TokenVote: Secured Electronic Voting System in the Cloud

Fahad Alsolami
Department of Information Technology
King Abdulaziz University , KSA

***Abstract*—With the spread of democracy around the world, voting is considered a way to collectively make decisions. Recently, many government offices and private organizations use voting to make decisions when the opinions of multiple decision makers must be accounted for. Another advancement: cloud computing attracts many individual and organizations due to low cost, scalability, and the ability to leverage big data. These considerations motivate our proposal of the TokenVote scheme. TokenVote is an electronic voting system in the cloud that uses revocable fingerprint biotokens with a secret sharing scheme to provide privacy, non-repudiation, and authentication. The TokenVote scheme spreads shares of secret (vote), embeds them inside the encoding biometric data (i.e. fingerprint), and distributes them over multiple clouds. During the voting process, each voter must provide his/her fingerprint, causing the TokenVote scheme to collect all voting shares from all voters to compute the final voting result. TokenVote does cloud parallel computing for the voting process in an encoded mode to prevent disclosure of the shares of voting and the fingerprint itself. Our experiments show that TokenSign has a significant performance and comparable accuracy when compared with two baselines.**

***Keywords*—Cloud; Fingerprint; Voting; Security**

I. Introduction

With the worldwide spread of democracy, voting is no longer an alternative; it is a necessity. The importance of voting is recognized by many individuals, organizations, and countries, not only for presidential elections, but also for making decisions in organizations. Making decisions within organizations has been made more difficult since many decisions must be made through consensus rather than by a single decision maker [1] [2]. Rather than allowing a debate in a meeting to continue unresolved for a long time, people can make use of an electrotonic system to speed up the process. Many electronic voting systems have been introduced in literature. Gibbard [3] proves the conjecture by proving a game theory where a voting scheme is a game form and individual actions are strategies, while Sako et al [4] proposes a voting scheme that proves a receipt-free system. For secure electronic voting system, Fujioka et al [5] proposes a secure voting scheme where the scheme ensures that no one can disclose the intermediate voting result. In addition, Peralto et al [6] proposes a computerized voting system that can identify participants and prevent duplicated and fraudulent voting.

Despite the great advantages of electronic voting systems, security and privacy are serious problems for voters and organizations/administrations. Thus, many electronic voting schemes are proposed in literature to provide security and privacy. Okamoto [7] proposes a secured voting scheme which solves fairness, anonymity, receipt, and privacy. Lee et al [8] proposes an electronic voting protocol that achieves receipt-freeness. Bannet et al [9] presents a voting system that demonstrates many bugs that can occur in a voting system. Other voting systems using biometrics data for authentication purposes have also been proposed [10] [11] [12] [13] [14]. Some use fingerprint data, while others use both fingerprint and face recognition. Other schemes use a secret sharing scheme [15] to distribute the voting secret among all voters [16] [17] [18]. Even though these schemes have solved many issues in electronic voting system, other issues remain research challenges.

In this paper, we propose the TokenVote scheme, which provides security and privacy for both voters and administrations. TokenVote scheme has multiple purposes, such as presidency elections, organizations elections, and formal meeting decision-making in both government and private organizations. Specifically, our contribution is to design, implement, and evaluate a TokenVote scheme that uses the revocable fingerprint biotokens (Biotope) [19], Bipartite token [20], and the secret-sharing scheme [15]. During the enrollment process, TokenVote encodes the biometric data (i.e. fingerprint). Then, TokenVote embeds a shared secret (i.e. voting) inside the encoded fingerprint data. TokenVote then distributes all shares of a vote over multiple clouds, so no single cloud stores the threshold required to recover the result of a vote. During the voting process, TokenVote matches the fingerprint data of voters in encoded mode, then computes the final voting result. This whole process being conducted in encoding form which provides security and privacy for voters. On the other hand, voters must provide their fingerprint data to vote which provides non-repudiation and authentications for administrations.

The rest of this paper is organized as follows: in section II, we briefly describe previous related work. The objectives of TokenVote are given in section III. Our proposed TokenVote algorithm is presented in section IV. In section V, the description of the experimental design is given. The experimental evaluation and results are provided in section VI. Finally, the conclusion is drawn in section VII.

II. Background

A. Voting system and security concerns

A great deal of literature has been devoted to designing a voting system that satisfy all purposes. Gibbard [3] proves the conjecture by proving a game theory where a voting scheme is set up in a game form and individual actions are strategies. The author discusses manipulation in a voting system and how to prove it. Fujioka et al [5] proposes a secure

voting scheme that provides privacy for voters, ensuring voting fairness. The scheme ensures that no one can disclosure the intermediate voting result. Sako et al [4] proposes a voting scheme that proves to be receipt-free, so voters can hide their votes from a powerful adversary. To achieve their goal, they replace the physical voting booth with a hardware assumption. Peralto et al [6] invents a computerized voting system that can identify participants and prevent duplicate and fraudulent voting. Jakobsson et al [21] proposes a new solution that provides proof of correct operation of the voting system. They use randomized partial checking to check the subset of input/output data instead of completely correct operation. However, to provide secure voting system, Okamoto [7] proposes a secured voting scheme that solves fairness, anonymity, receipt, and privacy. To achieve its goal, the scheme has four steps: authorization, voting, claiming, and counting. Lee et al [8] proposes an electronic voting protocol that achieves receipt-freeness. Bannet et al [9] presents a voting system to demonstrate many bugs that might occur in a voting system.

B. Using Biometric Authentication in Voting System

Authentication in a voting system proves that the participant giving his/her vote is the right person. Many researchers discuss the use of biometrics data as authentication tools in voting system. Ahammad et al [14] proposes an electronic voting machine based on fingerprint identification to provide security for voting system. Their system consists of four phases: enrollment, voting, election result demonstration, and database restoration. In enrollment phase, voters enroll their fingerprint data in the voting system to do matching in voting phase when voters come to vote. In the election result phase, the voting system calculates all votes; in the database restoration phase, the system deletes the current voting result for next voting event. Hof [12] proposes electronic voting with biometric authentications. They evaluate all biometrics (fingerprint, iris, face etc.) against another authentication tool, like a password or card. They also discuss the security issues related to biometric data. Kumar et al [10] proposes an electronic voting system based on fingerprint authentication. Their system requires successful matching of fingerprints to vote. Kumar et al [13] proposes a framework for electronic voting that maintains authentication security using fingerprint. Najam et al [11] proposes an electronic voting system based on fingerprint and face recognition.

C. Using Secret Sharing Scheme for Voting System

Secret sharing schemes have been used in electronic voting, as documented in literature. Schoenmakers [17] uses secret sharing schemes with cryptographic tools to secure electronic voting. Their electronic voting has two protocols: distribution and reconstruction protocols. The distribution protocols have two steps. The distribution step allows the dealer to create and distribute the shares of a secret among all voters. The verification-of-the-shares step allows any participant to use the public key of the encryption method to verify the share. Similarly, the reconstruction protocols have two steps: decrypting the share and pooling the share. Nair et al [18] proposes an electronic voting system (EVS) that uses a secret sharing scheme and secures multi party computation to provide security. The electronic voting system (EVS) has four modules: polling station, communication server, chief election commissioner, and collection center. The polling station has the voting machines and voting panel. The chief election is responsible for managing the candidate information in the voting panel. The communication server manages all activities and coordinates all modules. The collection center manages the collection centers. Liu et al [16] proposes an electronic voting scheme that uses a secret sharing scheme and k-anonymity to provide security and coercion-resistance. Their scheme ensures voters can verify the correctness without knowing others information.

III. TokenVote Objectives

The main goal of this paper is to explore a cloud electronic voting scheme which protects not only the voting information but also the biometric data (i.e. fingerprint). TokenVote protects each vote during its journey from the voter to administration who computes and declares the final voting. In this section, we explore the objectives of TokenVote in privacy, non-repudiation, and authentication.

A. Non-Repudiation and Authentication

TokenVote scheme uses biometric data (i.e. fingerprint) and a secret sharing scheme [15] to achieve its goal in non-repudiation and authentication. In the voting process, a user must provide his/her biometric data (i.e. fingerprint). Thus, a voter cannot deny his/her vote, providing non-repudiation. This strengthen the TokenVote scheme as any organizations/administrations can make sure any voter cannot deny his/her voting at a later time. Regarding the authentication objective, biometric data (i.e. fingerprint) is considered a highly regarded authentication tool for organizations. TokenVote scheme requires that any voter must enroll his/her fingerprint to participate in voting. In the voting process, the voters must provide their fingerprint again for matching, authentication and participation during voting. This allows organizations/administrations to verify who has participated in voting.

B. Security and Privacy

TokenVote provides security and privacy for each voters voting information and for the biometric data (i.e., fingerprint). TokenVote scheme uses bipartite tokens [20] to do matching/voting in an encrypted domain. For each voting share, TokenVote scheme uses secret sharing scheme to split the vote into multiple shares where each share is in encoded mode during all of voting process. No one knows the information hidden inside each voting share from the start stage until the last stage of voting process. The TokenVote provides security and privacy, not only for voting information but also for biometric data (i.e., fingerprint).

C. Scalability and Performance

The TokenVote scheme uses the cloud for many objectives including scalability and performance. The TokenVote scheme uses secret sharing scheme to split each vote into multiple shares of a vote where the size of each share is equal to the original size of a vote. The increased data size needs a scalable environment for computing. Thus, cloud computing

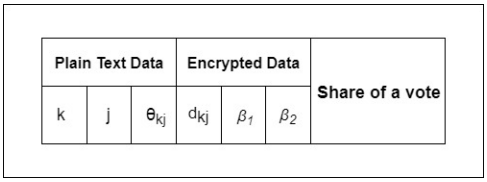

Fig. 1. The pair table data layout stores in the cloud. Each row of the pair table data contains plain text data (k, j, θ_{kj}), encoding data (d_{k_j}, β_1, β_2) and share of vote

is a great option for big data. Therefore, the TokenVote scheme distributes all shares of a vote over multiple clouds where no single cloud stores the whole shares of a vote. In matching/voting process, the TokenVote scheme uses threading to do matching/voting in parallel, resulting in improved voting performance.

IV. Design of TokenVote Scheme Algorithm

In our design, we present the architecture of TokenSign scheme in enrollment and matching/signing process. The TokenSign scheme consist of two protocols: single protocol and group protocol. Single protocol is used to perform a signature for one person while group protocol is used to perform a signature for a group of people.

A. Enrollment Process

First, TokenVote creates a vote (secret) that is distributed among all participants. Second, the TokenVote scheme uses secret sharing scheme [15] to split and distribute the vote (secret) between all voters where each voter has one share of the vote (secret). In this distribution, the TokenVote determines the maximum total shares, set equal to the maximum number of voters, and the threshold shares, set equal to the minimum number of voters. Third, the TokenVote scheme collects the fingerprint data from voters and applies the NIST Bozorth Matcher Algroithm [22] to create minutia files and pair-tables. The TokenVote scheme uses the revocable fingerprint biotokens (Biotope) [19] to transform the plaintext of fingerprint data (i.e., pair-table) in the encrypted fingerprint data. The TokenVote applies Bipartite token [20] to store each share of vote inside a voters encrypted fingerprint data. Finally, TokenVote distributes each share of votes (Biotoken share) in multiple clouds where each cloud does not store all shares of votes that needs to recover the final voting result. Algorithm 1 shows the details of the TokenVote enrollment process steps and figure 1 shows the layout share of vote store in the cloud.

B. Voting Process

In the voting process, the TokenVote scheme requires collection of fingerprint data from each voter who is enrolled as his/her fingerprint data is needed for the individual to participate in a vote. Second, the TokenVote scheme follows the same steps in the enrollment process where it creates minutia points, minutia files, pair-tables, and encodes the pair-tables for the probe fingerprint data. Then, the TokenVote scheme matches the encoding probe pair-table against an encoding gallery pair-table for all voters simultaneously. If the authenticating matching is successful between a voters probe and gallery fingerprint data, the share of voting is released

Data: 1. Gallery fingerprint image g_i, Where i=1,2,3,. . . ,n.
2. Voting Secret v_i.
Result: 1. Encrypted gallery fingerprint (pair-table t_i).
2. Share of Vote hidden inside Encrypted Gallery Fingerprint.

```
for ( each Voting Secret v_i && each gallery fingerprint image g_i ) {
    for ( each Voting Secret v_i ) {
        split the voting secret v_i into multiple shares N_i using SSS [15];
        determine all shares N_i and the threshold K_i using SSS [15] ;
        check (shares N_i == maximum number of voters R_i);
        check (threshold K_i == minimum number of voters R_i);
        check (shares N_i >= threshold K_i);
    }
    for ( each gallery fingerprint impression g_i ) {
        create minutia points m_i using NIST Bozorth [22];
        create minutiae file f_i using NIST Bozorth [22];
        create the gallery pair-table t_i using NIST Bozorth [22];
        encode the gallery pair-table t_i using Biotope [19];
        hide a secret of voting share N_i inside the encoding gallery pair-table t_i using Bipartite [20] ; upload the encoding gallery fingerprint (pair-table t_i) to the cloud;
    }
}
```

Algorithm 1: Enrollment process algorithm of TokenVote scheme

Data: Probe fingerprint image p_i where i=1,2,3,. . . ,n.
Result: Vote Result.

```
for ( each probe fingerprint impression p_i ) {
    create minutia points m_i using NIST Bozorth [22];
    create minutiae file f_i using NIST Bozorth [22];
    create the probe pair-table t_i using NIST Bozorth [22];
    encode the probe pair-table t_i using Biotope [19];
}
for ( all encoding probe pair-table t_i && encoding gallery pair-table t_i in the cloud ) {
    match each encrypted probe pair-table t_i in parallel against all encrypted gallery pair-table t_i ;
    if (match == true) then
        release the shared vote for each voter;
        collect all shared votes from all voters;
    if (shared votes >= minimum number of voters R_i) then
        compute the all shared votes from all voters using SSS [15];
        declare the voting;
}
Return the vote result.
```

Algorithm 2: Voting process algorithm of TokenVote

TABLE I. THE SPEED RESULTS WHERE THE VALUE OF P-VALUE FROM T-TEST REJECTS THE NULL HYPOTHESIS HO

	Cloud-ID-Screen	Bipartite	TokenVote
AVE	26.836	26.93	19.93
STD	0.22	0.31	0.24

for this voter. The TokenVote scheme conducts this process in parallel for all voters and releases all shares of voting from all voters. Finally, the TokenVote scheme applies a secret sharing scheme [15] to compute all shares of voting. If the number of shares is greater than or equal to the minimum number of voters (threshold shares of voting), the TokenVote scheme releases the voting secret and declares the voting result. Algorithm 2 shows the details of TokenVote voting process steps.

V. EXPERIMENTAL DESIGN

In our experiment we design a decision-making scenario in an organization where the decision has been taken from three levels of management. Each level of management has ten people as decision makers who propagate their voting decision from a lower level group to the upper level group. At the third level which is the final stage, the voting is computed and released. We compare our scheme against the Bipartite Biotokena algorithm [20] as the first baseline and Cloud-ID-Screen [23] as the second baseline. We conduct our experiment in Amazon Web Service cloud, so we use eight clouds: North Virginia, North California, Ohio, London, Paris, Ireland, Tokyo, and Sydney. During the enrollment process, TokenVote uses the fingerprint dataset (FV C2002Db2 a) [24] and follows the steps as explained in Section 4-A. Then, the TokenVote scheme uses the programming lanaguages C++ and Python to upload the gallery encoded fingerprint data to multiple AWS S3 cloud storages. The uploading process is done in parallel by using threading. During the voting process, we connect Amazon AWS S3 with Amazon AWS EC2 instance by using the Python boto library to do parallel matching. Finally, we did the matching/voting process twenty times in parallel and took the average of all these runs.

VI. EXPERIMENT EVALUATION

In our hypothesis: we aim to prove that if we distribute a vote among multiple people, we can do parallel voting to speed up the voting process while getting comparable accuracy against the baselines. To prove our hypothesis, we run two experiments, accuracy and performance, and evaluate the results.

A. Accuracy Evaluation

We run our accuracy experiment to evaluate the false accept rate (FAR) and the genuine accept rate (GAR) for both the baseline and TokenVote scheme. Then, we compare the result of our TokenVote scheme against the two baselines. Figure 2 shows the ROC curve result where our TokenVote scheme achieves GAR equal to 97 and FAR equal to 0. This promising result proves our hypothesis.

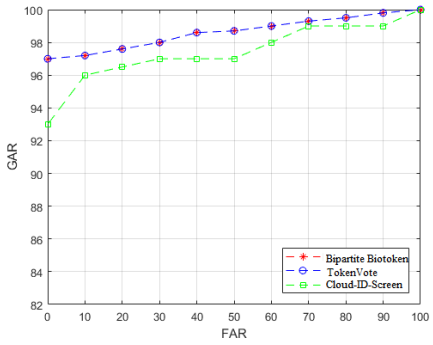

Fig. 2. The ROC curve comparing accuracy of our TokenVote scheme against the two baselines

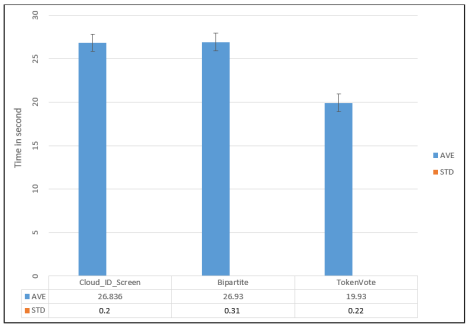

Fig. 3. The speed result comparing the performance of our TokenVote scheme against the two baselines

B. Performance Evaluation

We run an identification (1:N) experiment to evaluate the performance of our TokenVote scheme against the two baselines. We run our experiment in parallel for our TokenVote scheme and the two baselines. Then, we compare the result of our TokenVote scheme against the two baselines. Figure 3 shows the speed result where our TokenVote scheme achieves promising result over the two baselines. For formal testing, the null hypothesis Ho is that the time of matching for the baseline is less than or equal to TokenVote, i.e., the baseline performs better. Table I shows the speed results where the value of P-value from t-test rejects the null hypothesis Ho and proves our claim that the TokenVote achieves better performance over the baseline.

VII. CONCLUSION

In this paper we design, implement, and evaluate the TokenVote scheme. The TokenVote is a cloud electronic voting system uses the revocable fingerprint biotoken and secret sharing scheme. Thus, TokenVote provides privacy and security not only for the voters but also for administration. Moreover, TokenVote uses cloud computing and threading to provide scalability and performance. For future work we will use smart devices for voting since all smart devices use biometric for authentication.

REFERENCES

[1] F. C. Lunenburg, "Decision making in organizations." *International journal of management, business, and administration*, vol. 15, no. 1, pp. 1–9, 2011.

[2] P. Drucker, "The effective executive." 2016.

[3] A. Gibbard, "Manipulation of voting schemes: A general result," *Econometrica*, vol. 41, pp. 587–601, 1973.

[4] K. Sako and J. Kilian, "Receipt-free mix-type voting scheme: A practical solution to the implementation of a voting booth," in *Proceedings of the 14th Annual International Conference on Theory and Application of Cryptographic Techniques*, ser. EUROCRYPT'95. Berlin, Heidelberg: Springer-Verlag, 1995, pp. 393–403.

[5] A. Fujioka, T. Okamoto, and K. Ohta, "A practical secret voting scheme for large scale elections," in *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology*, ser. ASIACRYPT '92. London, UK, UK: Springer-Verlag, 1993, pp. 244–251.

[6] P. Ryan G, "Computerized voting system," Mar 1999.

[7] T. Okamoto, *An electronic voting scheme*. Boston, MA: Springer US, 1996, pp. 21–30.

[8] B. Lee and K. Kim, "Receipt-free electronic voting scheme with a tamper-resistant randomizer," in *Proceedings of the 5th International Conference on Information Security and Cryptology*, ser. ICISC'02. Berlin, Heidelberg: Springer-Verlag, 2003, pp. 389–406.

[9] J. Bannet, D. W. Price, A. Rudys, J. Singer, and D. S. Wallach, "Hack-a-vote: Security issues with electronic voting systems," *IEEE Security Privacy*, vol. 2, no. 1, pp. 32–37, Jan 2004.

[10] D. A. Kumar, T. Ummal, and S. Begum, "A novel design of electronic voting system using fingerprint," 2011.

[11] S. N. Syed, A. Z. Shaikh, and S. Naqvi, "A novel hybrid biometric electronic voting system: Integrating finger print and face recognition," *CoRR*, vol. abs/1801.02430, 2017.

[12] S. Hof, "E-voting and biometric systems," 2004.

[13] S. Kumar and M. Singh, "Design a secure electronic voting system using fingerprint technique." *International Journal of Computer Science Issues (IJCSI)*, vol. 10, no. 4, 2013.

[14] e. a. Ahammad, Ifthekhar, "Towards a secure and automated platform for fingerprint-based electronic voting machine." *International Journal of Intelligent Machines and Robotics*, vol. 1, no. 1, pp. 34–44, 2018.

[15] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[16] Q. Zhao and Y. Liu, "E-voting scheme using secret sharing and k-anonymity," in *Advances on Broad-Band Wireless Computing, Communication and Applications*, L. Barolli, F. Xhafa, and K. Yim, Eds. Cham: Springer International Publishing, 2017, pp. 893–900.

[17] B. Schoenmakers, "A simple publicly verifiable secret sharing scheme and its application to electronic voting," in *In CRYPTO*. Springer-Verlag, 1999, pp. 148–164.

[18] D. G. Nair, V. P. Binu, and G. S. Kumar, "An improved e-voting scheme using secret sharing based secure multi-party computation," *CoRR*, vol. abs/1502.07469, 2014.

[19] T. E. Boult, W. J. Scheirer, and R. Woodworth, "Revocable fingerprint biotokens: accuracy and security analysis," in *2007 IEEE Conference on Computer Vision and Pattern Recognition*, June 2007, pp. 1–8.

[20] W. J. Scheirer and T. E. Boult, "Bipartite biotokens: Definition, implementation, and analysis," in *Advances in Biometrics*, M. Tistarelli and M. S. Nixon, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 775–785.

[21] M. Jakobsson, A. Juels, and R. L. Rivest, "Making mix nets robust for electronic voting by randomized partial checking," in *Proceedings of the 11th USENIX Security Symposium*. Berkeley, CA, USA: USENIX Association, 2002, pp. 339–353.

[22] C. Watson, M. Garris, E. Tabassi, C. Wilson, R. McCabe, S. Janet, and K. Ko, *User's Guide to NIST Biometric Image Software (NBIS)*, 2007.

[23] F. Alsolami, B. Alzahrani, and T. Boult, "Cloud-id-screen: Secure fingerprint data in the cloud," in *2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA)*, Jan 2018, pp. 1–8.

[24] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, "Handbook of fingerprint recognition," 2009.