Fast and Secure Electronic Voting using BLAKE2

[1]Ankit Kumar Jain, [2]Puru Joshi, [3]Arpit Agarwal
[1,2,3]Dept. of Computer Engineering, MPSTME, NMIMS, Maharashtra, India

Abstract
The traditional implementation of an E-Voting system, while being superior to the physical voting system, happens to have a potential flaw in its chain of security, particularly the hash functions being used. The system is potentially susceptible towards attacks, such as pre-image attack or collisions, which could compromise the overall integrity and security of the entire E-Voting system. In this paper, we propose a modified version of the E-Voting system, where we replace the flawed hash with a superior one. In unison, the modern hash delivers a superior performance.

Keywords
Cryptography, Hash, SHA, BLAKE, Grid-Card

I. Introduction

Voting is avital and essential feature of a modern democratic government, to allow its citizens to choose their representative for the term [10]. To ensure a fair and transparent proceeding, where the anonymity of the voter is also maintained, there is need of a secure platform that placesintegrity at the highest level of importance. The system should be robust enough, to stand firm against and resist the many possible illicit behaviors which can potentially prove to be harmful to the system [1].

Conventionally, the voting populace have been electing their representative, using the physical ballot system. The presence of the voter is essential at the polling place. The votes are recorded for each voter on the paper ballots, which are later read and computed individually. The final results are then tabulated. The potential attacks to the system can involve ballot stuffing and false tallying. The traditional voting system is flawed and riddled with malpractices including, vote count falsification, ballot stealing and improper voting due to negligence and ignorance[6]. The aforementioned factorsdevelop a need for the voting system to be robust and secure.To improve the credibility of the elections, there was a need to add more levels of security to the system [1, 4].

Electronic voting or E-Voting involves the use of electronic means to record a user's vote [4]. The vote when casted, is then consigned to a data-store. After the election phase is completed, i.e. once all the individuals have successfully casted their votes, the votes from the data-store are interpreted and tabulated. This ensures protection against the fraudulent practices like vote count falsification, ballot theft and human negligence in managing the physical ballot [5, 6, 8].In this paper, an improvement to the previous E-Voting system is proposed, which incorporated a multifactor authentication scheme for the voters, following a cryptographic model for ensuring a higher level of security and integrity.

II. Related Work

Extensive research has been done in the field of secure electronic voting. Being the defining feature of democracy, government bodies have invested and promoted the system. Looking at the insecurities existing in the manual voting system, use of electronic voting is suggested, to ensure the transparency and credibility of the system [2]. Also with the view of improving the voter experience, which is an essential factor in determining the participating populace, Rossler T.G. has quoted that electronic voting actually helps in increasing the voter count [9].

Different security checks and measures are analyzed and reviewed by Avi Rubin [10], concluding that the factors like authentication, confidentiality, availability and integrity are essential for any electronic voting system.Ciprian suggested on adding more levels of security to the system, including firewalls and SSL connections [3]. He also quoted that these measures, being chief for the securityare still not sufficient.

Modern technologies and rapid advancement in the fields of communication and security, allow a voter to cast his/her vote from any place, at any time using a number of devices at hand [4].

Olayemi Mikail Olaniyi et al [11], have designed a secure platform for electronic voting, using multifactor authentication. The authentication check involves the use of cryptographic hash functions and grid card authentication for enhanced security. In this paper, the performance and the security is further increased, as discussed in the later sections.

III. System Design

The motivation behind system designing is to create an image of the system that helps in realizing the full-fledged system that satisfy all the functional requirements. Functional requirements are the requirements that depicts the behavioral aspects of the system, functional requirements are often identified during communication and planning phase of The Software Development Life Cycle.

A. Requirements Definition for the Secure E-Voting Systems

Every voting system must consist of a few basic properties for ensuring the validity of the system and also instilling confidence in not only the voters, but also the candidates contesting in the election[2, 3, 4, 7]. A few of these necessary requirements mentioned by NSF [7] are listed and elaborated below:

1. Confidentiality

By definition, confidentiality is to perform an act of some sort in secret or without the knowledge of others. In the scenario of an e-voting system, the vote of the voter should be kept secret.

2. Non-repudiation

By definition, Non-repudiation is referred to as the mechanism that is used to prove the ownership of a certain act or object to a particular individual. In the scenario of an e-voting system, the vote casted by a voter should uniquely identifiable.

3. Authentication

By definition, authentication is the act of proving something to be true or valid. In the scenario of an e-voting system, the voter should be able to prove to the system that he is who he claims to be.

4. Accuracy
Accuracy is freedom for mistakes and errors. In the scenario of an e-voting system, the votes that are casted by the voters should be accurately counted.

5. Integrity
Integrity of data is ensuring that the data is uncorrupted or modified and can be accessed or modified only by authorized personnel. In an e-voting scenario, the votes once casted should be unmodifiable.

6. Secrecy and Non-Coercion
In an e-voting system, the candidate for whom a voter is casting the vote should be known only to the voter himself and no mechanism should exist for proving otherwise. This is a necessary to avoid coercion and other malpractices like vote buying.

7. Audit trail
The e-voting system must contain a mechanism to prove that the votes casted by the voters are correctly accounted for and are correctly added to the candidates vote count.

8. Uniqueness
Every voter in any voting system has an equal weight attached to his single vote. Any voter should be able to vote only for a single candidate and should unable to vote multiple times.

9. Transparency
For any of the stakeholders of the entire voting system to have trust and confidence in the e-voting system, they must be able to the understand the procedure and the reasons for following them. This is only possible if the system is transparent in nature and does not attempt to hide or conceal information from the stakeholders.

10. Simplicity
When the system is designed, simplicity should be held with utmost importance keeping in mind the interests of the end users, that is the voters.

11. Democracy
In a democracy, every citizen is entitled to his or her own opinion and has the freedom to express it. The e-voting system must be impartial to its voters and candidates and treat them all as equals.

12. Privacy
To avoid influencing the decision of voters who are yet to vote, the votes of voters who have already completed the voting procedure must be kept a secret until the end of the voting procedure when the final results are announced.

13. Fairness
The e-voting system must be resistant to tampering and other malpractices like bribing of officials to resist the influence of such malicious entities.

B. Architecture of Secured Model for E-Voting System
The voting process comprises of three phases, namely, pre-election phase, election phase and post-election phase. All the users aspiring to vote, register themselves in the pre-election phase. The phase also involves generatingaunique ID and a grid-card for each individual user, following to which, aunique one-time password is also generated by the system, sent to the user. During registration, the users are required to fill in the necessary details, which includes, a phone number and an email address. All of the required details and information collected, are then stored in the database.In the election phase, all the voters use their one-time generated password and the grid-card code, to cast their votes, paired with their unique ID. The casted vote is then enciphered, and hash of the vote is calculated, using the SHA-256 hashing function. Both the enciphered vote and the hash of the vote is stored in the database. In post-election phase, for each unique ID, the encrypted vote is decrypted and hash of it, is calculated using the same hashing function, i.e. SHA-256. The stored hash is then compared with the newly generated hash value. If both the hashes match, then this signifies that the vote hasn't been tampered with in any way, and the integrity is intact. Otherwise, the casted vote is deemed as a fake, or hacked, and hence won't be taken into account, for the final counting of votes.Figure 1 shows the three phases involved in the E-Voting system.

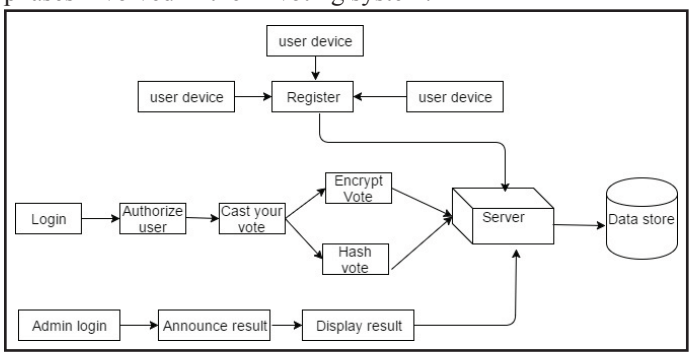


Fig. 1: Architecture of E-Voting System

C. Model Definition
Cryptographic hash functions are often used to verify the integrity of data, due to the inherent property of cryptographic hash functions to result in a drastically different hash output for even a minute change to the input data. Thus, cryptographic hash functions are often used to generate a digital finger print. For some given data x and a cryptographic hash function h, let the calculated cryptographic hash of the data x using the hash function h be denoted by y as shown in equation (1).

$$y = h(x) \quad (1)$$

Say that the data x has been tampered in some way during transmission, we denote this tampered data as x'. Correspondingly, the calculated hash of this tampered data is denoted by y' as shown in equation (2).

$$y' = h(x') \quad (2)$$

Thus, if the integrity of a given data x is under suspicion, denoted by x^*, it can be verified by re-computing the cryptographic hash, denoted byy^* and compared with the initial cryptographic hash value y obtained in earlier.

$$y^* = h(x^*)$$

If the data is not tampered with, that is x^*=xthen, the following is true:

$$h(x^*) = h(x)$$
$$y^* = y$$

As y* = y, we can say that the integrity verification of the data x* is successful.

If the data has been tampered with that is x* = x' then, the following is true:

$$h(x^*) = h(x')$$
$$y^* = y'$$

As y* ≠ y, we can say that the integrity verification of the data x* has failed.

D. Grid Card Authentication

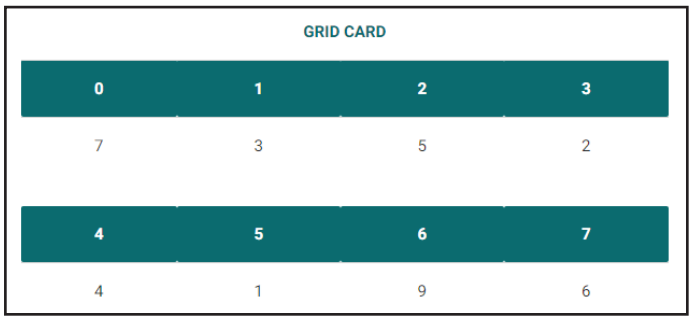


Fig. 2: Generated Grid Card

Fig. 2 describes the grid card. provided to the user when user registers into secure E-Voting system, the grid card here is (2X4) grid. There are random values in all the 8 cells of the grid card.

When users need to log into the system, they are prompted to enter values from specific cells of the grid give to them. The values which user provides is then matched against the corresponding cells of the grid that was provided to user at the time of registration. if they match then user is logged into the system.

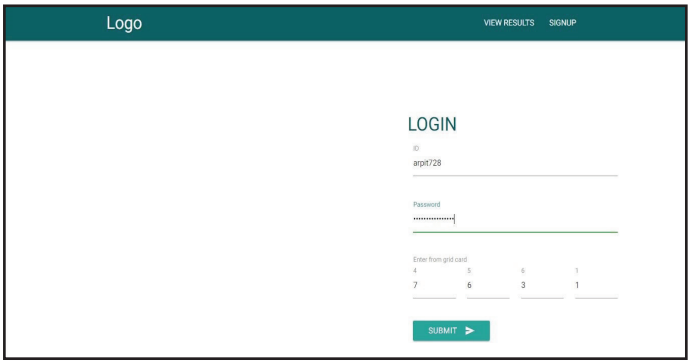


Fig. 3: Prompt to Enter Numbers From Grid Card When Logging In

E. Integrity Check

Integrity check is used to ensure that all the votes casted in favor of a particular candidate is a valid vote, that is, the votes have not been tampered with since the time user casted that particular vote. At the time of voting, boththe encrypted vote and the hash digest of the vote are stored in to the database. To ensure the integrity of the votes when results are announced, for each vote the encrypted vote is decrypted and has digest of the decrypted vote is again calculated, if this hash digest matches the hash digest that was stored in database at the time of voting it means the vote has not been hacked and thus the vote is valid, while if they are not equal this means, the vote has been hacked.

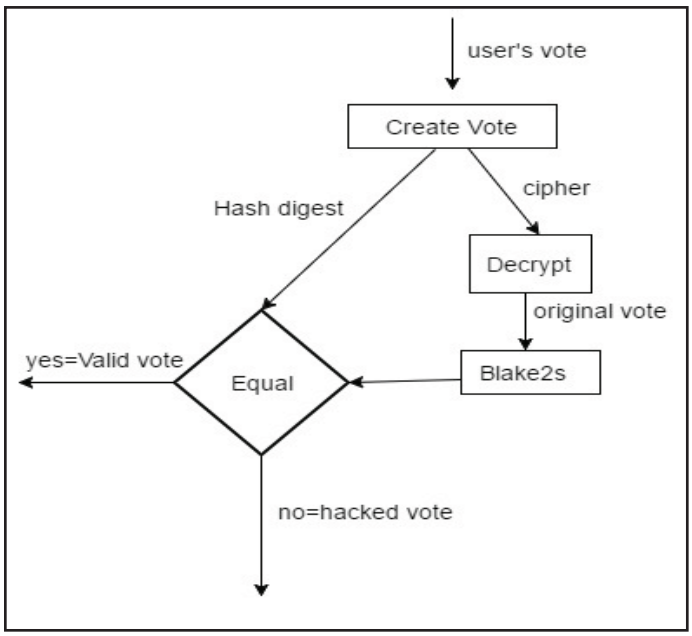


Fig. 4: Checking For Integrity

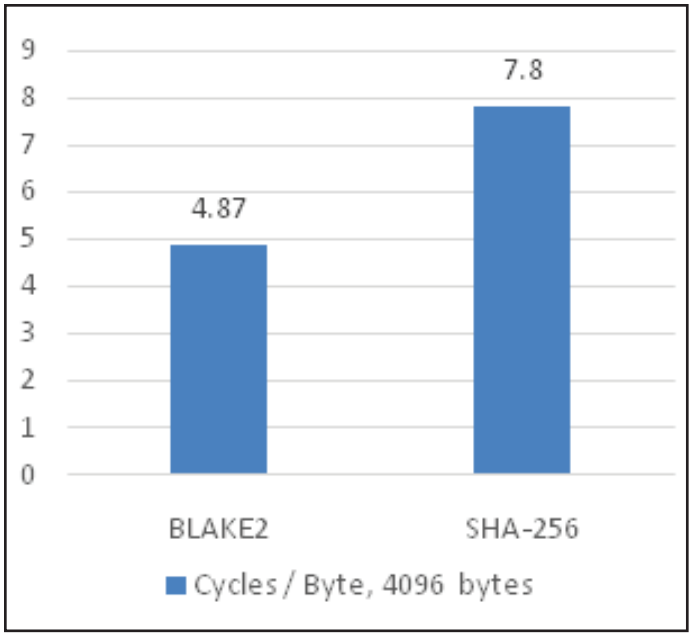
IV. Modification and Result Analysis

Replacing SHA-256 with BLAKE2, it has been observed that the BLAKE2 performs much faster. The time taken by SHA-256 to compute the hash is twice as much, when done by BLAKE2. This results in increased performance of the system.Comparison between the two hashing algorithms in terms of CPU cycles-per-byte is shown in the Table 1.

For Intel Core i5-6600; 4 x 3310MHz:

Table 1: Comparison Between Blake2s and SHA256

Cycles/byte for 4096 bytes			
Quartile	Median	quartile	Hash
4.87	4.87	4.87	Blake2s
7.79	7.80	7.81	SHA-256

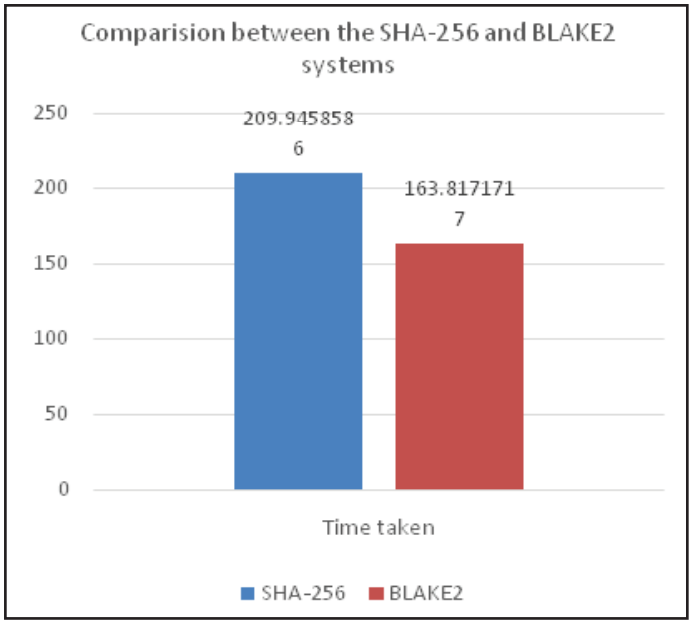


Graph 2 Comparison Between Blake2 and SHA-256

It is observed that the number of CPU cycles used per byte for Blake2 is lower by a proportion of 40%. This helps in achieving a significant performance boost in the overall system.

Both variants of the system(SHA-256 and BLAKE2) were timed for a hundred iterations and the corresponding averages were computed. It was observed that there was a 12% improvement in performance of the system regarding time taken, when using BLAKE2. The averages for the time taken are shown in chart 2.

Table 3: Comparision Between the Time Taken by the Two Variants of the System



V. Conclusion

The original e-voting system developed by MikailOlaniyi, Olayemi, et al uses some very novel ideas like the grid card authentication system and multifactor authentication and is a mostly secure system, except for a small oversight regarding the choice of the hashing algorithm in the original system.
As stated earlier in this paper, we suggest to replace the SHA-256 algorithm used in the original design with a more modern and secure algorithm, specifically BLAKE2.

Not only is this modified system more secure than the original design, but also significantly faster due to the nature of BLAKE2.

VI. Future Work

By improvement and can be made into a more secure system. Some areas where improvements can potentially be made are as follows:

- Work with the local government of a country to include the biometric information of its citizens (example: Aadhar cards in India) as another factor of authentication as part of the multi factor authentication nature of this e-voting system.
- Implement other factors of security like privacy and confidentiality into this system
- A more secure and faster hashing algorithm (such as BLAKE2x which is currently under development) can be used to improve the performance of the system.

References

[1] Kohno T., Stubblefield A., Rubin A., Wallach D. S, "Analysis of an Electronic Voting System", In Proceedings of IEEE Symposium on Security and Privacy 2004, pp. 1-23, 2004.

[2] Manish K, Suresh K.T, Hanumanthappa. M, Evangelin G.D (2005), "Secure Mobile Based Voting System", [Online] Available: http://www.iceg.net/2008/books/2/35_324_350.pdf on November 17th 2012.

[3] Ciprian Stănică-Ezeanu (2008), "e-Voting Security", Buletinul Universităţii Petrol – Gaze din Ploieşti, Vol. LX (2), pp. 93-97.

[4] Okediran O. O., Omidiora E. O. Olabiyisi S. O., Ganiyu R. A. and Alo O. O. (2011),"A Framework for a Multifaceted Electronic Voting System", International Journal of Applied Science and Technology, Vol. 1(4), pp. 135 – 142.

[5] Olaniyi, O.M, Adewumi D.O, Oluwatosin E.A, Arulogun, O. T and Bashorun M.A(2011),"Framework for Multilingual Mobile EVoting Service Infrastructure for Democratic Governance", African Journal of Computing and ICT (Journal of IEEE Nigeria Computer Section), Vol. 4, (3), pp. 23 – 32.

[6] Olaniyi, O.M, O.T Arulogun, E.O, Omidiora, A Omotoso, Ogungbemi O.B. (2012), " Design of A Secured Model For Electronic Voting System Using Stegano-Cryptographic Approach ", Proceedings of the 7th International Conference on ICT Applications, Application of ICT to Teaching, Research, and Administration (AICTTRA 2012), National Defense College Abuja, pp. 84-89.

[7] NSF (2001)," Report on the National Workshop on Internet Voting: Issues and Research Agenda" , National Science Foundation, [Online] Available: http://news.findlaw.com/cnn/docs/voting/nsfe-voterprt.pdf.

[8] Abdulhamid S M , O.S. Adebayo, D. O,Ugiomoh,M.D AbdulMalik,"The Design and Development of Real Time EVoting System In Nigeria with Emphasis on Security and Result Veracity", International Journal of Computer Network and Information Security",Vol.5, pp. 9-18, [Online] Available: http://www.mecs-press.org/ijcnis/ijcnis-v5-n5/IJCNIS-V5-N5-2.pdf on 7th August 2013.

[9] Rossler T.G,"E-voting: A survey and Introduction", 2011.

[10] Rubin, Avi,"Security considerations for remote electronic voting over the Internet", [Online] Available: http://wiki.agoraciudadana.org/images/5/56/An%2BIntroduction%2 Bto%2BElectronic%2BVoting%2BSchemes.pdf Retrieved on 15th June 2012.

[11] Olaniyi, Olayemi Mikail, et al.,"Design of secure electronic voting system using multifactor authentication and cryptographic Hash Functions", 2013.

Mr. Ankit Jain has Completed his M.Tech from NIT Rourkela and B.E. from RGPV Bhopal. He has more than 5 years of experience in teaching, and is currently working as Assistant Professor in Department of Computer Engineering, NMIMS Shirpur. His area of research is Network Security.

Mr. Puru Joshi is a 4th year student pursuing his Bachelors of technology degree in the field of Computer Engineering from the institute Mukesh Patel School of Technology Management Engineering, NMIMS. At present his research interest lies in image processing, machine learning and artificial engineering.

Mr. Arpit Agrawal is a 4th year student pursuing his Bachelors of technology degree in the field of Computer Engineering from the institute Mukesh Patel School of Technology Management Engineering, NMIMS. At present his research interest lies inmachine learning and artificial intelligence.