrypted = decipher.update(encryptedData, 'base64',
'utf8');
    decrypted += decipher.final('utf8');
    return decrypted;
  } catch (error) {
    console.error('Error during decryption:', error);
    return null;
  }
}

exports.encrypt = async (data) => {
    try {
      const secretKey = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ123456';
      const iv = secretKey.substring(0, 16);
      const cipher = crypto.createCipheriv('aes-256-cbc',
secretKey, iv);
      let encrypted = cipher.update(data, 'utf8', 'base64');
      encrypted += cipher.final('base64');
      return encrypted;
    } catch (error) {
      console.error('Error during encryption:', error);
      return null;
    }
  };
```

**Figure 6.** File encryption.js

This research produces an Android-based application system for securing village head election e-voting data using the AES-256 cryptographic algorithm called Vodes. The application produced in this study was built using the Kotlin programming language on the Android frontend side by utilizing the Android Studio IDE as a tool in the development process. While on the backend side it uses the Javascript programming language using the Node js framework. The database used in the Vodes application uses MySQL. Basically the application built is an e-voting application for village head elections in general, but with the development of various features, especially on data security. The data that is entered, processed, and generated in this application almost completely goes through the encryption and decryption process using the AES-256 algorithm. Data security is not only on the backend side. But on the Android frontend there is also data security. Security on the backend by utilizing the library on Node js, namely the Node.js Crypto Module. Meanwhile, security on the Android frontend utilizes the Chiper class algorithm, which is available by default in Android Studio.

The Vodes application can be used in any village throughout Indonesia to simplify the village head election process. This application is used by three main entities, namely independent institutions, committees, and voters. An independent institution in this case is the Village Consultative Body (BDP) which has main access to enter data on citizens who will vote, enter village head candidate data, schedule Pilkades, and create committee accounts. The committee only has access to create an election QR code and receive a report on election results by first decrypting it by entering the token code. While the electorate entity, has access to embarrassment the process of voting or voting and see the results of the election votes. The way this application works when you want to carry out the election or voting process is by moving the QR code generated by the committee. If the QR code matches, then new voters will be able to carry out the voting process. You will then be asked to verify the PIN code to validate each village head's choice made by the voting entity. The voice data will be encrypted using the AES-256 algorithm. In addition, citizen data, candidate data, and election results data in the form of reports are also encrypted using AES-256.

*Citizen Data File Encryption Process*

The stages of the citizen data file encryption process use the AES-256 cryptographic algorithm. The entity entitled to carry out this process is an independent institution. The first stage that must be carried out by an independent institution is to input a citizen data file in xlsx format. The file will first be converted into a text file using the base64 encoding system. Then an automatic process will be carried out to input the secret key. In this case, the secretkey has been determined, which contains the text "ABCDEFGHIJKLMNOPQRSTUVWXYZ123456".

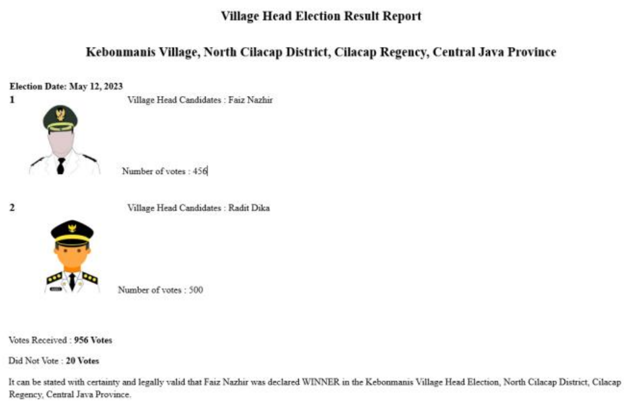
The next step is to do the AddRoundKey process. The AddRoundKey process is carried out by XOR operation between plaintext and secretkey. This encryption process consists of 4 types of transformation bytes, namely SubBytes, ShiftRows, Mixcolumns, and AddRoundKey. At the beginning of the encryption process or Round = 0, the input will undergo a byte AddRoundKey transformation. After that, the state will undergo a repeated transformation of SubBytes, ShiftRows, MixColumns, and AddRoundKey as much as Round = 13. If Round = 14, it will perform three transformation processes of SubBytes, ShiftRows, and AddRoundKey and will produce ciphertext. The encryption process is complete. All encryption data will be stored in the database.

The stages of the vote data encryption process when the voting entity conducts the village head election process using the AES-256 cryptographic algorithm. The voice data encryption process occurs on the Android and backend parts. The encryption process on the Android part is carried out to ensure data security when sending via the internet. The stages of the voice data encryption process are almost the same as in the process of encrypting citizen data files, the difference is that at this stage what is input as plaintext is text of type string data. Then an automatic process will be carried out to input the secret key. In this case, the secretkey has been determined, which contains the text "ABCDEFGHIJKLMNOPQRSTUVWXYZ123456".

The next step is to do the AddRoundKey process. The AddRoundKey process performs an XOR operation between the plaintext and the key. This encryption process consists of 4 types of transformation bytes, namely SubBytes, ShiftRows, Mixcolumns, and AddRoundKey. At the beginning of the encryption process or Round = 0, the input will undergo a byte AddRoundKey transformation. After that, the state will undergo a repeated transformation of SubBytes, ShiftRows, MixColumns, and AddRoundKey as much as Round = 13. If Round = 14, it will perform three transformation processes of SubBytes, ShiftRows, and AddRoundKey and will produce ciphertext. The encryption process is complete.

The stages of the process of decrypting all data use the AES-256 cryptographic algorithm. The decryption process in simple terms can be interpreted as a process to change back the form of disguised data that has gone through the encryption process into readable data. In this study, the decryption process begins by entering the ciphertext generated from the encryption process. In the system designed in this study, the intended ciphertext is in the form of a token code. The ciphertext will be merged with the same secretkey during the encryption process into one block by carrying out the AddRoundKey process. AddRoundKey is the process of adding ciphertext to the state by XOR operation with secretkey.

This decryption process consists of 4 types of transformation bytes, namely InverseSubByte, InverseShiftRows, InverseMixcolumn, and AddRoundKey. At the beginning of the decryption process or Round = 0, the state input will undergo a byte AddRoundKey transformation. After that, the state will undergo a transformation of InverseSubBytes, InverseShiftRows, InverseMixColumns, and AddRoundKey repeatedly as much as Round = 13. If Round = 14, it will perform three transformation processes InverseSubBytes, InverseShiftRows, and AddRoundKey and will produce plaintext or original data. The decryption process is complete. When the village head election process has been completed. The system will automatically generate a report in pdf format. Then the file will be encrypted first using AES-256. To see the results of the report, the user must decrypt it first.


**Village Head Election Result Report**

**Kebonmanis Village, North Cilacap District, Cilacap Regency, Central Java Province**

**Election Date: May 12, 2023**

1 Village Head Candidates : Faiz Nazhir

Number of votes : 456

2 Village Head Candidates : Radit Dika

Number of votes : 500

Votes Received : **956 Votes**

Did Not Vote : **20 Votes**

It can be stated with certainty and legally valid that Faiz Nazhir was declared WINNER in the Kebonmanis Village Head Election, North Cilacap District, Cilacap Regency, Central Java Province.

**Figure 7.** Report AFTER description

During the voting process, residents will vote for one of the village head candidates. The system will send the selected village head id for processing. Before the citizen's chosen data is sent to the backend via the API for processing, the village head's id data is encrypted first on the Android side. Then, the encrypted data is decrypted before being processed. After that, the system will automatically calculate incoming votes. Voice data will be encrypted first before being stored in the database. To process the voice data, the encrypted voice data will be decrypted first. Then after processing, the voice data will be encrypted again.

## Conclusion

Based on the results of this study, it can be concluded that an e-voting data security application for village head elections has been created using the AES-256 cryptographic algorithm. The application produced in this study has succeeded in properly securing all aspects of the data in the village head election process. Important data such as citizen data, village head candidate data, election results report data, and election vote acquisition data can be properly secured on the backend and frontend using the AES-256 cryptographic algorithm. The suggestion for the village head e-voting system is to develop a face recognition feature as verification for validation when selecting potential Pilkades candidates. In addition, it is necessary to develop security-related networks that are used to minimize digital attacks.

**Author Contributions**

Faiz Nazhir Amrulloh: conceptualization, methodology, initial draft preparation, formal analysis, and system development. Yuli Asriningtias: paper review and editing, validation, supervision, and resources.

**Funding**

This research did not receive funding from external parties.

**Conflicts of Interest**

The authors declare no conflict of interest.

## References

Anjarsari, I., & Andryana, S. (2020). E-Voting Application Security Using Web-Based Cryptography RSA type. *Jurnal MANTIK*, *3*(4). Retrieved from https://iocscience.org/ejournal/index.php/mantik/article/view/505

Cahyo, H. N., & Suryawinata, M. (2022). Responsive Web-Based E-Voting Information System. *Indonesian Journal of Innovation Studies*, *20*. https://doi.org/10.21070/ijins.v20i.739

Djuyandi, Y., Herdiansah, A. G., Yulita, I. N., & Sudirman, S. (2019). Using vote E-recapitulation as a means to anticipate public disorders in election security in Indonesia. *Humanities and Social Sciences Reviews*, *7*(5). https://doi.org/10.18510/hssr.2019.7515

Eka Putri, A., Kartikadewi, A., & Abdul Rosyid, L. A. (2021). Implementasi Kriptografi dengan Algoritma Advanced Encryption Standard (AES) 128 Bit dan Steganografi menggunakan Metode End of File (EOF) Berbasis Java Desktop pada Dinas Pendidikan Kabupaten Tangerang. *Applied Information System and Management (AISM)*, *3*(2). https://doi.org/10.15408/aism.v3i2.14722

Fischhoff, B. (2019). Evaluating science communication. *Proceedings of the National Academy of Sciences of the United States of America*, *116*(16). https://doi.org/10.1073/pnas.1805863115

Fitriani, I., & Utomo, A. B. (2020). Implementasi Algoritma Advanced Encryption Standard (AES) pada Layanan SMS Desa. *JISKA (Jurnal Informatika Sunan Kalijaga)*, *5*(3). https://doi.org/10.14421/jiska.2020.53-03

Guntur, M. (2020). Perancangan Sistem E-Voting Pemilihan Kepala Desa pada Kecamatan Teupah Selatan Kabupaten Simeulue. *Journal Informatic, Education and Management*, *2*(2). Retrieved from http://jurnal.stmikiba.ac.id/index.php/jiem/article/view/32

Hao, Y. L., Tian, C. L., & Yuan, Q. (2019). Improved meet-in-the-middle attacks on round-reduced crypton-256. *Journal of Cryptologic Research*, *6*(3). https://doi.org/10.13868/j.cnki.jcr.000309

Hasibuan, E. H., Nuary Singarimbun, R., & Harahap, B. (2022). Implementation of The E-Voting System in The Election of The OSIS SMA Dharma Pancasila Vocational School Based on Web Based Method Rapid Application Development (RAD). *Jurnal Infokum, 10(*2). Retrieved from https://infor.seaninstitute.org/index.php/infokum/article/view/451

Hidayat, F. (2020). Resistance to Maping Change : Penolakan Masyarakat Terhadap Rencana Pelaksanaan Pemilihan Kepala Desa (PILKADES) Berbasis Electronic-Voting di Kabupaten Sleman Provinsi Daerah Istimewa Yogyakarta. *Jurnal Ilmu Pemerintahan Suara Khatulistiwa*, *5*(1). https://doi.org/10.33701/jipsk.v5i1.890

Hu, S. D. K., Palit, H. N., & Handojo, A. (2019). Implementasi Blockchain: Studi Kasus e-Voting. *Jurnal Infra*, *7*(1). Retrieved from https://publication.petra.ac.id/index.php/teknik-informatika/article/view/8069

Indapwar, A. (2020). E-Voting system using Blockchain technology. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(3). https://doi.org/10.30534/ijatcse/2020/45932020

Noor, M. U. (2020). Implementasi Blockchain di Dunia Kearsipan: Peluang, Tantangan, Solusi atau Masalah Baru? *Khizanah Al-Hikmah : Jurnal Ilmu Perpustakaan, Informasi, Dan Kearsipan*, *8*(1). https://doi.org/10.24252/kah.v8i1a9

Nugroho, F. P., Abdullah, R. W., Wulandari, S., & Hanafi. (2019). Keamanan Big Data di Era Digital di Indonesia. *Jurnal Informa*, *5*(1). Retrieved from https://informa.poltekindonusa.ac.id/index.php/informa/article/view/65

Oprea, S. V., Bara, A., Andreescu, A. I., & Cristescu, M. P. (2023). Conceptual Architecture of a Blockchain Solution for E-Voting in Elections at the University Level. *IEEE Access*, *11*. https://doi.org/10.1109/ACCESS.2023.3247964

Pan, Y., Ge, X., Fang, C., & Fan, Y. (2020). A Systematic Literature Review of Android Malware Detection Using Static Analysis. *IEEE Access*, *8*. https://doi.org/10.1109/ACCESS.2020.3002842

Pandit, P., Bhawar, S., & Desai, P. M. (2014). Campus E-Voting for Android and Web Based Application. *International Journal of Emerging Engineering Research and Technology*, *2*(7). Retrieved from https://www.ijeert.org/pdf/v2-i7/13.pdf

Petitpas, A., Jaquet, J. M., & Sciarini, P. (2021). Does E-

Voting matter for turnout, and to whom? *Electoral Studies*, *71*. https://doi.org/10.1016/j.electstud.2020.102245

Prasetyawan, P., Rusliyawati, & Sari, D. (2018). Pengembangan Aplikasi Mobile E-voting Pilkades. In *Seminar Nasional Teknologi 2018*, (pp. 742-748). Retrieved from https://www.researchgate.net/publication/324694555_PENGEMBANGAN_APLIKASI_MOBILE_E-VOTING_PILKADES/link/5addab5e0f7e9b285941a1b0/download

Pratama, Y. W., & Kurniadi, D. (2021). Implementasi Blockchain dalam Aplikasi Pemilu. *Voteteknika (Vocational Teknik Elektronika Dan Informatika)*, *9*(3). https://doi.org/10.24036/voteteknika.v9i3.113787

Rachawati, D., Nurjaman, A., & Sihidi, I. T. (2022). Implementation of E-Voting in the Village Head Election (Pilkades) Selotinatah, Ngariboyo District, Magetan Regency. *Jurnal Public Policy*, *8*(1). https://doi.org/10.35308/jpp.v8i1.3812

Risnanto, S., Rahim, Y. A., Mohd, O., & Abdurrohman, A. (2022). E-Voting: Technology Requirements Mapping. *TEM Journal*, *11*(3). https://doi.org/10.18421/TEM113-37

Said, K., Kurniawan, A., & Anton, O. (2018). Development of media-based learning using android mobile learning. *Journal of Theoretical and Applied Information Technology*, *96*(3). Retrieved from https://www.jatit.org/volumes/Vol96No3/10Vol96No3.pdf

Simsir, I., & Mete, B. (2022). Digital Age of Human Resources Management. In *Special Human Resource Management Practices and Strategy*. Retrieved from https://acikerisim.subu.edu.tr/xmlui/handle/20.500.14002/1628

Siswanto, A. (2020). Pengamanan Transfer Data Pada Api Untuk Aplikasi E-Voting Menggunakan Algoritma Rsa. *Skanika*, *3*(4). Retrieved from https://jom.fti.budiluhur.ac.id/index.php/SKANIKA/article/view/2740

Verma, S., & Sheel, A. (2022). Blockchain for government organizations: past, present and future. *Journal of Global Operations and Strategic Sourcing*, *15*(3).. https://doi.org/10.1108/JGOSS-08-2021-0063

Wijayanti, A., & Chamdani. (2022). The Utilization of Information and Communication Technology in Industrial Relations Disputes Resolution in Indonesia. *Journal of Positive School Psychology*, *6*(2). Retrieved from https://www.journalppw.com/index.php/jpsp/article/view/3507/2286

Yi, H. (2019). Securing e-voting based on blockchain in P2P network. *Eurasip Journal on Wireless Communications and Networking*, *2019*(1). https://doi.org/10.1186/s13638-019-1473-6

Yulianton, H., Santi, R. C. N., Hadiono, K., & Mulyani, S. (2018). Implementasi Sederhana Blockchain. *Sintak*, 2. Retrieved from https://www.unisbank.ac.id//ojs/index.php/sintak/article/view/6635

Zhao, K., Cui, J., & Xie, Z. (2017). Algebraic Cryptanalysis Scheme of AES-256 Using Gröbner Basis. *Journal of Electrical and Computer Engineering*. https://doi.org/10.1155/2017/9828967