Internet – Voting System Using Blockchain Technology

S.Thiruvenkatasamy[1], L.Barathkumar[2], P.Navinkumar[3], K.Ranjith[4], A.Vigneshwaran[5]

[1]Assistant Professor, Dept.of Computer Science and Engineering(CSE), Nandha College of Technology, TamilNadu, India
[2,3,4,5]UG Student, Department of CSE, Nandha College of Technology, TamilNadu, India

---***---

Abstract - *In recent years, the blockchain has gained popularity, and its underlying consensus algorithms have become the subject of research. Most consensus mechanism research is now focused on public blockchains and is based on existing consensus mechanisms or complex distributed algorithms. Various application scenarios based on the consortium blockchain have been developed, although few researchers have focused on proprietary consistency algorithms. Electronic voting has gradually replaced paper voting to avoid redundancy and inconsistencies. Due to security and privacy vulnerabilities noticed over time, the historical viewpoint offered in the last two decades implies that it has not been as successful. This paper proposes a methodology for ensuring data security by employing effective hashing techniques. This paper introduces the concepts of block formation and block sealing. The implementation of a block sealing concept aids in the customization of the blockchain to match the requirements of the polling process. It is advised that a consortium blockchain be used, which ensures that the blockchain is held by a governing body (e.g., an election commission) and that unauthorized access from the outside is impossible. The framework suggested in this study uses the customizable blockchain technique to discuss the effectiveness of the polling process, the value of hashing algorithms, block formation and sealing, data accumulation, and result declaration. It claims to understand blockchain's security and data management concerns and to provide a better representation of the electronic voting process.*

Key Words: Blockchain voting, I-voting, E-voting, Ranked voting systems, SHA, Future voting.

1. INTRODUCTION

The implementation of e-voting has the same obstacles as any other "e"-related topic, such as e-government. Legislators or administrators may anticipate simply uploading a paper version of a service or process on the internet. Unfortunately, the reality is more complicated, and nowhere is this more true than electronic voting. Institutions such as the 'Election Commission' were established in many parliamentary democracies to improve the voting process.

Along with establishing the procedure and legislation for conducting elections, the institutions established voting districts, electoral processes, and balloting systems to aid in the conduct of transparent, free, and fair elections. Since the inception of the voting system, the concept of secret voting has been introduced.

Because public faith in democratic systems is growing, public trust in voting systems mustn't deteriorate. Since the Committee of Ministers adopted the Council of Europe Recommendation on legal, operational, and technical standards for e-voting in 2004, there have been numerous developments in the field of e-voting.

Some countries no longer use e-voting, while others have experimented with it and decided not to implement it. Other countries, on the other hand, are continuing to run pilot programs and implement e-voting. Other elections, such as student councils or youth boards, have used electronic voting. Some countries or organizations want to start piloting e-voting schemes but haven't looked into all the possibilities. This document was written specifically for them.

2. METHODOLOGY

We will adopt a process to address the following activities.

2.1 MODELING OF ENTIRE E-VOTING PROCESS

The system modeling helps in drawing the entire system on paper to develop a ***deep*** understanding of the system and to identify errors and flaws that can be observed before the system can be implemented.

2.3 DETERMINATION OF THE TECHNOLOGY PLATFORM TO ENSURE PRIVACY AND SECURITY

The e-voting process requires the features like privacy, security, anonymity, and verifiability as the core function of this solution, it is important that the choice of the underlying technology is consistent to meet these challenges. It has been identified that Blockchain technology sufficiently deals with all such challenges.

2.4 DEVELOPMENT & TECHNOLOGY INTEGRATION WITH THE PERCEIVED E-VOTING MODEL

Based on the system model, the system will be developed and will be integrated with the baseline technology.

3.VOTER AUTHENTICATION

Any voting system should have voter authentication. A voting system must ensure that a voter:

- Is exactly who they claim to be
- Has the right to vote when authenticating them.
- Has not yet voted

A system that does not authenticate voters will be unable to prevent duplicate voting, voter impersonation, and another election tampering. In older voting systems, polling station staff frequently confirm voter identity manually. In online voting systems, however, digital identity verification techniques should be implemented.

A person's identity can now be verified using the following information:

- Digital identification
- Keys to personal security
- Authenticated mobile devices

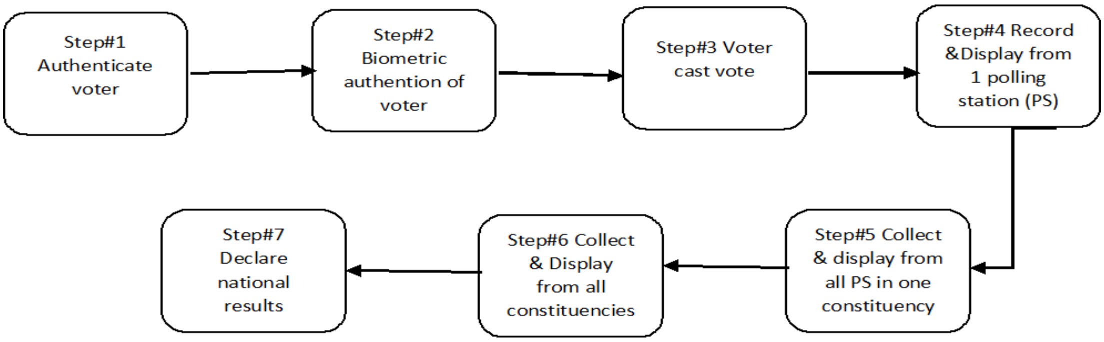
Step#1 Authenticate voter
Step#2 Biometric authention of voter
Step#3 Voter cast vote
Step#4 Record &Display from 1 polling station (PS)
Step#5 Collect & display from all PS in one constituency
Step#6 Collect & Display from all constituencies
Step#7 Declare national results

Fig-1 : The electronic voting process and contributing entities

The voter is routed (Fig-1) to the voting screen to cast his ballot after passing the authentication check. Each candidate's name and relevant party insignia are displayed on the voting machine, and the voter can vote as he likes. The voter's vote is recorded on the confirmation screen, and the voter's confirmation is sought.

a) A voter can only vote once, and once that vote is made, the voter's voting record is marked as "voted," making it impossible for them to vote again. A voter's name can be blocked or removed from the list of eligible voters for the current elections after he has cast his vote.

He developed a method in which voters can vote many times, with each vote canceling the previous one in his work on internet voting. If the voting procedure is to be completed in one day and roughly 110 million people are required to vote, as in Pakistan, this does not appear to be a practical approach.

b) The polling process continues until the voting time ends or all voters on the voter list have cast their ballots.

c) The polling station results are announced, together with the vote totals for each candidate. The process is repeated for all voting stations in the constituency, with the sum of all polling station results determining the constituency's outcome. Similarly, all of the constituency results are pooled to provide national election results. The voting procedure and the results are depicted in this diagram.

d) Fig-2 illustrates the method's three-layered operation. The first layer (Who) defines the system's participants, such as voters, polling employees, and polling machines, who can interact with the polling process. The second layer (How) is focused on determining the necessary tools and technologies to ensure that the process runs smoothly.

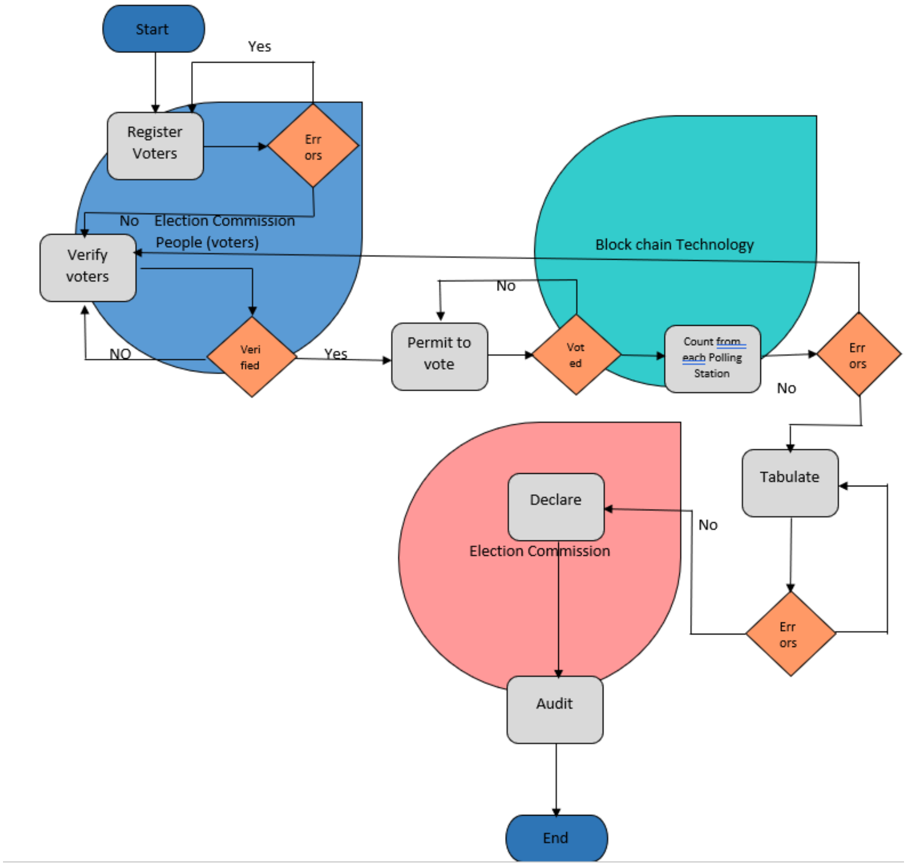

Fig-2 : The electronic voting process with institutions involved

4.HASHING & BLOCKCHAIN TYPES

Previous events in a person's life have been timestamped and connected. They are impossible to reverse or duplicate in any way. Many others are also aware of the events' correctness and may double-check the facts if necessary. The blockchain comes into play here, as it creates an irreversible, distributed, public ledger to store data chunks. The events can be represented as data blocks that are connected to form an invisible blockchain of our lives. A computational blockchain is similar in concept. In the past, a computational blockchain was an open and distributed ledger that, depending on the conditions, could be accessed and amended by anybody. The goal is to establish a trust-based system in which records cannot be altered.

4.1 TYPE OF BLOCKCHAIN

The three types of blockchain are public blockchain, private blockchain, and consortium blockchain. Publicblockchains, such as Bitcoin and Ethereum, allow anyone, from anywhere, to join and be relieved at his discretion. This is demonstrated by the complicated mathematical functions. The private blockchain is the corporation's internal-public ledger, and the company that owns the blockchain provides access to it. Block construction and mining are much faster in a private blockchain than in a public blockchain since there are fewer nodes. Instead of consensus, membership standards are developed to better manage blockchain transactions in the consortium blockchain, which exists among corporations or groups of firms. This study uses a consortium since the blockchain will be regulated by a national authority in the country.

The blockchain's foundation is the block. The transactions to be written to the system are contained in the body of a block, which has a header and a body. The block's header contains information about the block, such as the previous hash, nonce value, and difficulty, as well as the timestamps of the block and transactions. The length of the block is unknown. however, it is thought to be between 1 and 8 megabytes. The block's header uniquely identifies the block to be put.

4.2 HASHING

The technique of converting an arbitrary and variable size input to a fixed size output is known as hashing. Encryption converts data into a secure format that cannot be read unless the recipient possesses a key. The data can be any size in encrypted form and is typically just as long as it is unencrypted. By using SHA-256 hashing, a 512-bit string of data can be turned into a 256-bit string.

Table -1 : Hashing algorithms.

Name	Input block size	Message limit (bits)	Hash code size
MD5	512	264	128
SHA-1	512	264	160
SHA-256	512	264	256
SHA-512	1024	2128	512

The MD5 algorithm gives a 128-nit or 32-character hash output and is widely used for hashing. MD5, which came after Md2, Md3, and Md4, is the most current algorithm in the sequence. The algorithm was designed as a cryptographic hashing approach. however, it has weaknesses that limit the number of unique hash values it can generate, making it vulnerable. In 1996, Hans Dobbertin created the RIPEMD (Race Integrity Primitive Evaluation Message Digest) family of hash algorithms. This approach was developed as a safer alternative to MD5. Some of the versions that have emerged throughout time are RIPEMD-128, RIPEMD-160, RIPEMD256, and RIPEMD-320.

The MD5 technique is frequently used for hashing and produces a 128-nit or 32-character hash output. The most recent algorithm in the sequence is MD5, which comes after Md2, Md3, and Md4. Although the technique was intended to be used for cryptographic hashing, it has flaws that limit the number of unique hash values it can generate, rendering it vulnerable. Hans Dobbertin developed the RIPEMD (Race Integrity Primitive Evaluation Message Digest) hash algorithm family in 1996. This method was created to be a safer alternative to MD5. RIPEMD-128, RIPEMD-160, RIPEMD256, and RIPEMD-320 are some of the variations that have appeared over time.

5. PROOFS

5.1 Proof of Work:

The proof of work idea deals with mining/block creation in such a way that it can be demonstrated that a significant amount of effort was put into solving the mathematical issue given by the blockchain's development. With each new block constructed, the mathematical difficulty grows, making block construction a challenging and gratifying activity. To introduce increasing levels of complexity, hash functions, Markle trees, and the nonce value are used.

5.2 Proof of Stake:

The proof of stake concept is based on the blockchain's identification of stakes. The owners of assets have a higher priority when it comes to forming blocks. It's impossible to dismiss the notion that a few block authors control the entire blockchain through their holdings. This method can be employed in a consortium blockchain or a private blockchain where the holding corporations need administrative access.

5.3 Proof of Burn:

The proof of stake concept is based on the blockchain's identification of stakes. The owners of assets have a higher priority when it comes to forming blocks. This method can be employed in a consortium blockchain or a private blockchain where the holding corporations need administrative access.

The proofs described above are commonly used in bitcoin mining and are well-known in the literature. However, the application of blockchain varies in various industries, and the proofs presented in this section may not be applicable in practice; however, based on the nature of the application, a modification to the implementation may be requested. The answer to the question is determined by the nature of the application area where blockchain technology will be deployed.

This study examines the use of blockchain in secure electronic voting, and it is found that the current blockchain may require some changes for the following reasons. Creation of Block, Block creation is a critical part of the election process; without it, voters will be unable to record their ballots. As a result, the bricks must be constructed without first solving the mathematical puzzles that comprise the evidence of labor. Proof of stake and proof of burn will be irrelevant because each produced block will be held by a single individual, as it will be a consortium blockchain. Sealing of Blocks:

Voters can cast ballots, and their choices are recorded in blocks. The blocks must be sealed using hash functions, the Merkle tree, and the nonce function once the polling period has ended. Sealing is not mentioned in any of the extant theories.

5.3.1 Polling Time:

Because the voting process takes between 8 and 10 hours, the blocks must be constructed, sealed and secured during that period. Proof of work, proof of stake, and proof of burn are not suitable for use in trustworthy electronic voting since they require a lengthy process to apply.

5.3.2 Result Delay:

After the polling process is completed and the results are published, there will be no need to continue mining or block generation. The proof of labor and proof of stake algorithms consume (waste) a substantial amount of computational resources over time because they recursively repeat themselves. Because the suggested system uses few resources, it is cost, time, and energy-efficient.

Given the limitations of existing algorithms, it's vital to build an algorithm that can solve the problem while also overcoming the limitations of existing algorithms when applied to the field of trustworthiness. The previous block's hash is mixed with a fresh random integer, and the result is hashed once again to ensure that the hash outcome function cannot be solved without the ability to tackle NP-hard problems.

The goal of blockchain-based electronic voting is to provide a safe voting system that can gain the trust of all stakeholders, including voters, political parties, and government agencies.

The security of the casting vote is ensured through block creation, block sealing, and content hashing. The produced block is secure and employs the SHA-256 algorithm. The blocks are sealed with the SHA-256 algorithm's unique hashes, which are known to be sufficiently secure for the e-voting process.

In terms of accepting and delivering the hash value that is used to stitch the block with the chain, each block (except the first and last block) is associated with the next and previous block, building Merkle trees.

Fig 3 - Block 2… n= hash (hash (pairs of transactions) +hash (Block(n-1)) +Random Number (length n+2)

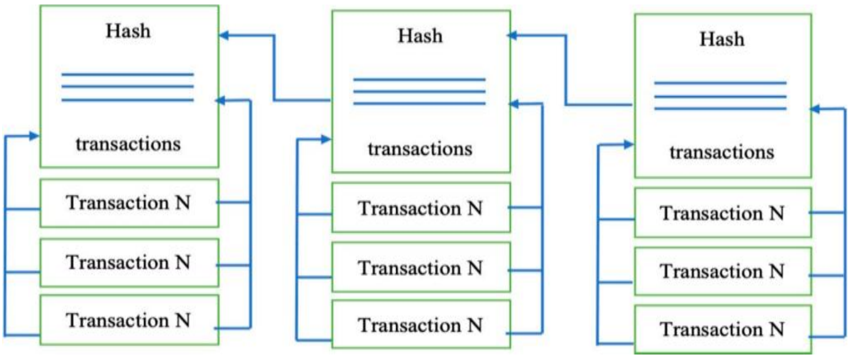

Fig-3: Blockchain-based hashing mechanism

The method for sealing the blocks is demonstrated. The sealed block reflects the actual block once it has been sealed. The sealed blocks are represented in such a way that they are linked using a chained hash key, with the key from one block being utilized by the next block to generate the next hash, and so on until all of the blocks are completed.

During the process of applying the hash function to the transactions, a pair of transactions (sequential) are chosen and the hash function is applied to them. All pairs of transactions are sequentially hashed, and a hash is created using the SHA256 method based on all hashed data. It's time to use a block's hash after it's been generated.

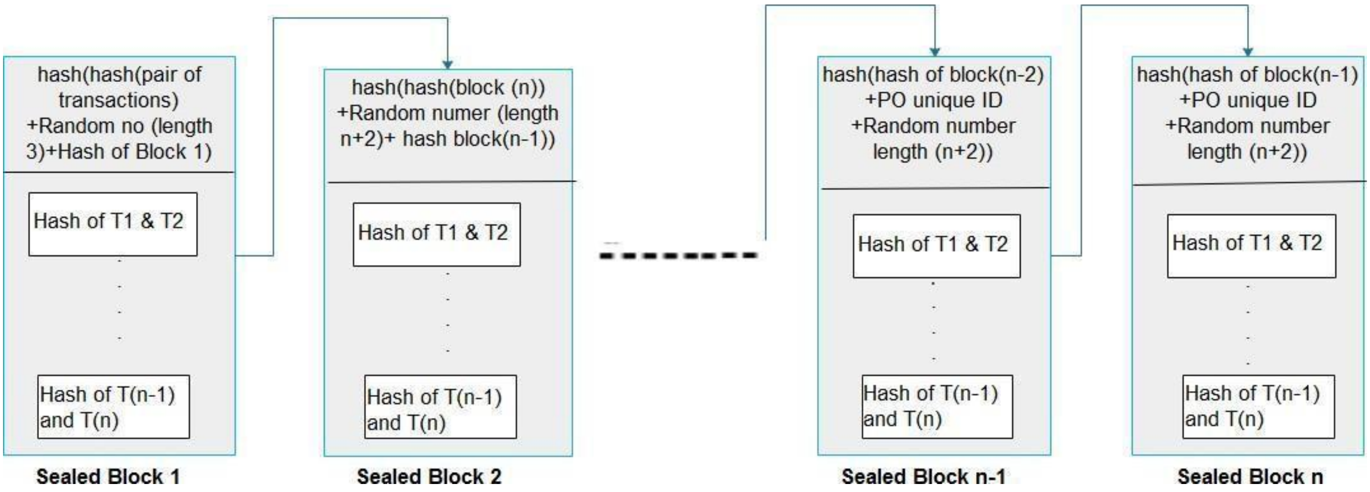
hash(hash(pair of transactions) +Random no (length 3)+Hash of Block 1)
Hash of T1 & T2
Hash of T(n-1) and T(n)
Sealed Block 1
hash(hash(block (n)) +Random numer (length n+2)+ hash block(n-1))
Hash of T1 & T2
Hash of T(n-1) and T(n)
Sealed Block 2
hash(hash of block(n-2) +PO unique ID +Random number length (n+2))
Hash of T1 & T2
Hash of T(n-1) and T(n)
Sealed Block n-1
hash(hash of block(n-1) +PO unique ID +Random number length (n+2))
Hash of T1 & T2
Hash of T(n-1) and T(n)
Sealed Block n

Fig -4: Conversion of blocks to sealed blocks.

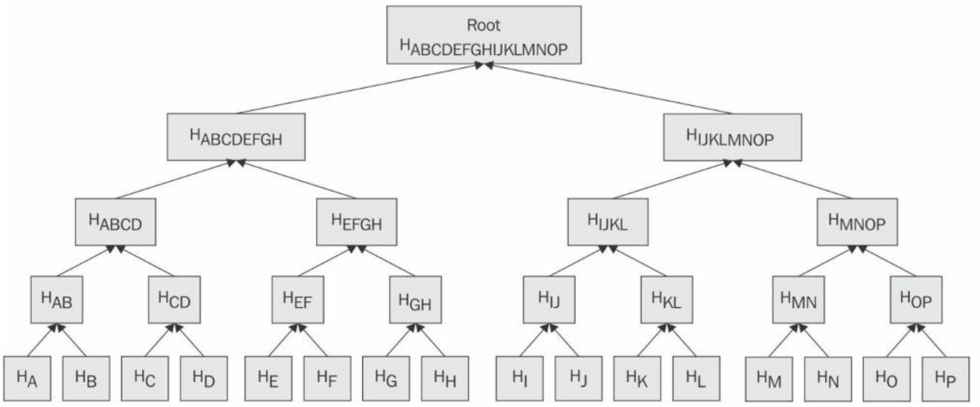

Fig -5: Distributed block structure.

6. VOTING RESULT COLLECTION

Thanks to the blockchain's excellent node organization, the findings are derived from the data stored on the blocks. The chain of blocks at the bottom collects data in containers (blocks) that are serially connected by an algorithm.

A Merkle tree, on the other hand, is retained to track the block's distribution and degree of breakdown. Fig 4 depicts the logical allocation of national assembly seats and polling places in each national assembly seat.

Fig 5 shows the Merkle tree representation of the system, and it can be observed that each transaction's record is saved at the top level, i.e level 0. The national seats are depicted at level 1, whereas polling stations in any region are depicted at level 2.

Each transaction in any block can be directly discovered and documented by keeping them dispersed and open for transactions while preserving the contents with the BSJC technique of proof of completion.To increase and maintain voter trust, it is vital to tell voters about the results of their ballots. To make the process visible, a trail of the voters who cast their votes is established at the end of the polling session.

7. LIMITATIONS

Several assumptions are considered in this research.

a) The voter understands his constitutional rights and the polling process. Within the time limit, each voter must be able to vote.

b) All voter information is public and available for verification. The data must be submitted by the data management agency at the national level. It is also expected that internet connectivity is always available, with no communication delays or pauses due to internet outages.

c) Polling officials should be familiar with the technology and able to help voters through the procedure.

8. CONCLUSION

The purpose of this study is to examine and evaluate electronic voting systems based on blockchain technology. First, the blockchain concept and its applications are discussed, followed by existing electronic voting methods. The blockchain's potential to improve electronic voting, present solutions for blockchain-based electronic voting, and future research routes on blockchain-based electronic voting systems are all important considerations. Legislators, technologists, civil society, and the general public must all think deeply about some issues. This research proposed a framework based on an adaptable blockchain that can address challenges in the polling process such as choosing a suitable hash algorithm, choosing blockchain updates, managing voting data, and voting process security and authentication. Because of its adaptability, blockchain has been able to adapt to the dynamics of electronic voting.

REFERENCES

[1] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf. (accessed on 28 July 2020).

[2] Prashar, D.; Jha, N.; Jha, S.; Joshi, G.; Seo, C. Integrating IoT, and blockchain for ensuring road safety: An unconventional approach. Sensors 2020, 20, 3296. [CrossRef]

[3] Mohanta, B.K.; Jena, D.; Panda, S.S.; Sobhanayak, S. Blockchain technology: A survey on applications and security privacy challenges. Internet Things 2019, 8, 100107. [CrossRef]

[4] Hussain, H.A.; Mansor, Z.; Shukur, Z. Comprehensive Survey And Research Directions On Blockchain IoT Access Control. Int. J. Adv. Comput. Sci. Applications. 2021, 12, 239–244. [CrossRef]

[5] Schinckus, C. The good, the bad and the ugly: An overview of the sustainability of blockchain technology. Energy Res. Soc. Sci. 2020, 69, 101614. [CrossRef]

[6] Typographic dimensions and conventional wisdom: A discrepancy? Technical Communication 46 (1): 67-74. Wright, Patricia. 1988. Issues of content and presentation in document design. In Handbook of human-computer interaction, ed. M. Helander, 629-652. New York: North-Holland. Wright, Patricia. 1998.

[7] Printed instructions: Can research make a difference? In Visual information for everyday use: Design and research perspectives, ed. Harm J. G. Zwaga, Theo Boersema, and Henriette C. M. Hoonout, 45-66. London: Taylor and Francis. Zimmerman, Donald E. and Terri Prickett. 2000.

[8] A usability case study: Prospective students' use of a university web page. Innings: STC's 47th Annual Conference. Society for Technical Communication. http://www.stc.org/ConfProceed/2000/PDFs/00099.pdf (accessed December 4, 2007).

[9] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," in*Cryptographic Hardware and Embedded Systems*. 2004, pp. 357–370.

[10] Y. Stein and H. Primo, "Programmable data encryption engine for advanced encryption standard algorithm," U.S. Patent 7 508 937 B2, 2009. Accessed: Aug. 1, 2018. [Online]. Available: https://patents. google.com/patent/US7508937B2/en [10] B. Shehzad, K. M. Awan, M. I.-U. Lali, and W. Aslam, "Identification of patterns in failure of software projects," *J. Inf. Sci. Eng.*, vol. 33, no. 6, pp. 1465–1480, 2017.

[11] A. M. Abdullatif, B. Shahzad, and A. Hussain, "Evolution of social media in scientific research: A case of technology and healthcare professionals in Saudi Universities," *J. Med. Imag. Health Inform.*, vol. 7, no. 6, pp. 1461– 1468, 2017.

[12] B. Shahzad, "Identification of risk factors in large scale software projects: A quantitative study," *Int. J. Knowl. Soc. Res.*, vol. 5, no. 1, pp. 1– 11, 2014.

[13] A. B. Shahzad and A. Said, "Application of quantitative research methods in identifying software project factors," *Int. J.*

Inf. Technol. Elect. Eng., vol. 1, no. 1, pp. 30–33, 2012.

[14] K. Saleem, A. Derhab, J. Al-Muhtadi, and B. Shahzad, ‘‘Human- oriented design of secure machine-to-machine communication system for e-healthcare society,'' *Comput. Hum. Behav.*, vol. 51, pp. 977–985, Oct. 2015.

[15] K. Saleem, A. Derhab, J. Al-Muhtadi, B. Shahzad, and M. A. Orgun, ‘‘Secure transfer of environmental data to enhance human decision accuracy,'' *Comput. Hum. Behav.*, vol. 51, pp. 632– 639, Oct. 2015.

[16] R. A. Abbasi *et al.*, ‘‘Saving lives using social media: Analysis of the role of Twitter for personal blood donation requests and dissemination,''*Telematics Inform.*, vol. 35, no. 4, pp. 892–912, 2018.E.

[17] Alwagait, B. Shahzad, and S. Alim, ‘‘Impact of social media usage on student academic performance in Saudi Arabia,'' *Comput. Hum. Behav.*, vol. 51, pp. 1092–1097, Oct. 2015.

[18] B. Shahzad and E. Alwagait, "Does a change in weekend days have an impact on social networking activity?'' *J. UCS*, vol. 20, no. 15, pp. 2068–2079, 2014.

[19] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, ‘‘Blockchain challenges and opportunities: A survey,'' *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018. [20] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA),'' *Int. J. Inf. Secure.*, vol. 1, no. 1, pp. 36–63, Aug. 2001.

[20] J. Barcelo, "User privacy in the public bitcoin blockchain,'' *J. Latex Class Files*, vol. 6, no. 1, p. 4, 2007.