E-Voting Infrastructure System for Indonesia

Agustina Ampuni, Adi Fitrianto, Renaldy Indrajaya

***Abstract*: In digital era, Indonesia as democratic country needs to implement e-voting for presidential and governor election. Some countries have implement e-voting and two of them are more populated than Indonesia. E-voting can make voting process and vote distribution better. In this paper we proposed IT infrastructure for e-voting using load balancing, cryptography, and block chain. Also this proposed model can be discussed further about application and system replication to produce similar data from all servers.**

***Keywords*: E-voting, Infrastructure, Security, System**

I. INTRODUCTION

As a democratic developing country, Indonesia also uses the general election to determine the President and the People's Deputy. The election of Presidential Election has been conducted three times but the time for voting and vote counting process is approximately 6 weeks - 2 months and after that the process can be continued with handling Dispute Presidential election which takes more or less 2 month so that time to set President-elect less more reach 4 month [1]. Countries holding elections are already deployed with an E-voting system such as the United States, the vote counting and recapitulation process takes approximately one week with a population of 290 million people and other examples in developing countries such as India. The process takes only 1 month 15 days, the number of people in India reached approximately 1.1 billion if viewed from the data. Indonesia which has a population of approximately 240 million people [2] should be able to conduct the process of general elections E-voting.

In general, the way to choose is to use a way to cast or mark on ballot paper. However, as technology develops, there is another technique, namely electronic voting. Electronic voting is a method of voting by using electronic devices. The variety of electronic devices includes voter registration electronically, electronic vote counting and, later, including channels for remote picking, especially internet voting[3] .

However, the E-voting has problems especially on security such as data leakage, data manipulation and double voting. The problem is not only happened in the voting of E-voting but the still manual selection of votes is also experiencing the constraints so that this research will discuss about how to apply President Election in Indonesia by E-voting and how to maintain the security system so that society can be accepted and can solve the problems of President Election in Indonesia[4] .

Revised Manuscript Received on November 06, 2019.

Agustina Ampuni, Information System Management, Bina Nusantara, Jakarta, Indonesia. Email: agustinaampuni@outlook.com

Adi Fitrianto, Information System Management, Bina Nusantara, Jakarta, Indonesia. Email: adi.fitrianto2@gmail.com

Renaldy Indrajaya, Information System Management, Bina Nusantara, Jakarta, Indonesia. Email: renaldy.indrajaya@gmail.com

II. LITERATURE REVIEW

E – voting is a voting system where the data of the ballot is recorded and processed in form of digital information starts from voter registration until the election result is published [5].

E – voting can be classified into two types based on the vote casted [4] :

1**. Poll site**

Voters have to go to specific place and cast the ballot through available Direct Recording Electronic (DRE) devices on the location.

2. Remotely

Voters cast the ballot remotely through their owned Direct Recording Electronic (DRE) devices such as personal computer or mobile devices.

E – voting itself can give advantages as described below [6]:

1. Speeds up ballot calculation.
2. More accurate ballot calculation.
3. Reduce ballot printing cost.
4. Reduce ballot delivery cost.
5. Better access for disabled community.
6. Accessibility for people with limited time to visit poll.
7. Multilingual ballots.
8. Better information about candidates.
9. Better voter's requirement verification.

Despite of those advantages, e – voting can give some disadvantages and risk [7] such as :

1. High risk on large scale voting because it needs huge and high data communication.
2. Nobody can be blamed on cheating when frauds happened because most of e – voting system only ensure that each voter's vote counted.
3. An error vote can be untraceable.
4. Low anonymity.

There are e – voting requirements that required on e - voting [8] :

1. Privacy.

Voter's privacy has to be guaranteed during and until after election period for a long time span

2. Eligibility.

Voters must be on eligible criteria and registered by the rules of the election.

3. Uniqueness.

Voters can only give one vote for one of the candidates in the election.

4. Uncoercibility.

Voters must vote the candidate without any pressure from anybody and cast with their own heart.

5. Receipt-freeness.
In order to prevent buying and selling the votes, voters can't receive the receipt which can show and prove their choice of the candidates

6. Fairness.
The results must be displayed only in the end of the voting period, so there is no "currently leading" on the election period

7. Transparency.
The voting process have to be transparent. Tools such as bulletin boards can be used to show the election process

8. Accuracy.
Vote from voters cannot be edited, removed, or duplicated and all of the votes have to be counted

9. Robustness.
Any faction, parties, and authorities cannot interrupt and influencing election process and final tally. This must be ensured in order to increase the confidence of the election result although there are many ways fraud happens like registration committee may cheat by allowing ineligible voter to cast the vote, vote is represented by another or ineligible one.

Security standard must be ensured in order to make sure that the voters have confidence that the e – voting system will deliver their expectation securely and privately, and vote can only be casted once by the eligible voters [9]. Security challenges faced in e-voting such as any successful attack and hacking activity would be very high profile. The worst case would come from someone who motivated by the ability to manipulate the votes result without anybody notices it. [9]

Security attack of e-voting that can happen[10] are:

1. Hacking from electronic media
2. Attack using malicious software

Nowadays, e-voting technology tools is being developed. But, the issues of this technology is about the voters eligibility verification and virus like Trojan Horse[10].

In Indonesia, e – voting has been implemented on village chief election in Jembrana, Bali. This e – voting has showed cost efficiency and high participation of the voters. According to the case and result, the e - voting itself can be described as successful vote [11].

III. PROPOSED INFRASTRUCTURE MODEL

This journal uses double-blind review process, which means

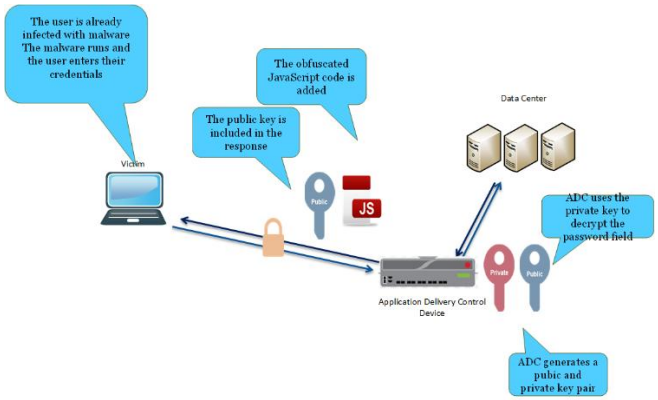

Fig. 1 E-Voting Security Mechanism

Figure 1 above shows security mechanism that designed to prevent data leakage when the device that is used is infected by malware is described below:

1. When user votes, then it will do request to web server that available at data center by using ADC device.
2. ADC device will generate public key and private key that will be used to encrypt the data.
3. ADC Device will distribute the request that made by user by using javascript that will ensure that the user is not a bot and the public key will be delivered at the same time together with the javascript.
4. User then input username and password to the system, then vote for candidates and will send it back to server through ADC device.
5. ADC device will decrypt using the key that has been generate.
6. This method is safe because malware will only get username and password including public key so when it is decrypted by the hacker, it will be failed because they don't have the private key [12].

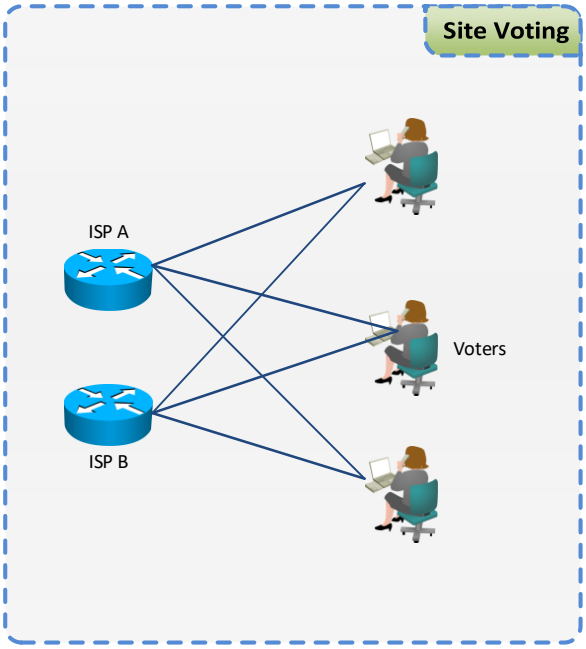

Fig.2 E-Voting Poll Site Simulation

Figure 2 describes how voters will vote on poll site. For the infrastructure, two routers that support GSM will be available on voting site. That is used to connect the SIM card to network. These routers will used two different GSM with one of it as backup. In the implementation, the router also supports wifi network so the only portable PC like notebook is enough. We choose to use poll site voting because remote voting is having higher risk of fraud like privacy issues and can lead coercion to candidates by the environment [3]. If it happens, the requirement of e – voting [8] is not fulfilled. It also opposed Indonesia election principles.

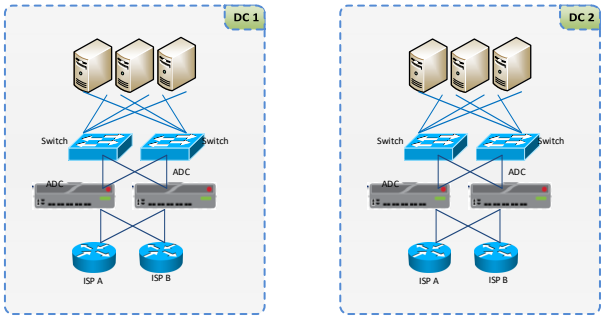

Fig.3 E-Voting Data Infrastructure

Figure 3 shows data infrastructure. Data center that will be built will support block chain concept. There will be more than one data center and there will be some servers on every data center so the voting will be smooth because the server will always on good network. The ADC device will do load balancing to every single data center and every single server that will be used so every server will have same load. Every data that is stored will be replicated when the vote is done.

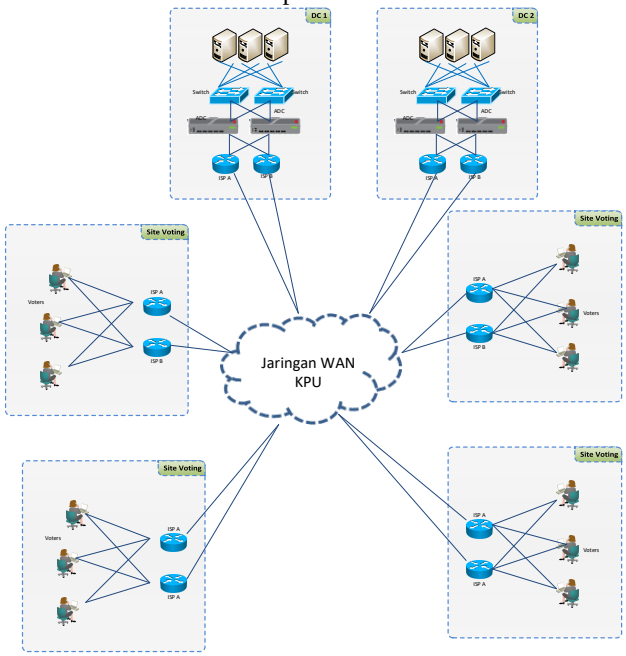

Fig.4 E-Voting Proposed Model

Figure 4 shows the design of data, network and infrastructure that proposed on this paper. It described that every poll site will be connected to Indonesia Election Commissioner WAN. The WAN will be used to distribute vote data to each server where the vote will be stored

IV. CONCLUSION

The infrastructure designed in this paper can help to secure data from elections by e-voting. In addition the concept of this paper also allows high network availability because it has load balancing and redundant concepts. From this research is expected the concept of network infrastructure and its security is realized, and the concept for software system, server, and others can be developed also in the future so that can be integrated and realize the process of e-voting in the selection process in Indonesia

REFERENCE

1. "KPU - Portal Publikasi Pemilihan Umum 2019." [Online]. Available: https://infopemilu.kpu.go.id/. [Accessed: 19-May-2018].
2. "Population Clock: World." [Online]. Available: https://www.census.gov/popclock/world/id. [Accessed: 19-May-2018].
3. D. Gritzalis, "Secure Electronic Voting: New trends, new threats, new options," 7th Comput. Secur. Incidents Response Teams Work., 2002.
4. A. Riera and P. Brown, "Bringing Confidene to Electronic Voting," Electron. J. e-Government, vol. 1, no. 1, pp. 43–50, 2003.
5. M. K. Wisnu, Dyah A. M. G., Aswin Suharsono, S.T., M.T., M.Kom., Denny S. R., S.Kom., "Rancang Bangun Sistem E-Voting Dengan Menerapkan Hash Dan Digital Signature Untuk Verifikasi Data Hasil Voting," Progr. Stud. Inform. Progr. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya Malang, 2012.
6. A. Rokhman, "Prospek dan tantangan penerapan e-voting di indonesia," Semin. Nas. Peran Negara dan Masy. dalam Pembang. dan Masyrakat Madani di Indones., pp. 1–11, 2011.
7. H. T. Liaw, "A secure electronic voting protocol for general elections," Comput. Secur., vol. 23, no. 2, pp. 107–119, 2004.
8. O. Cetinkaya and D. Cetinkaya, "Verification and validation issues in electronic voting," Electron. J. e-government, vol. 5, no. 2, pp. 117–126, 2007.
9. B. ΜΕΛΠΟΜΕΝΗ, Γ. ΘΟΔΩΡΗΣ, and K. ΣΠΥΡΟΣ, "Procedural Security and Social Acceptance in E-Voting," Proc. 38th Annu. Hawaii Int. Conf. Syst. Sci., vol. 00, no. C, p. 118a–118a, 2005.
10. Kundiana, "Tinjauan Implementasi Teknologi E-Voting di US dengan di India." 2004.
11. M. L. Anistiawati, "Implementasi Kebijakan Penerapan Elektronik Voting Dalam Pemilihan Kepala Desa," Citiz. Chart., vol. 1, no. 2, 2012.
12. Y. Mu and V. Varadharajan, "Anonymous secure e-voting over a network," Proc. - Annu. Comput. Secur. Appl. Conf. ACSAC, vol. Part F1347, pp. 293–299, 1998.