Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 42-48 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

E-Voting Application Security Using Web-Based Cryptography RSA type

Istiarati Ayustina Anjaswari[1], Septi Andryana[2], Aris Gunaryati[3]

[1,2,3]Informatika,Falkutas Teknologi Komunikasi dan Informasi, Universitas Nasional, Jl. Sawo Manila Kec Pasar Minggu, Jakarta Selatan, Indonesia

E-mail: ayuszahra@gmail.com, septi.andryana@civitas.unas.ac.id, aris.gunaryati@civitas.unas.ac.id

ARTICLE INFO

Articlehistory:
Received: 01/11/2020
Revised: 01/12/2020
Accepted: 01/02/2020

Keywords:
E-Voting, Youth South Manggarai, Private Key, Public Key, RSA Encryption

ABSTRACT

In 2017 we held the election of the chairman of the Youth South Manggarai in a conventional way, Which were displayed many members who did not came.There are many causes that are still unused ballots and the results of the voting are calculated Relatively long Also have a risk in the results of voting. With the existence of such contradictions, then to Utilize technology has been developed that makes the Electronic Voting author system.However application, the public did not trust e-voting, there will be manipulation of the results approved by each candidate. For that reason, the system can guarantee results of voting using RSA security, public key and private key to approve when you do the voting. Built using the method with waterfall SDLC. The validation test results concluded that the system is valid. Algorithm testing is done by the user entering the first odd value of 15 and the second odd value of 13 getting the value of m 168 and public key 169 from the calculation of the FPB the which is Relatively prime to m. If the public key is inputted Correctly then the user can vote.The voting results show that candidate # 2 has 32 votes, the candidate 1 has 20 votes and the others is non-voters.

1. Introduction

Voting is an election activities of small scale to large, in Indonesia usually marked in the election to vote langung President, Governors, Mayors, District, RW, RT until at least the low scale class president election. In this study, I took a case study of urban youth conclave southern Manggarai, Tebet, South Jakarta conducted once every 5 years. Each unit per Rw will propose one candidate as a candidate.

Electronic voting is a voting method using the latest implementation of electronic media such as android assistance and website. The purpose of the electronic voting is the voting process is very efficient, it does not cost to print ballots, the system can be used repeatedly.

Referring to previous research related to e-voting. First journal discusses the Design of Electronic Voting local elections Garut. This study makes the e-voting system local elections Garut. In this system the voter to login with the NIK number of each citizen. In the second journal that discusses the design of Web-based E-Voting. This study makes the selection of e-voting system of the RT. The system performs the registration by including NIK, Full Name and Password. Journal of Third namely Presidential Election Student Application STMIK Hang Tuah Android-Based Pekanbaru. This study makes the selection of e-voting systems STMIK Hang Tuah new head Pekanbaru built using the Java programming language, XML, PHP. The system performs the registration by entering the NIM,

Based on previous research the author wants to create a similar system that is e-voting by implementing security methods RSA algorithm (Rivest, Shamir, A'dleman) which is a type of cryptography in which to enter the name and public key previously made the same as that stored in the

Accredited "Rank 4"(Peringkat 4/S4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 42-48 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

database for verification purposes at the time wanted to do the voting.

2. Method

2.1. Research methods

Design applications using the System Development Life Cycle (SDLC) models waterfall,

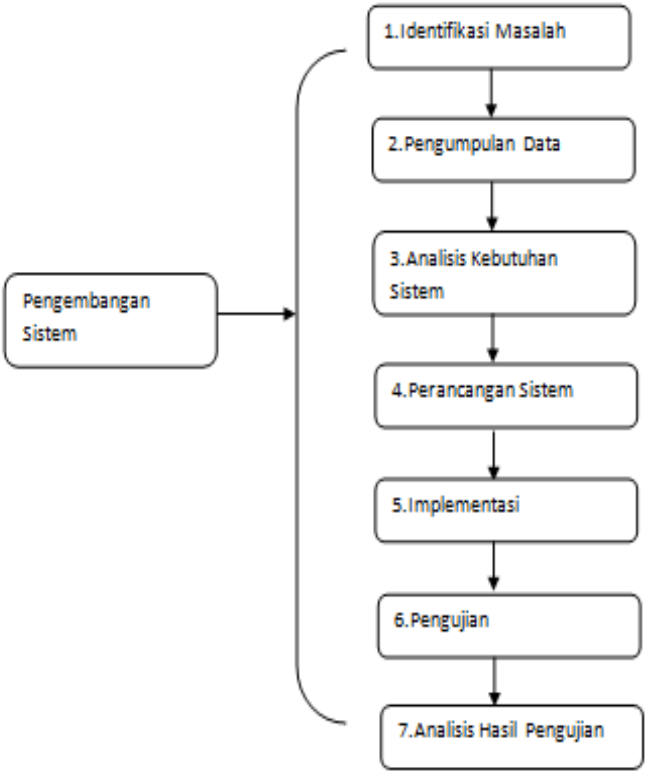

Figure 1. Phase manufacture Research

a) Identification of problems

The problem that exists is to vote in a manner that is conventional resulted in losses on the cost of printing ballots, security is not guaranteed, the risk of human error during the calculation results of the vote and require a relatively long time. With the above problems come solutions that make e-voting. Marzan A. Iskandar explained the purpose of electronic voting is the voting process is very efficient, it does not cost to print ballots, the system can be used repeatedly.

b) Data collection

Collecting data in this study using literature obtained from books and journals on similar research and interviews with the parties concerned.

c) System Requirements Analysis

Functional requirements are as follows:

1) Sound system can perform calculations in a short time and valid.
2) The system has a security system that guaranteed using the RSA algorithm.
3) The system can verify the password to the email notifications that have been inputted.

Non-functional requirements are as follows:

1) Can be used on a Windows operating system that has a web browser.
2) Using a MySQL database as the database server
3) Compatible on all web browsers.

Accredited "Rank 4"(Peringkat 4/S4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 42-48 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

2.2. Design Applications

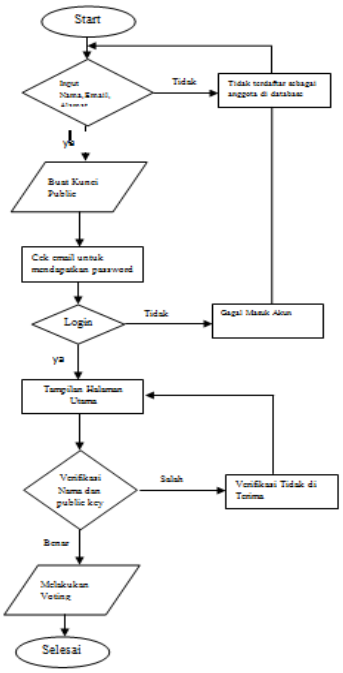

Figure 2. Application Development Phase

Figure 2 illustrates in research to make the application of e-voting for the election of the chairman of the youth manggarai south begins with registration by entering their name and email, if the name is written is registered in the database then the password will be sent via email, and members will be directed towards form makes public key for verification at the time of voting. After that the member can login by entering your name and password that has been in the can.

2.3. RSA algorithm

The RSA algorithm in this system is a cryptographic algorithm by incorporating public key which previously made the same as that stored in the database for verification purposes.

a) Enter two primes, say p and q.
b) Calculate m by the formula (P - 1) x (q - 1) .... (1)
c) Choose an integer for the public key, says his name e, relatively prime to m. The purpose of the relatively prime are (e, m) = 1.
d) To compute the private key d call his name, by the formula

$$d = \frac{1+(k \times m)}{e} \quad \text{.....} \quad \text{.....} \quad \text{.....} \quad (2)$$

By trying to value the different k = 1..2..3..dst to find the results of integer or nearly unanimous
Information :
d = the private key
k = integer 1..2..3 etc.
m = the calculation of the first equation
e = key public

3. Results and Discussion

3.1. The RSA algorithm implementation on the System

Accredited "Rank 4"(Peringkat 4/S4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 42-48 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

```
74      $Nama = $_POST["Nama"];
75      $p = $_POST["p"];
76      $q = $_POST["q"];
77      $n = $p*$q;
78      $m = ($p-1)*($q-1);
79      for($e=2;$e<=$m;$e++){
80      $gcd =gmp_gcd($e,$m);
81      if(gmp_strval($e,$m)=='1')
82      break;}
83      for($k=1;$k<1000;$k++){
84      $d = (1+($k * $m) ) / $e;
85      break;}
```

Figure 3. Syntax use the RSA algorithm

Figure 4. Display Generating Keys with RSA Algorithm

Figure 4 is to create a key with the RSA algorithm by entering the first prime number and prime number-2 which will be calculated by the system and will get the value of n, m, e, and d.

Figure 5. Key Data Display

Figure 5 Shows the result of the calculation of the RSA algorithm in which the p value, q, n, m, e and d.

Accredited "Rank 4"(Peringkat 4/S4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 42-48 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

1. User memasukkan nilai prima pertama,sebut saja p = 15.
2. User memasukkan nilai prima kedua,sebut saja q = 13.

Sistem melakukan perhitungan,sebut saja m dengan rumus :

m = (p-1) x (q-1)

m = (15-1) x(13-1)

m = (14) x (12)

m = 168

3. Untuk membuat kunci publik sebut e,sistem melakukan perhitungan looping dengan mencari nilai bulat yang relatif prima terhadap m.Dengan menghitung FPB(Faktor Persekutuan Terbesar) dari kunci publik dan m yang didapat bisa diketahui apakah kunci publik tersebut benar atau tidak.

E =169

FPB dari 168 & 169

168 =1,2,3,4,6,7,8,12,14,21...168

169 =1,13,169

⇨ Relatif prima terhadap m.Dimana (e,m) = 1

4. Untuk mencari kunci privat sebut d,sistem melakukan perhitungan dengan rumus.

$D = \frac{1 + (k \times m)}{E} = \frac{1 + (1 \times 168)}{169} = 169/169 = 1$

Figure 6. Calculation of RSA Algorithm Manually

Figure 6 Calculation Manual Describes the RSA algorithm, which results manually counted the same as the results in the system.

Figure 7. Display key Verification Form

Figure 7 Explaining after the Vote button click this form will appear, this page is useful to verify the public key, if the public key is entered exactly as previously calculated it will show the voting form.

Accredited "Rank 4"(Peringkat 4/S4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 42-48 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

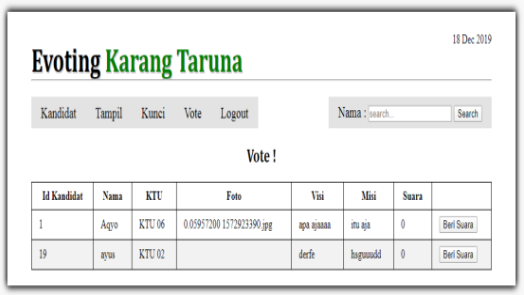

Figure 8. Display Voting Form

Figure 8 is a page after successful verification of the public key.User simply click the Vote button on the line candidates who want to be selected.

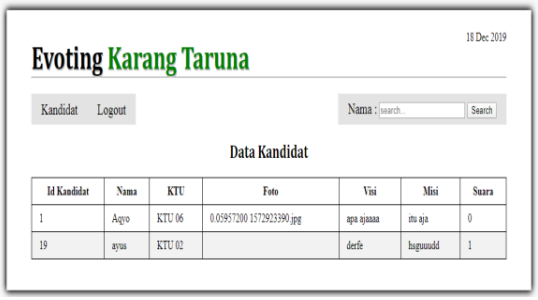

Figure 9. After Voting Display

Figure 9 is a page after voting. You can see the noise at the candidate number 19 turned into one voice.

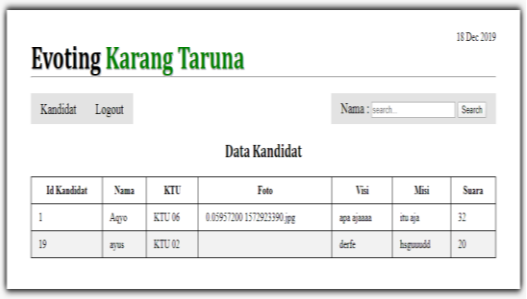

Figure 10. Display Voting Results

Figure 10 is a final calculation of 80 Members voting where only 52 members voting, 32 votes for the candidate number 1 and 20 votes for the candidate number 19.

3.2. Testing Using Blackbox

No.	Scenario	Test Case	Expected results	Test result	Conclusion
1.	Name and Password blank, click login	Name: (empty) password: (empty)	The system will reject and display a warning message	According to expectations	valid
2.	Name and Pass filled in, click login	Name: (Admin) password: (Admin)	The system receives the access log and display the main page of admin	According to expectations	valid
3.	Typing the name and e-mail, click on register	name: contents E-mail: contents	The system will send your password via email if names are duly registered in the database members	According to expectations	valid
4.	Typing the name and e-mail, click	name: contents	The system will not send your password via email if the name is not	According to expectations	valid

Accredited "Rank 4"(Peringkat 4/S4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 42-48 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

	on register	E-mail: contents	listed in the database is filled member		
5.	Typing the name and password in the form Login	name: contents E-mail: contents	The system will continue to form a key for	According to expectations	valid
6.	Names, Numbers 1 & Numbers odd odd 2 in the content and click save	Clicking save the data filled	The system will receive input data and calculate results using the RSA algorithm	According to expectations	valid
7.	Ote give to prospective candidates	Clicking Vote	The system will verify by entering a previously created key	According to expectations	valid

4. Conclusion

Based on the above discussion, it was concluded as follows:

a. E-voting can only be attended by members of the Youth South Manggarai course, by entering a name and email. If the name is entered in the database of members of the electorate will get the password in an email.
b. Implementation of RSA security algorithm in the system is valid and is used when going to the voting, which include the name and public key for verification purposes.
c. The system can send an email to the user's password login process.

5. Reference

[1]. Badan Pengkajian Penerapan Teknologi. Evoting untuk pemilu 2014. Available: https://www.bppt.go.id/.
[2]. Rahayu, Muludi,& Hijriani,"Journal of Information System Engineering and Business Intelligence.,Volume 2 Number 2,ISSN 2443-2555,Desember 2016.
[3]. Ariyus Dony,Pengantar *Ilmu Kriptografi Teori Analisis dan Implementasi*,Yogyakarta : CV Andi Offset, 2008.
[4]. Yusfar Ilhaqul Choer, Dede Kurniadi,"Rancang Bangun Electronic Voting Pemilihan Kepala Daerah Kabupaten Garut,"*Jurnal Algoritma Sekolah Tinggi Teknologi Garut*.,Vol. 14 No.2,ISSN 2302-7339.2017.
[5]. Sandi Septian, Hendry Fonda, Refni Wahyuni,"Aplikasi Pemilihan Presiden Mahasiswa STMIK Hang Tuah Pekanbaru Berbasis Android,"*Jurnal Ilmu Komputer(Computer Science Journal).*,Vol. 7 No.1,ISSN 2579 – 3918.2018.
[6]. Muhammad Ridwn, Zainal Arifin, Yulianti,"Rancang Bangun E-Voting Dengan Menggunakan Keamanan Algoritma Rivest Shamir Adlemn(RSA) Berbasis Web"*Jurnal Informatika Mulawarman*,Vol.11 No.2,ISSN 1858-4853.2016.
[7]. Rizki Andhestria Adhi, Harjono,"Developing E-Voting Information System SMS Based"*JUITA Jurnal Informatika*.,Vol. III No.2,ISSN 2086-9398.2014.
[8]. I Putu I Permana,I Ketut G Darma Putra,I Gusti M A Sasmita,"Rancang Bangun Sistem Pilkades Menggunakan Teknologi Smart Card Sebagai Kartu Pemilih"*Lontar Komputer Jurnal Ilmiah Teknologi Informasi*., Vol.7 No.2,ISSN 2088 – 1541.2016.
[9]. M. Hasim Siregar,"Rancang Bangun Pengembangan Aplikasi Pemilihan Presiden Mahasiswa Melalui SMS Gateway"*Jurnal Teknologi dan Open Source*.,Vol. 2 No.1,ISSN 2655 – 7592.2019.
[10] Nurul Azwati,"Perancangan E-Voting berbasis Web"*Jurnal Komputer Terapan*.,Vol.3 No.2(Dipublikasikan)