FINGERPRINT-BASED AUTHENTICATION AND CRYPTOGRAPHY IN AN E-VOTING SYSTEM

Tohari Ahmad
Teknik Informatika ITS, Kampus ITS Surabaya, tohari@if.its.ac.id

Anik Hanifatul Azizah
Teknik Informatika ITS, Kampus ITS Surabaya

Hudan Studiawan
Teknik Informatika ITS, Kampus ITS Surabaya

Abstrak

Voting telah menjadi bagian penting dari demokrasi. Terdapat beberapa faktor yang harus dipenuhi agar proses voting dapat dilaksanakan dengan baik. Misalnya, otentikasi pengguna, yaitu hanya mereka yang benar-benar memenuhi syarat saja yang boleh mengikuti proses voting tersebut; keamanan data, yaitu data yang dikirimkan untuk proses voting harus bersifat rahasia. Sistem voting secara manual bisa memenuhi persyaratan tersebut, akan tetapi penggunaan sistem voting secara elektronik (*e-voting*) bisa menjadi suatu alternatif. Dengan penggunaan e-voting, diharapkan proses yang dilakukan bisa lebih transparan dan bisa lebih mudah untuk memenuhi persyaratan yang ada. Dalam makalah ini, kami mengusulkan penggunaan biometrik, khususnya sidik jari, sebagai media untuk melakukan otentikasi; dan kriptografi kombinasi kunci privat dan publik untuk menjada kerahasiaan data. Tidak seperti PIN (*personal identification number*) atau kata sandi (*password*), sidik jari relatif sulit dipindahtangankan atau bahkan dipalsukan. Di sisi yang lain, kriptografi kunci privat digunakan untuk menjaga kerahasiaan data, sedangkan kriptografi kunci publik digunakan untuk menjaga kerahasiaan kunci privat. Selain itu, desain arsitektur e-voting juga diusulkan. Evaluasi dilakukan, terutama untuk mengetahui tingkat akurasi proses otentikasi dan juga waktu yang diperlukan untuk melakukan otentikasi, enkripsi dan dekripsi terhadap data. Berdasarkan uji coba yang dilakukan, didapatkan bahwa waktu yang diperlukan relatif tinggi, yang dipengaruhi oleh banyak faktor, seperti spesifikasi komputer yang digunakan.

Kata Kunci: keamanan data, otentikasi, kriptografi

Abstract

Voting has played an important role in the democracy. There are some factors must be met to make the voting process running well. For example, the authenticity of the users, this means that only they who fulfill the requirements are granted access to participate in the voting process; data security, which means that the data sent during voting process must be protected. A manual voting system may be able to meet those requirements, however, an electronic voting (e-voting) system can be an alternative. By implementing e-voting, the process may be more transparent and makes it easier to fulfill the requirements. In this paper, we propose to use biometrics, particularly fingerprint, to be a medium for authenticating users; and private and public key cryptography for securing the data confidentiality. It is more difficult for attackers to transfer, distribute or even forge fingerprint than PIN (personal identification number) or password. In addition, private key cryptography is used for protecting the data, while public key cryptography is for securing the key of the private cryptography. Furthermore, architecture of e-voting is also presented. The evaluation is performed, especially to measure the acccuracy level of the authentication; and the time taken for this authentication process as well as encryption and decryption of the data. According to the experimental result, it can be inferred that the time taken is relatively high. In fact, it is affected by various factors, for example, the specification of the computer being used.

Keywords: data security, authentication, cryptography.

INTRODUCTION

A voting system has been a popular mechanism to elect someone from a group of people. This has been implemented in various levels of government, from a local district to have a mayor, to national-wide election to have members of house of representative of even a president. All these election levels must comply with the voting requirements which include confidentiality, integrity and anonymity [1] [2]. In addition, there are some factors should be considered. For example, accuracy, reliability and the counting speed.

A manual voting system, however, which is widely implemented in many countries, may be hard to meet those requirements. This is because, the ballots are counted manually which can lead to inaccuracy of the result as well as relatively long time taken before the result is obtained. This condition may affect the reliability and confidence levels of the respective election system.

In order to overcome this problem, an electronic voting system is proposed. This employs devices, called DRE (Direct Recording Electronic), on where the voters put their vote. In a certain level, some countries have implemented this e-voting system [3]. In Indonesia, the possibility of e-voting is also investigated [4].

Nevertheless, the implementation of e-voting does not fully solve the problem. There are some weak points which can be exploited by attackers to compromise both the sytems and the voting result. For example, (1) the authenticity of the users where only authorized users who are able to deliver their vote; (2) the confidentiality of voting data being sent to the server. In this paper, we develop an e-voting system which provides protection to both authenticity and confidentiality by implementing fingerprint-based authentication and cryptography.

The rest of this paper is organized as follows. Section 2 provides the related works. Section 3 describes the proposed method along with its architecture. The analysis and conclusion of the proposed method are presented in section 4 and 5, respectively.

RELATED WORKS

Authenticity

Practically, e-voting can be implemented in many ways. In terms of authentication, the main principle must be fulfilled is that only authorized users are allowed to give their vote. The terms *authorized users* means that:

- Users who have met the requirements and been registered in the system.
- Users who have not deliver their vote; this means that a user must not vote more than once.

In order to only allow authorized users, the system has to verify the user identity and their status (as specified before) at the beginning. Therefore, there must be a mechanism which is able to do verification accurately.

There are some types of verification have been proposed which can be classified into three groups [5]. Those are: what the users have, what the users know and what the users are. The first deals with something belongs to the users, such as token. The second is about what the users remember, such as password or PIN number; while the last relates to the characteristics or activities of the users. Overall, each of those methods has strength and weakness. Which method is approriate to implement depends on the characteristics of the respective system.

Biometrics, which is part of the third group, is relatively harder to forge than the other two groups. Its accuracy, however, is likely less than 100% [6]. This is because, the features obtained from biometrics may slightly change, although the biometrics itself is not. How high its accuracy level is determined by the system administrator, since there is a trade-off between the accuracy and convenience. This means that more secure, less convenient it is, and vice versa. Because of its permanence characteristic, the biometric data itself should be well protected. Therefore, in the worst case that it is compromised, the data is still secure.

Confidentiality

Confidentiality of the data is commonly protected by a cryptographic algorithm, where the data is encrypted before being sent to the destination. In addition, the security of the data also relies on the architecture of the system, that is, inappropriate use of a strong cryptography in the system may result to unsecure data. Therefore, both cryptography and the system architecture design are important from the security point of view.

There are some architecture designs of the systems which have been researched. In [7], Ahmad et. al propose to use two counting machines. Two main purposes of this design is to provide confidentiality of the ballots and reliability of the system. The voting result obtained by one machine must be exactly same as that of another. So, it is more difficult for an attacker to compromise the system. Furthermore, this can also be a hindrance for the insider to commit attack.

In the architecture design of [7], all communication to the user (voter) is done by the administrator. Later, the administrator is responsible for delivering the vote of each user to both counting machines whose result is made public once the whole process has finished. In practice, the authenticity of the system is also validated by using a digital certificate issued by a certificate authority. In general, those parties involved in a voting process are also described in [8] [9].

The research in [5] presents a challenge-response protocol for authenticating users. It explores the features available in the client, including MAC address. It is worth to note that this design uses mobile devices for the voting process. Despite common limitation of the devices, the research has made it easy for people to send their vote.

In terms of confidentiality, there are many methods have been described. In [8], Yi et. al propose to use Modular Square Root (MSR) for securing the data. It is believed that less complex the algorithm, more appropriate it is to implement because it reduces the computation and may increase the speed of the process. Some analysis of the proposed system has also been done in terms of its security.

Different from it, Ahmad et. al [7] introduce the use of elliptic curve cryptography (ECC) for encrypting the data. For a comparison purpose, they also implement AES and ECC for securing the ballots and the AES key, respectively. The experimental results depict that the proposed method is acceptable to implement. Slightly different from this method, the research in [5] implements RSA to protect the data sent by clients to the server. Here, all clients encrypt that data by using the same public key of the server. In spite of its relatively long key, RSA is still the factual standard in the public key environment. Therefore, that research implements this algorithm. Furthermore, not only the ballots are encrypted, but also other related data, such as the identity of users and response obtained from the previous challenge.

The general process of encryption/decryption is presented in Fig. 1, where plain text and cipher text are the data before and after being encrypted, respectively. These encryption and decryption processes are performed by using respective key pair, depending on whether its cryptographic algorithm is symmetric or asymmetric cryptography.

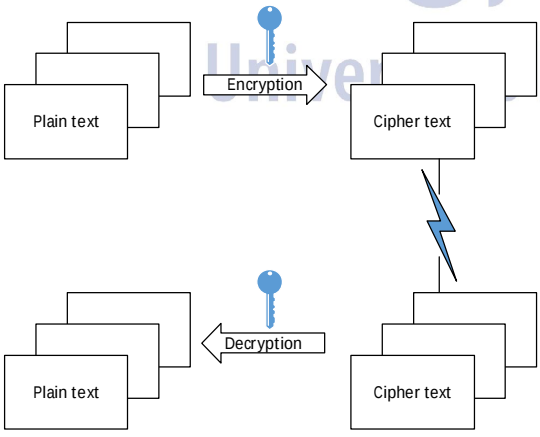

Figure 1General process of encryption - decryption

PROPOSED METHOD

The general process of the proposed method is presented in Fig.2. In this design, the users must be firstly authenticated, so that, only authorized users are able to vote. Once passing the verification, they are authorized to vote whose data is stored in the database. Finally, the tallying is performed to have the e-voting result.

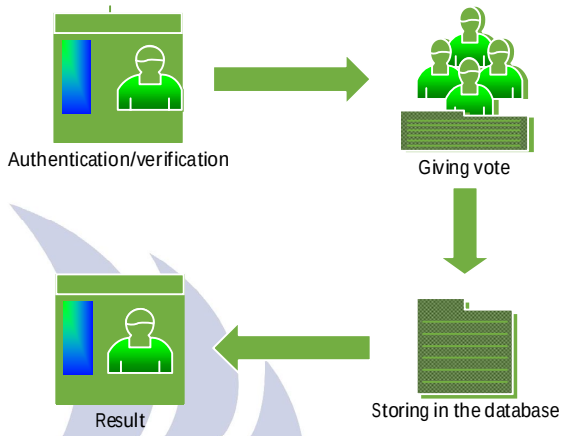

Figure 2 Architecture of the e-voting

Fingerprint-based authentication

Firstly, fingerprint features are extracted. This includes some steps, namely: binarization, thinning and minutiae extraction. Once the features have been obtained, they are stored in the database for later verification use. It is assumed that administration checking, such as minimum user age, is also done at this step. This includes the users eligibility according the respective voting system. So, the existing administration verification must still be done. Secondly, the same step as the previous is performed whose result is compared to the one in database. If it matches, then the user is granted an access to the system, otherwise the authentication result fails. The general diagram of this authentication is presented in Fig. 3.

In practice, the access granting to the user not only depends on the matched fingerprint data, but also other consideration. For example, the status of whether the user has already given the vote, so that, duplicate vote can be avoided. Therefore, in this case, the use of fingerprint-based verification is complement to the existing procedures.

Protecting data

The data sent from a client to the server is protected by a cryptographic algorithm. In this case, this data is encrypted by using AES whose key is protected by RSA. The flow of the process is described in Fig. 4. This makes it easy for the system to distribute the AES key from the server to the client.

The ballots consists of identity of voters and candidates. This data is concatenated before being encrypted and sent

to the server. Once received by the server, this resulted data is parsed and delivered to the tallying machine.

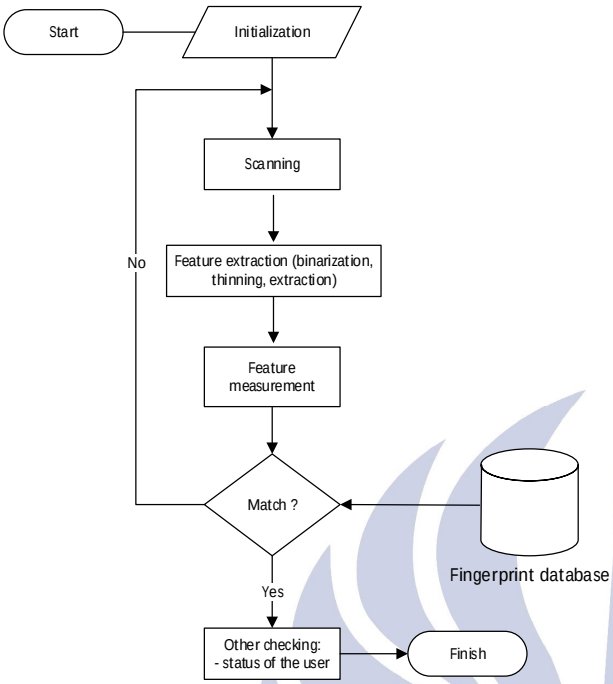

Figure 3 General process of the authentication

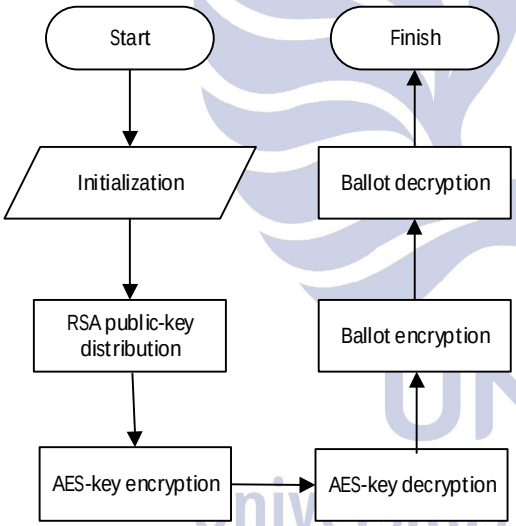

Figure 4 Protecting data

EXPERIMENTAL RESULT

The fingerprint-based authentication is implemented by using available SDK (software development kit) [10]. The implementation is evaluated by using data set obtained from FVC2002DB2 [11]. There are 10 pairs of fingerprint image in the experiment.

This fingeprint-based authentication is measured based on the true positive rate (TPR) and false positive rate (FPR). The first is the proportional number of images can be successfully verified. It is to measured how accurate the method in verifying legitimate data. The comparison is done between those fingerprint image pair. So, there are 10 comparison is performed. The second is that of a fingerprint image compared to other fingerprint images. It is to evaluate the capability the system in recognizing non legitimate data. From this FPR evaluation, there are 90 comparison is carried out. Both TPR and FPR evaluation can be depicted in Fig. 5 and 6 as well as eq. 1 and 2, where *T*, *F* and *N* are the number of image successfully matches its pair, the number of image successfully matches different pairs, and the number of comparison, respectively.

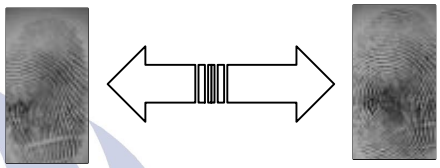

Figure 5 Comparison of images in a pair

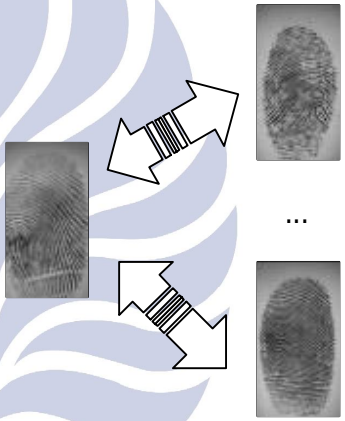

Figure 6 Comparison of images in different pairs

$$TPR = \frac{T}{N} \text{x } 100\% \quad (1)$$

$$FPR = \frac{F}{N} \text{x } 100\% \quad (2)$$

Based on the experiment, it is found that TPR and FPR are 90% and 2.3%, respectively. This means that the system is able to recognize about 90% of legitimate users; and has capability to detect about 97.7% of illegitimate users.

In terms of speed, each fingerprint matching requires about 9 seconds. It is relatively high, considering that in practice, the number of users may significantly grow. Furthermore, this may also affect the user acceptance of the system. Nevertheless, this value depends on many factors, such as the specification of both client and server, the connection between client and server, and the number processes running on the that time. Practically, those factors (capability of client-server as well as the connection) should be improved along with the growth of

the number of users. Overall, this value should be decreased as low as possible.

In terms of encryption and decryption processes, the time taken is respectively 5.8 and 7.5, on average. These values include data concatenation (for encryption) and data separation (for decryption). Similar to that of the authentication process, the time taken for encryption and decryption processes is relatively high, even though these values are also affected by some factors.

CONCLUSION

This paper has presented an e-voting system which is developed by considering two main properties in the computer security: authenticity and confidentiality. The first is constructed by fingerprint-based method, while the second is by implementing cryptographic algorithms.

Despite its speed, the system has been able to provide authentication and confidentiality of the data. In practice, the system should be implemented in a high performance computing machine which is able to do better computation.

REFERENCES

[1] B. I. Simidchieva, M. S. Marzilli, L. A. Clarke dan L. J. Osterweil, "Specifying and verifying requirements for election processes," dalam *2008 international conference on Digital government research*, 2008.

[2] M. Volkamer dan M. McGaley, "Requirements and Evaluation Procedures for eVoting," dalam *The second international conference on Availability, reliability and security*, 2007.

[3] A. H. Trechsel dan F. Breuer, "Voting: E-voting in the 2005 local elections in Estonia and the broader impact for future e-voting projects," dalam *International conference on Digital government research*, 2006.

[4] *Jembrana told to prepare for e-voting*, The Jakarta Post, 2010.

[5] T. Ahmad, H. Studiawan, I. Aryadinata, R. M. Ijtihadie dan W. Wibisono, "Challenge Response-based Authentication for a Mobile Voting System," dalam *To be presented in International Conference on Electrical Engineering and Technology*, Tokyo, Japan, 2014.

[6] T. Ahmad, J. Hu dan S. Wang, "Pair-polar coordinate-basedcancelablefingerprinttemplates," *Pattern Recognition*, vol. 44, no. 2011, p. 2555–2564, 2011.

[7] T. Ahmad, J. Hu dan S. Han, "An Efficient Mobile Voting System Security Scheme based on Elliptic Curve Cryptography," dalam *Third International Conference on Network and System Security*, GoldCoast, Australia, 2009.

[8] X. Yi, P. Cerone dan Y. Zhang, "Secure Electronic Voting for Mobile Communications," dalam *Vehicular Technology Conference*, 2006.

[9] G. Schryen, "Security aspects of Internet voting," dalam *37th Annual Hawaii International Conference on System Sciences*, 2004.

[10] AFIS, "Fingeprrint data set," AFIS, 2009.

[11] FVC2002DB2, "Fingeprint verification competition," 2002.