International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Proposed Authentication Platform for E-Voting IoT System

Ahmed Salman Mohsen*[1], Mohamed Ibrahim Shujaa[1], Ahmed Bahaaulddin A. wahhab[2]

Submitted: 12/11/2022 **Accepted:** 13/02/2023

Abstract: In recent years, traditional elections have failed to satisfy public and political authorities. The traditional elections paper based is suffering from many issues of cheating the ballots or spoilage of the election documents. As a result to these mentioned issues many countries go forward adopting the electronic voting system to tackle the issues of traditional voting. Elections aren't entirely safe because votes can be easily hacked. It also jeopardizes voter privacy and transparency. Furthermore, counting the ballots takes far too long. This paper suggests a Blockchain-based solution to address all of the problems of traditional elections. Theoretically, vote security, authentication, and data integrity are guaranteed. This research proposed a voting center by using and IOT point that saves the votes as a blockchain block attached to a blockchain. Because the data inside the blockchain is not encrypted so there is a need for encryption to ensure the privacy of the data in each block, accordingly the security is ensured by Speck cipher lightweight block cipher and bakers chaotic key generator to increase the safety of the information in each block (Vote). The reason behind choosing the lightweight is to operate the encryption method on IOT point with a limited hardware resources like Raspberry pi. The use of the blockchain as a secured public leader with a powerful hashing system with light weight speck cipher show a good improvement in block's data integrity and privacy. Authentication is also provided using a fingerprint logging system. The authentication fingerprint system was accurate and efficient. The proposed e-voting system lets voters Vote either in-office or elsewhere. Finally, the proposed Blockchain voting mechanism significantly reduced the time of creating blocks and encryption of data inside each block.

Keywords: *E-voting, Blockchain, Raspberry Pi, Computer security, Lightweight block cipher, Speck algorithm.*

1. Introduction

People often used votes to choose someone from a group. This was done at many levels of government, from the local level up to the president, including the mayor and people in the House of Representatives. Everyone should be able to vote if they want to. Needs like privacy, respect, and not being judged there are more things to think about. For example, figuring out how accurate, reliable, and fast something is. In any case, these requirements might be hard to meet with the manual voting system that is used in many countries. This is because the ballots have to be counted by hand, which can lead to a wrong or mostly wrong result. An electronic voting system has been suggested as a way to solve this problem. But putting in place electronic voting does not solve the problem completely. There are some weak spots that attackers can use to put systems and voting results in danger. In this paper, we've made a fingerprint-based authentication system for an electronic voting system that protects both reliability and privacy [1].

[1]*Middle Technical University, Electrical Engineering Technical College-Baghdad, Iraq*
[2]*Middle Technical University, Technical College of Management, Baghdad, Iraq*

**Corresponding author email: bbc0053@mtu.edu.iq*

The computerized voting method has become a hot topic in academic circles. Voters can vote from afar using smart devices such as smartphones and tablets to determine the best candidate for a particular institution, country, or university. Electronic voting over paper voting includes real-time counting, rapid scoring, environmental friendliness, anonymity, fewer errors, and decentralization. In addition to these essential system requirements, several security flaws and attacks accompany the evolution of the digital system. In e-voting systems, to preserve privacy and anonymity between voters and polling materials, this method used public-key encryption and blind signatures. In recent years, much study Has been achieved on the electronic voting method by using blockchain technology [2].

There are several types of voting processes, such as casting ballots, which involve selecting the right candidate. Punched cards, polls, and voting booths are some examples of electronic voting methods. Many outdated voting system procedures in our modern world of advanced technology have been modified to better suit conditions in various areas of life. For automated electronic voting systems, voting also includes secret ballot boxes and secret voting. In this there is an "IOT based electronic voting system" which can be used over long distances. Helps voters save time, money and effort when traveling to the polls. Check the result will be

quick and simple. Provides modern electronic voting with great data security Here, the raspberry pi is used as an Internet of Things (IoT) device to reduce or eliminate unintended human error [3]. As a fundamental component of human democracy, voting has been subjected to several improvements throughout the years, including improvements to the processes, mechanisms, and methods used to make voting more verifiable, transparent, and accessible. Since the advent of information and communication technology (ICT), there has been an increased emphasis on using information and communication technology to facilitate voting processes, especially to promote transparency and accessibility of voting procedures. Since their first use in the 1960s, electronic voting systems have made a lot of progress in adapting them to use the Internet's technology. People use terms like "electronic voting," "digital voting," and "electronic voting" to describe these changes (using a web browser to cast a vote) [4]. When it comes to the Internet of Things, security is paramount. Authentication systems might take the form of either theoretical models or actual hardware. Passwords and smart cards are the most convenient and straightforward methods of physical authentication. Using a biometric method of authentication is more convenient and quicker than using a password or PIN. Biometric authentication provides an extra layer of protection when logging into our personal gadgets [5]. Blockchain technology has sparked widespread interest, with notable banking, healthcare, and supply chain management applications. Blockchain is a data structure that has stored and distributed all transactions since its inception. It's a decentralized distributed database that keeps track of an ever-growing list of data records while keeping them safe from illegal modification, manipulation, and amendment. Connecting to the grid, sending new transactions, checking transactions, and making new blocks are all possible with the Blockchain. Each block is given a ciphered hash (which can be thought of as a block's fingerprint) that is valid as long as the data in the block isn't modified. If the block is changed, the cryptographic hash will switch to signify the data change, which could be due to malicious activity. As a result of its strong cryptographic foundations, Blockchain has been utilized to minimize fraudulent transactions across various industries. Electronic voting is a developing Blockchain application. The advantages of integrity, anonymity, and non-repudiation are vital to the voting application. In recent years, efforts have been made to utilize Blockchain to facilitate electronic voting. It uses blockchain technology to protect and verify voting. Particularly, the Blockchain allows for constructing a voting pool by generating unique physical addresses for voters and candidates [6]. Recent media developments, technical improvements, and public opinion surveys will make national elections quicker and more successful online. Due to its simplicity and affordability, fingerprint biometrics are preferred over other technologies. Since each person's fingerprint is unique and might be lost or forgotten, the most frequent approach makes stealing difficult. This research compares biometric voting to regular voting. The identification and identification system compares the information you supply to a database. Then he asks, "Are you who you say you are?"[7]. Blockchains can be used in many other areas over time due to this system's high degree of transparency. Transparency, decentralization, irreversibility, and non-divorced ability are only a few of the characteristics of an electronic digital system. Many security and transparency challenges have arisen due to the digital electronic voting method. The problem tackled in this paper is how to authenticate and secure each block in the blockchain e-voting center. Accordingly, the goals of this paper will be: first, build an e-voting center that saves ballots using Blockchain and secure each block (Vote) using Speck lightweight block cipher that is suitable to work within the raspberry pi system. Second, ensure authentication before the voter enters the voting chamber by fingerprint system.

2. Related Work

Kiruthika Priya and Vimaladevi, B. Pandimeenal, T. Dhivya (2017) Create an electronic voting machine that helps eliminate fraud on manual voting systems and previous versions of electronic voting. The thesis examines and proposes a system that includes multiple layers of checks to ensure the reliability of the device. With the inclusion of a biometric fingerprint sensor [8]. Rizal Widyarta Gowandy, et al [2018] . This proposes a secure electronic voting system that uses fingerprints and Radio Frequency Identification (RFID) to verify who is voting. Before having their fingerprints scanned, voters must first scan their RFID cards. The key features of Fingerprint are taken from Enhanced Fingerprint [9]. B. Shahzad and colleagues (2019) presented a methodology for ensuring data security through efficient hashing algorithms. In this study, block creation and sealing concepts are introduced for the first time. The inclusion of the block seal idea contributes to the scaling of the Blockchain to fulfill the requirements of the polling process. It is proposed to use the blockchain consortium, the utility of hash algorithms, block generation and stamping, data aggregation, and results reporting using the modifiable blockchain method [10]. It was suggested by N.R.Sathis Kumar and T.Nirmalraj (2019) that fingerprint authentication systems are the most common and accurate. Fingerprint attendance system that keeps track of students' attendance by matching their fingerprints with those in a database. This is done to

praise the students' attendance. It uses a fingerprint-based attendance system to make sure there aren't many mistakes when taking attendance. This also saves money and time compared to using paper to keep track of attendance. By using berries, less work is done by people and the process is made easier. A Raspberry Pi is linked to the fingerprint system [11]. B. Sudharsan (2019) suggested a Blockchain-based technique for securing the votes stored in an EVM (e-voting management system). Additionally, a fingerprint authentication method is included to avoid double voting. The proposed EVM will be tamper-proof, detecting any effort to modify the registered votes and replacing them with the proper data [12]. K. Isirova et al. (2020) proposed a new concept for developing a decentralized electronic voting system using blockchain technology. The two-tier architecture provides a secure voting process without duplicating existing systems (not based on Blockchain). The presented blockchain-based voting protocol has six steps that ensure all requirements provided for such types of protocols, including voting transparency and anonymity [13]. According to A. Shah (2020), blockchain technology enables many applications that leverage distributed economies. The proposed model is an Android application incorporating additional security features such as authentication and permission. Authentication is accomplished by using a uniquely identifying key, and permission is accomplished through the use of a fingerprint. Additionally, voters are confirmed using a one-time password. Security is ensured in this project through the use of the AES 128-bit encryption method, SHA-256, and the Blockchain [14] . Mr. M. Ganesan.et al. (2021) present a voting system that incorporates biometrics (fingerprint) and a physical key (RFID) to cast the vote, as well as the option for the voter to snap a picture while casting their ballot. The server stores all voting data, including the timestamps, so the results of the vote may be made public immediately after they have been counted [15]. S. P. Gupta and colleagues (2021) developed a novel architecture for electronic voting that uses blockchain technology. With Paillier encryption, this strategy ensures the confidentiality of voters' votes. Because of the tamper-proof nature of the blockchain, it is impossible to modify votes. Following that, methods for registration, voting, result declaration, and the results of Paillier encryption for voting have been discussed in detai.[16]. Oke and O.M. Olaniyi (2021)The electronic voting system now utilizes multi-factor authentication security measures. Electronic voting using a smart card and voter authentication based on a modified Feistel block cipher algorithm has been presented [17].

3. Blockchain

A blockchain is a data structure that organizes the storage of transaction blocks. Each brick in the chain is attached to the block immediately preceding it. The initial block in the chain serves as the stack's foundation. Each new block is stacked on top of the preceding one to create a Blockchain stack. Each header contains information that links a block to the block previous it in the chain, so building a chain that ties to the foundation, is the much first block ever created .A hash written on the header identifies each block in the stack. This hash is created using the Secure Hash Algorithm (SHA-256) to create a fixed-size 256 hash that is nearly distinctive. The National Security Agency (NSA) designed the widely used 2001 and was applied as the protocol to secure all federal connections [18]. Any size plaintext can be fed into the SHA-256, encrypting it and turning it into a 256 256-byte binary value. The SHA-256 algorithm produces a 256-bit binary value that is always one-way. It is also a strictly one-way function. Fig 1 shows blockchain.

A distributed ledger of transactions, stored as immutable and interconnected blocks, thus forming a chain, the validity of which is agreed upon by peers on a decentralized network and secured with cryptography. Each block in the chain is connected to the block that came before it. The preceding block's hash value is included in the following block's hash value, “Which is used to determine the hash value of the next bloc”. The previous block's hash values are used to generate the following block, which connects the blocks. Thus, updating the data becomes more complicated, as all subsequent blocks must also be modified. The initial block in the chain serves as the stack's construction block. Each subsequent block adds a layer to the previous block, forming a [Blockchain] stack. Each node maintains data consistency by implementing a consensus algorithm, and the system automatically supports timestamps and ledgers. This means that it does not need any third party in the system [19].

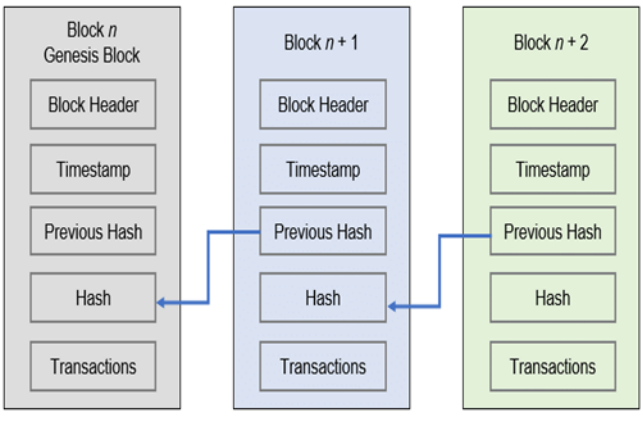

Fig. 1: example of blockchain public ledger.

4. Speck

The National Security Agency (NSA) released Speck, a lightweight block cipher, to the general public in June 2013. The purpose of Speck was to meet the demand for security, robustness, and analytics. A small set of ciphers is designed to provide high performance on various devices. Speck includes ten distinct block ciphers with various key sizes and permutations. It performs well on hardware and software platforms, is adaptable enough to accept a wide range of applications on a single platform, and can be studied using existing technologies. It performs admirably in various lightweight applications; Speck works so well on every platform because it's so well-rounded [20]. Fig 2 shows Speck's lightweight cipher network.

The Speck2n encryption maps make use of the following operations on n-bit

words:

1- bitwise XOR, $\oplus$,

2- addition modulo 2n, +,

3- left and right circular shifts, Sj and $S^{-}j$, respectively, by j bits.

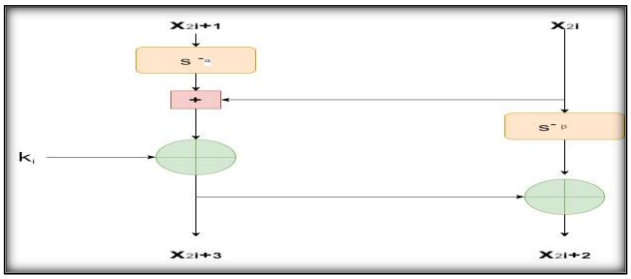

Fig. 2: Speck lightweight cipher network.

For k 2 GF(2)n, the key-dependent Speck2n round function is the map Rk:

$GF(2)^n \times GF(2)^n \rightarrow GF(2)^n \times GF(2)^n$ defined by

$R_k(x, y) = ((S^{-\alpha}x + y) \oplus k, S^{\beta} y \oplus (S^{-\alpha}x + y) \oplus k), ,$ **(1)**

with rotation amounts $\alpha = 7$ and $\beta = 2$ if n = 16 (block size = 32) and

$\alpha = 8$ and $\beta = 3$ otherwise.

The inverse of the round function, necessary for decryption, uses modular

subtraction instead of modular addition, and is given by

$R^{-1}_k(x, y) = (S^{\alpha}((x \oplus k) - S^{-\beta}(x \oplus y)), S^{-\beta}(x \oplus y)),$ **(2)**

5. Baker's Chaotic Map

The chaotic map creates a succession of pseudo-random numbers by continuing intuitively in step with the original settings. The chaotic map's early sets and control limitations are quite subtle. BAKER'S MAP uses invertible two-dimensional chaotic maps on a square for encryption. The Chaotic Baker map is a method for encrypting images popular in the image processing community. The baker map removes bits from the input data to decrease the connection between it and the encrypted data depending on the secret key. Discrete Baker maps are denoted by B (r1, r2,..., RQ), where the order of the q integers r1, r2, r3,..., RQ is selected in such a way that each integer RJ divides N, and Ni = r1 + r2..... + RJ [21].

6. Authentication

Authentication is required in order to both safeguard computer programs and participate in network activities. Because the Internet of Things (IoT) and a large number of social networking applications call for efficient authentication of a group of participants, whether it be user authentication or device authentication[22]. In the present blockchain-based authentication systems, the data relating to the authentication of several Internet of Things devices may be kept in a single blockchain [23]some limitations and challenges of existing blockchain based authentication schemes as follows :

- **Scalability issue:** As IoT has gained popularity, the identity authentication issue in IoT has spread to other IoT applications that have the same authentication requirements, or what we refer to as "cross-domain" authentication.
- **Low authentication efficiency:** Although blockchain-based authentication schemes enable distributed management of the authentication process and no longer rely on a single centralized authentication center, the authentication process for IoT applications still requires an authentication server to handle authentication requests.
- **Storage Overload**: Due to the nature of a blockchain, a complete node must keep every block and the transactions they contain. All of the registered IoT endpoint authentication data must first be stored on each authentication server.

7. Fingerprint Authenticity

Data security calls for the protection of any information sent over the air throughout the voting process. An electronic voting system (also known as electronic voting) can be used instead of a manual voting system . The procedure may be made more transparent and make

it simpler to achieve the standards by introducing electronic voting. the verification of users using biometrics, particularly fingerprints; the encryption of secret and public keys to ensure data confidentiality. Compared to a PIN or password, a fingerprint is significantly more challenging for attackers to transmit, spread, or even fabricate. fingerprint once acquired, the properties are kept in the database for further use for verification [1].

8. The Proposed Electronic Voting System

The proposed electronic voting system uses blockchain technology and system requirements, which are described in detail below. For a nationwide voting system to be effective, it must be obtained The following criteria: integrity, accessibility and availability, privacy, transparency, and affordability. In addition, the system must be economical for voters and easy for the government to maintain, and it must be less expensive than the traditional paper ballot system. The system is built on two concepts: hashing and encryption, both of which are discussed below. The Blockchain structure that has been proposed is depicted in the figure. The system is comprised of the following components: Subscribers (also known as "voters"), Organizers (also known as "Election Authority"), and a cryptographic algorithm. Figure 3 depicts the entire planned system, including all of its components. The following steps are included when a voter wants to vote at election time. Steps before voting:

1) Voters must register in the voting system. In the first step, the voter chooses a password to log in and the private key for signing. Via Raspberry Pi via a fingerprint scanner

2) If the registration is successful in the system, then

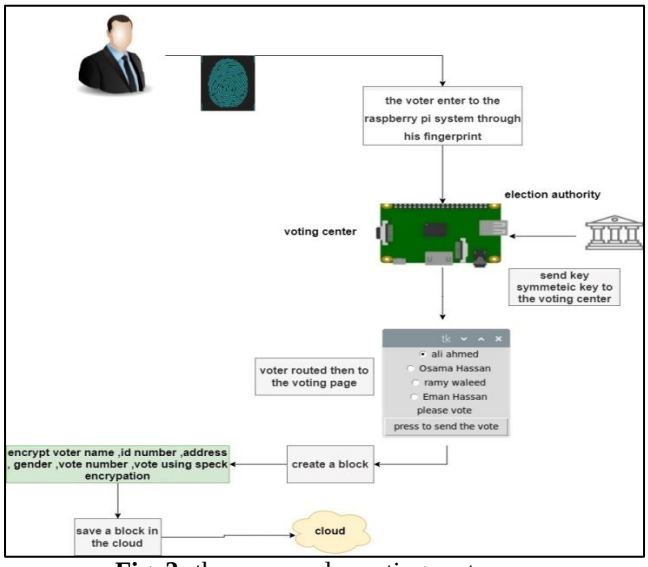

Fig. 3: the proposed e-voting system.

The voter gets a voter ID card. The voter's private key signs the encrypted vote. The generated voter information is stored in a file Online voter server. This is the first block from the Blockchain(encrypt voter name, id number, address, gender, and number. vote using speck encryption). The block itself is programmed using python language as a class in the following figure 4. Each voting block consists of (index, name, vote, vote, date, previous version, current hash), then mining is performed to find six zeros at the beginning of the block only and then add the block to the previous block. The keygenrator is bakers chaotic map that is programmed also using Pyhton3.8 that is celar in the following figure 5.

```
Block
+ ID: number
+ name: string
+ address: string
+ phone: number
+ vote_ID: number
+ vote: number
+ previous_hash : number
+ current_hash: number
+ SHA-256(TEXT)
```

Fig. 4. The class of blockchain in Python language.

Algorithm (3.4) : Mining New Hash Algorithm		
Input	:	Index, f_name, l_name, date, address, voter_id, previous-hash, prefix_zeros = 3 , max_nonce= 1000.000
Output	:	Hash SHA-256 for new block
1	:	Start
2	:	For nonce in range (0 to Max_nonce) : A: input text T(Index, f_name, l_name, date, address, voter_id, previous-hash) + string (nonce) B: new_hash = SHA-256(T) C: if new_hash is start with (0000) then : Return new_hash Go to 3
3	:	End

```
from math import sqrt
def keygen(x,y,a,size):
    key = []
    key1 = []
    xkey = []
    ykey = []
    for i in range(size):
        if (0<=x<=0.5):
            x= 2 * x
            y = a * y
        elif (0.5 <x <= 1):
            x = 2 * x-1
            y = a * y +0.5

        xkey.append(x)
        ykey.append(y)
        key.append(int((x * pow(0,3))% 256))
        key1.append(int((y * pow(10, 6)) % 256))

    return xkey,ykey,key,key1
def SelectPrime(n):
    primno = 0
    p = 0
    if (n>1):
        for i in range(2,int(sqrt(n))+1):
            if(n % i ==0):
                primno = 1
                break
            if (primno == 0) :
                p=n
    return p
```

Fig. 5: bakers chaotic map key generator.

For a 512-bit input message, sha-256 calculates a 256-bit hash value. Figure 6 shows the hash calculation for a long message. The hash value for a long message may need to be calculated in the actual world. The message is broken into numerous 512-bit data blocks in such instances. PADDINg is added if the last block is less than 512 bits. The sha-256 algorithm computes intermediate hash values for data blocks, with the current block's hash result serving as the initial input hash for the following data block's hash computation. The hash value of the entire message is calculated from the result of the final data block.

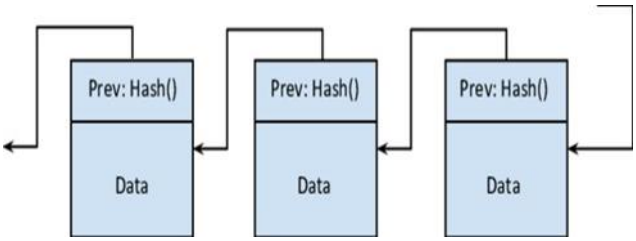

Fig. 6: hashing process in a blockchain system.

9. Experimental Results

The blockchain e-voting system has been built using Flask framework under raspeian in Raspberry pi microcomputer using python 3.10. the user firstly enters the homepage of the e-voting system and is asked to scan his fingerprint and upload the picture as in figure 7:

Fig. 7: Scanning the fingerprint login web page.

After uploading the fingerprint, the system shows the voter fingerprint while checking if the fingerprint matches the saved one in the database. See figure 8. The voter when authenticated using his fingerprint as in figure 9 below after finding the fingerprint of the entered voter in the fingerprint database. The system allows the voter to vote using the voting page of the system as in figure 10.

Fig. 8: Scanning fingerprint validation.

Fig. 9: The uploaded fingerprint matched a saved one in the database.

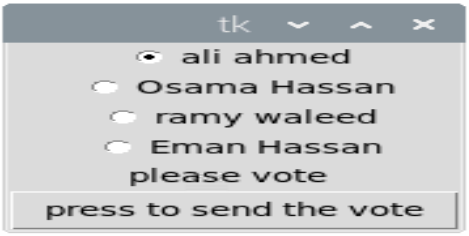

Fig. 10: The voting page where the voter can choose his party.

The blockchain e-voting system has been tested in time and key generator randomness. The proposed approach depends on the Speck encryption algorithm that is used to encrypt the whole block that consists of (ID, name, address, age, vote_id, vote, previous hash, current hash) as in figure . The size of the Blockchain consisted of 2000 was 200 kilobytes. The test begins with computing the time consumed in generating and encrypting 2000 blocks in a chain in the proposed electronic election office. The tests have been executed using a raspberry pi environment with CPU cortex A 53 and 1 Gigabyte RAM. The same test was repeated using the AES block cipher algorithm. The results were registered in table 1.

Table 1. time comparison between speck lightweight block and AES block cipher.

Speck lightweight block cipher	**AES block cipher**
8 minutes	14 minutes
[24]	150 minutes
[25]	14 minutes for just 5 blocks

The system design key generator's key randomness is compared to RSA using NIST tests. The baker's chaotic key generator used with the Speck cipher was also tested in the scope of randomness. There are fifteen randomness tests implemented:

1. Monbiot measures the proportion of zeros and ones in the whole sequence. Check if the amount of ones and zeros in a row matches a random series.
2. Frequency test within a block: A second frequency test is performed during a block. The ones in an M-bit block are checked to see if they are sparse randomly
3. Run test: Looking for a continuous series of identical bits. Before and after each k-bit run is a bit of the opposite value. Tests the length of one-to-zero runs against a random sequence. In this test, 0s, and 1s oscillate at the same rate.
4. Longest run of ones: The fourth one is the longest in M-bit blocks. The longest run of ones in the tested sequence is compared to a random series.
5. Cumulative sums (forward): test the focus of the fifth Test, which is cumulative sums (ahead test).
6. Cumulative sums (backward): which is the backward test. Both tests measure the maximum excursion (from zero) of the random walk, defined by the sequence's cumulative total of adjusted (-1, +1) digits.
7. Binary matrix run test: Check for linear dependence among fixed-length substrings of the original sequence by constructing matrices of sequential zeroes and ones from the sequence and checking for linear dependence among the rows or columns of the produced matrices. The statistic of interest is the divergence of the matrices' rank (or rank deficit) from a theoretically expected value.
8. Non-overlapping template match: Sequences with too many or too few occurrences of a specific aperiodic pattern is rejected by this test and considered not random
9. Serial test: The (generalized) serial test is a set of procedures for determining the consistency of pattern distributions of varying lengths.

10. Approximate entropy test: The string's approximate entropy characteristics are based on repeated patterns. This entropy. in this case, the sequence to be m-irregular (m-random) if its approximate entropy takes the largest possible value
11. Random excursions test: This test uses a one-dimensional random walk to consider consecutive sums of binary bits (plus or less simple ones). The test looks for outliers in the random walk's number of trips to a specific "state," which can be any integer value.
12. Discrete Fourier transforms: The peak heights in the sequence's Discrete Fourier Transform are the focus of this exam. This test aims to find periodic features (repetitive patterns that are close together) in the tested sequence that indicate a deviation from the randomness assumption. The goal is to see if the number of peaks exceeding the 95 percent criteria differs considerably from the 5 percent barrier.
13. Linear complexity test: The length of a linear feedback shift register is the topic of this test (LFSR). This test is used to see if the sequence is complicated enough to be called random. Longer LFSRs are associated with random sequences. Non-randomness is implied by an LFSR that is too short.
14. Random excursions variant tests: The actual values used in these cases are shown in parenthesis next to the statistical test's name. Each sample has a length of 1,000,000 bits. Only one of the potential eight and eighteen P-values for “the random excursions and random excursions variant tests" has been published.
15. Longest runs of ones in a test: The goal of this test is to see if the longest run of ones in the tested sequence corresponds to the longest run of ones that would be expected in a random sequence.

The baker's randomization successes in all that fifteen tests. The tests have been executed using python 3.10. the result of the randomness tests has been listed in table 2.

Table 2. The randomness tests table

Test	Baker key generator randomness
Monbiot	Yes
Frequency test within a block	Yes
Run test	Yes
Longest run of ones	Yes
Accumulative sums (backward)	Yes
Accumulative sums (backward)	Yes
Binary matrix run test	no
Non-overlapping template match	Yes
Serial test	Yes
Approximate entropy test	Yes
Random excursions test	Yes
Discrete Fourier transform	Yes
Linear complexity test	No
Random excursions variant tests	Yes
Longest runs of ones in a test	No
Monobit	Yes
Frequency check within a block	Yes
Test Run	Yes
The Longest run of ones	Yes
Accumulative Sums (Backwards)	Yes
Accumulative Sums (Backwards)	Yes

The fingerprint verification model also has been tested using a database FVC2002 DB1 databases containing images of 100 different fingers with eight impressions for each finger. Figure 11 represents a sample of the fingerprint photo. The image size is 388X374 (142kpixel). The experiments show that the fingerprint verification system used in the e-voting system achieved 99% accuracy in specifying the targeted fingerprint with the KNN classifier.

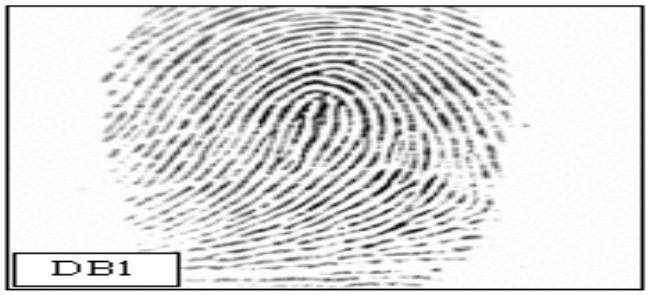

Fig. 11: a sample of the fingerprint from database FVC2002 DB1.

10. Conclusion

The E-voting system has become one of the improving democracies nowadays. E-voting systems let many people participate in elections either from home or through elections offices. The proposed approach depends on Blockchain as a public ledger to save voters' ballots. The Blockchain is a public ledger that enables

the data to be read publicly. So, the data election must be encrypted to ensure privacy and confidentiality for each voter's block. Securing a voting block for each voter is achieved using a lightweight block cipher that can consume less time than the traditional AES cipher algorithm. The speck encryption algorithm is improved using baker's chaos key generator. Authentication is also achieved through adopting a fingerprint logging system. This fingerprint system was implemented using SIFT and KNN classifier. The efficiency of the fingerprint logging system got 0.99 % of accuracy. This research achieved two goals. First, confidentiality by using a speck lightweight block cipher that can work in stations and devices with limited processing power in a suitable time for each block in the Blockchain. The second goal is to ensure the fingerprint login system's authentication to let registered voters in the database vote.

Reference

[1] T. Ahmad, A. H. Azizah, and H. Studiawan, "Fingerprint-Based Authentication and Cryptography in An E-Voting System," *Jurnal Manajemen Informatika*, vol. 2, no. 2. pp. 7–11, 2013. [Online]. Available: http://jurnalmahasiswa.unesa.ac.id/article/10004/65/article.pdf.

[2] K. Dhinakaran, P. M. Britto Hrudaya Raj, and D. Vinod, *A Secure Electronic Voting System Using Blockchain Technology*, vol. 166. IEEE, 2021. doi: 10.1007/978-981-15-9689-6_34.

[3] K. Srikrishnaswetha, S. Kumar, and M. Rashid Mahmood, "A Study on Smart Electronics Voting Machine Using Face Recognition and Aadhar Verification with IOT," *Lecture Notes in Networks and Systems*, vol. 65. pp. 87–95, 2019. doi: 10.1007/978-981-13-3765-9_10.

[4] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," *Futur. Gener. Comput. Syst.*, vol. 105, pp. 13–26, Apr. 2020, doi: 10.1016/j.future.2019.11.005.

[5] S. Kanchana, "Fingerprint Based Biometric Authentication in Iot for Resolving Security Challenges," *International Journal of Research and Analytical Reviews*, vol. 5, no. 4. pp. 1000–1003, 2018. [Online]. Available: www.ijrar.org

[6] A. K. Koç, E. Yavuz, U. C. Çabuk, and G. Dalkiliç, "Towards secure e-voting using ethereum blockchain," 2018. doi: 10.1109/ISDFS.2018.8355340.

[7] A. A. Altun and M. Bilgin, "Web based secure e-voting system with fingerprint authentication," *Scientific Research and Essays*, vol. 6, no. 12. pp. 2494–2500, 2011.

[8] V. Kiruthika Priya, V. Vimaladevi, B. Pandimeenal, and T. Dhivya, "Arduino based smart electronic voting machine," in *Proceedings - International Conference on Trends in Electronics and Informatics, ICEI 2017*, 2018, vol. 2018-Janua, pp. 641–644. doi: 10.1109/ICOEI.2017.8300781.

[9] "ELECTRONIC VOTING SYSTEM BASED ON FINGERPRINT RECOGNITION AND RADIO," no. January, pp. 0–11, 2018.

[10] B. Shahzad and J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology," *IEEE Access*, vol. 7, pp. 24477–24488, 2019, doi: 10.1109/ACCESS.2019.2895670.

[11] T. N. N.R.Sathis Kumar, "FINGERPRINT BASED ATTENDANCE SYSTEM USING RASPBERRY PI." pp. 46–50, 2019.

[12] B. Sudharsan, V. Rishi Tharun, N. M. P. Krishna, J. Boopathi Raj, S. M. Arvindh, and M. Alagappan, "Secured Electronic Voting System Using the Concepts of Blockchain," in *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2019*, 2019, pp. 675–681. doi: 10.1109/IEMCON.2019.8936310.

[13] K. Isirova, A. Kiian, M. Rodinko, and A. Kuznetsov, "Decentralized electronic voting system based on blockchain technology developing principals," 2020.

[14] A. Shah, N. Sodhia, S. Saha, S. Banerjee, and M. Chavan, "Blockchain Enabled Online-Voting System," *ITM Web Conf.*, vol. 32, p. 03018, 2020, doi: 10.1051/itmconf/20203203018.

[15] M. M. Ganesan, M. M. Shafeek, K. Thiyagarajan, M. Logesh, and M. Akash, "Biometric E-Voting With Multi Factor Authentication Using Iot Technology," *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 13. pp. 759–761, 2021. [Online]. Available: https://www.freepdfconvert.com/membership

[16] S. P. Gupta and A. M. T. Computer, "E-Voting using Blockchain." Journal of Physics: Conference Series, 2021.

[17] B. A. O. and O. M. Olaniyi, A. A. Aboaba, and O. T. Arulogun, "Multifactor authentication technique for a secure electronic voting system."

[18] A. Ben Ayed, "A Conceptual Secure Blockchain Based Electronic Voting System," *Int. J. Netw. Secur. Its Appl.*, vol. 9, no. 3, pp. 01–09, May 2017, doi: 10.5121/ijnsa.2017.9301.

[19] A. Md. Shahriare, S. Niloy, H. Md. Inzamam-Ul, and B. Mohammed Golam Sarwar, "IRJET-Blockchain-Based Secured E- Voting System to Remove the Opacity and Ensure the Clarity of Election of Deve ...," *International Research Journal of Engineering and Technology*. 2020. [Online]. Available: www.irjet.net

[20] A. Bossert, S. Cooper, and A. Wiesmaier, "A comparison of block ciphers SIMON , SPECK , and KATAN," 2016, [Online]. Available: https://www.cdc.informatik.tu-darmstadt.de/fileadmin/user_upload/Group_CDC/Documents/Lehre/Seminar_IoT/2016-09-05_TR_SimonSpeckKatan.pdf

[21] "A Framework for Digital Image Encryption using Chaotic Baker Map with SHA Algorithm," *Int. J. Innov. Technol. Explor. Eng.*, vol. 9, no. 2, pp. 4093–4097, Dec. 2019, doi: 10.35940/ijitee.b7716.129219.

[22] H. Y. Chien, "Group Authentication with Multiple Trials and Multiple Authentications," *Secur. Commun. Networks*, vol. 2017, p. 7, 2017, doi: 10.1155/2017/3109624.

[23] X. Jia, N. Hu, S. Yin, Y. Zhao, C. Zhang, and X. Cheng, "A2Chain: A Blockchain-Based Decentralized Authentication Scheme for 5G-Enabled IoT," *Mobile Information Systems*, vol. 2020. 2020. doi: 10.1155/2020/8889192.

[24] "ETRI Journal - 2020 - Abuidris - Secure large-scale E-voting system based on blockchain contract using a hybrid consensus.pdf."

[25] J. ABEGUNDE, "ADEVA: A Decentralized Electronic Voting Application Using Blockchain Technology." 2022. [Online]. Available: http://dx.doi.org/10.36227/techrxiv.18331538.v1%0Ahttps://ndownloader.figshare.com/files/33094067