International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 01 | Jan 2020 www.irjet.net p-ISSN: 2395-0072

Blockchain-Based Secured E-Voting System to Remove the Opacity and Ensure the Clarity of Election of Developing Countries

Md. Shahriare Arnob[1], Niloy Sarker[2], Md. Inzamam-Ul Haque[3], Mohammed Golam Sarwar Bhuyan[4]

[1,2,3] Student of B.Sc. Engineering, Dept. of Computer Science & Engineering, Bangladesh Army University of Engineering and Technology, Qadirabad, Natore-6431
[4] Associate Professor, Dept. of Computer Science & Engineering, Bangladesh Army University of Engineering and Technology, Qadirabad, Natore-6431

Abstract - *Election is a very major symbol of democracy activities, but it is very pathetic that a large portion of people in the world does not keep faith in their election system. Many countries are still using a centralized system for the election that can arise some discrepancies. Increasingly digital technology in the present era helped to solve the confusing situation among the people. The nature of the aspect of security and transparency is a threat from the worldwide election with the conventional system. Blockchain technology is one of the solutions, because it strains a decentralized system and the entire database system is owned by many users. As blockchain technology is still emerging, it has mainly focused on the technical and legal issues instead of taking benefits of this novel concept and creating advanced digital services. By adopting blockchain in the decentralization of databases on a voting system can lessen the deception of database manipulation. As most of the people of developing countries are living below the poverty line, they do not have any cryptocurrency wallets. As a result, they do not bear the expenses of any type of cryptocurrency transactions. For this, a major portion of people will be deprived of taking the privileges of this blockchain technology and it is one of the primary demerits in blockchain-based e-voting systems. Through our work, we are going to resolve this problem by leveraging the open-source blockchain technology to propose an architecture for a new electronic voting system that could be used in local or national elections to ensure the voter participation supremely.*

***Key Words*: Blockchain, E-voting, Distributed ledger, Key generation, Hash value, Ambiguity.**

1. INTRODUCTION

An election is a way that people can elect their candidate or their preferences in a representative democracy or other forms of government. Most democratic countries hold a new election for their national legislature. Elections keep a democratic country functioning, as they give people the right to select their government. But it is a matter of sorrow that, most of the people don't keep faith in the election system for some difficulties nowadays. For this, the use of technology has become a very essential part at this point to regain faith in the daily activities of humans.

In a modern democracy, as most people don't trust their government, for which the increasing use of technology as brought new challenges for making elections very important [1]. Blockchain is an emerging technology that has gained popularity in a few years. Blockchain technology originally developed for the cryptocurrency bitcoin, but it does not stop there and offers several other opportunities in many sectors. Blockchain eliminates the need for relying on an existing intermediary and the communication directly occurs between peers rather than through a central node. Some countries have already taken the initiative to improve their voting system by using blockchain technology and decentralized public ledger accompanied by a peer to peer network. This network allows users to remain innominate and suggests that it is a compatible basis for electronic voting and it could have the potential to make e-voting more adaptable and reliable [12].

While most government elections are held physically using traditional systems like sealed paper ballots, EVM machines and questionaries are usually made on the internet or news channels whether it provides sufficient transparency due to human interactions or not [3]. But security, transparency and neutralism are the biggest concerns for an election. With the development of technology, the use of blockchain can be the proper solution to overcome the problems that usually occurred in election. However, this paper proposes an e-voting system based on blockchain technology that meets the inevitable e-voting properties as well as provides a degree of decentralization and places as much control of the process in the hand of the voters as was regarded possible.

1.1 CURRENT ELECTION SYSTEM

There are some major technical challenges regarding different voting systems that currently exist in present election systems. Every voter should have been enlisted in the voting system before the elections. Their information should be kept digitally secured processed format saved in the database and also there identity information should be kept private.

Traditional ballot paper system: In the ballot paper system, every voter has to go to polling booths and cast their vote according to their choice of candidates. After casting the votes

results are announced by counting the votes manually. In this scheme, it has some weakness. It requires all voters must vote and once someone abstains from voting, the result can temper [3] [8]. It is also very time consuming, costly and difficult to count the vote for an overpopulated country. Replacement of ballot paper boxes with duplicate paper, damages of ballot paper and marking stamp seal for more than one candidate make the ballot paper system much unreliable.

Electronic Voting Machine (EVM): EVM was first used in Estonia during the October 2005 local elections. EVM's are universally used in India since the general elections of 2004, when ballots were completely out of trend [8]. It was also used for first time in Bangladesh in 2018 in the 11th national election. To overcome the problems behind ballot paper systems EVM was introduced consisting of two components:

(1) Control Unit: It stores and assembles votes, used by poll operators.

(2) Ballot Unit: It is placed in the election booth and used by the voters to cast their votes.

By using EVM, votes are correctly recorded and there is no problem in counting, scalability, accuracy, fast declaration of results and robustness of systems [8]. But the main problem lies in authentication, the person who is voting may not be the legitimate person. Other problems like capturing booths by political parties, casting of votes by under aged people and fraud voting may occur.

E-voting: Since the late 1990s/early 2000s, electronic voting has become more popular instead of a ballot paper system and EVM system. E-voting is being studied extensively, and many implementations are tested and even used for a while [3]. Electronic voting is often facilitated by the kiosk hardware system that is introduced to polling stations. These machines typically include an interactive touch screen interface through which voter can cast their votes. Electronic voting is still very popular despite having many concerns around auditing and authenticity. More, what is most valued in democratic societies is a robust electoral process that provides transparency and privacy. But it has some drawbacks. Trojan horse spyware may change or monitor votes. These cause loss of privacy and difficulties in counting. Automated vote-buying and insider attacks on the voting system may compromise the election. Spoofing by uploading viruses can be launched from anywhere and compromised the transparency of elections [10].

1.2 WHAT IS BLOCKCHAIN?

A distributed ledger of transactions, stored as immutable blocks that are connected thereby forming a chain, the validity that has been agreed upon by peers on a decentralized network and secured by cryptography. Bitcoin is recognized as the first application of blockchain technology to create a currency that could be transacted among the related parties over the internet based on the cryptographic method to secure the transactions. Blockchain was only used for commercial transactions but in the meantime, it is using in many ways in many sectors that can improve access to the internet. There is no need for a central authority to accomplish the operation on P2P based system, for which not only the money transactions but also all kinds of information can be kept secured in this distributed chain [3].

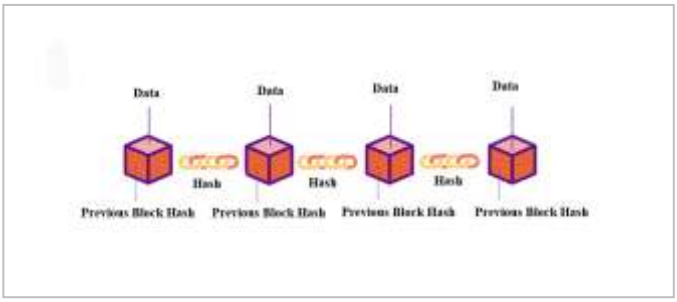

Fig -1: A visual representation of Blockchain

Each block is connected to the previous block in the chain. To connect between one block with another block, the hash value of the previous block included in the next block, then calculated its hash value. The blocks are related because the hash values of the previous block are used in the next block creation process [7]. The effort to change the information will be more difficult because it must change the next blocks [1]. The first block in the chain is considered as the foundation block of the stack. Each new block created a layer on top of the previous block to form a stack called a blockchain [4]. For each node, it maintains the consistency of the data by performing a consensus algorithm [2].The time stamps and ledgers are maintained automatically by the system. This means that it need not any third party official figures in the system.

1.3 WHY BLOCKCHAIN IS A BETTER TECH FOR E-VOTING?

Blockchain has brought an entirely new way to challenge the security threat and is the only solution to the security concerns of this era. An e-voting system must be accessible to every eligible voter and provide a high level of security [9]. But providing security of digital voting is always a big problem in voting systems [11]. However, this system is vulnerable to various security challenges and threats [13]. To reduce the challenges, blockchain has introduced some elements to make the technology stand out in the crowd:

(1) Decentralization: A database system with open access control to anyone connected to the network. Voters are recorded precisely, permanently, securely and transparently. Furthermore, blockchain assures the participant's anonymity while still being open to public review. So no one can modify or manipulates votes [5] [6].

(2) Ambiguity: Blockchain can reduce ambiguities. For example, in the 2017 Virginia House of Delegates election, the winner was chosen from paper ballots placed in a pot. One vote initially wasn't calculated because that voter made confusing marks on the ballot. Such ambiguity is less likely to arise with BEV [6] [14].

(3) Transparency: As of 2017, 23 countries had adopted online voting. Current online-voting processes might be confused for some voters. It's not easy to know whether a vote was cast as expected or whether it was counted as cast [6]. Some security systems in electronic and online voting methods were possibly developed decades ago and are unprotected to tampering. A security expert found that anyone within a half-mile of a voting machine could have altered votes without being detected [14]. The transparent nature of blockchains could certainly prevent data from being altered or stolen [5].

(4) Anonymity: As data transfer occurs between node to node, the identity of the individual remains anonymous, thus making it a more stable and reliable system [5]. This might encourage more voter participation.

(5) Autonomy: The blockchain system is unconventional and autonomous, meaning that each node on the blockchain system can access, store, and update the data securely, making it trustworthy and free from any external interruption [5].

2. PROPOSED ARCHITECTURE

We propose a secured blockchain-based e-voting system that includes system integrity, data integrity, reliability, data confidentiality, and voter anonymity.

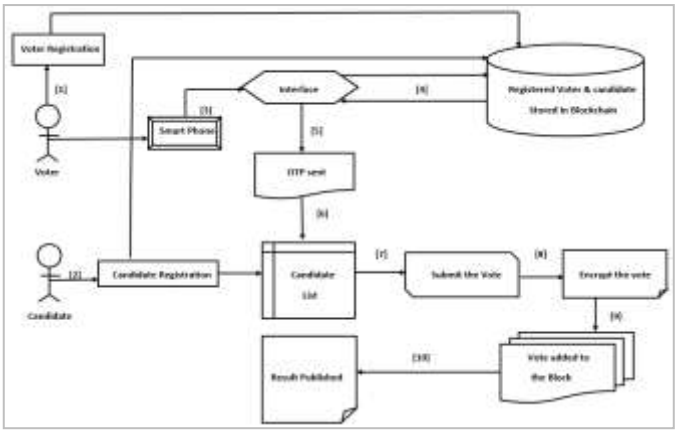

Fig -2: Proposed Architecture of Blockchain based E-Voting System

As per the proposed architecture of Blockchain-based e-voting system, there are mainly four parts:

- Voter Registration
- Candidate Registration
- Vote Casting Procedure
- Result Publication

2.1 VOTER REGISTRATION

Every person must go to their nearest voter registration office and submit their required information for being a legitimate voter. A key generation algorithm will be used to generate both public key and private key as a pair. Public key will be used for encrypting all the information of a valid voter and private key for submitting vote securely. Finally, a block will be created with all the encrypted information for each valid voter.

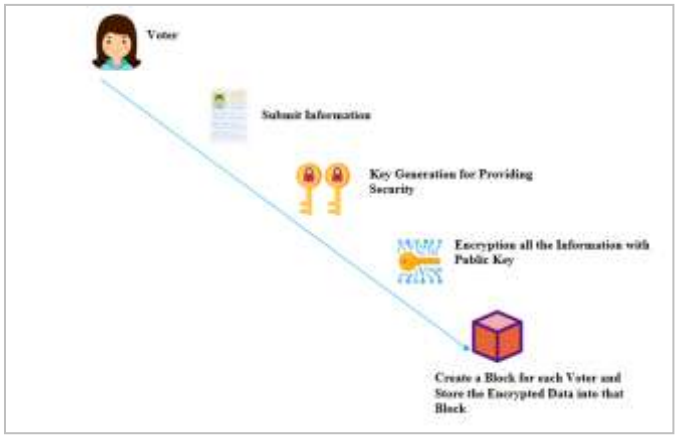

Fig -3: Architecture of Voter Registration

2.2 CANDIDATE REGISTRATION

Every nominated candidate has to complete their registration as like voter registration because a candidate is also a voter. Every information of the candidate will also be encrypted and create a block as like voter registration.

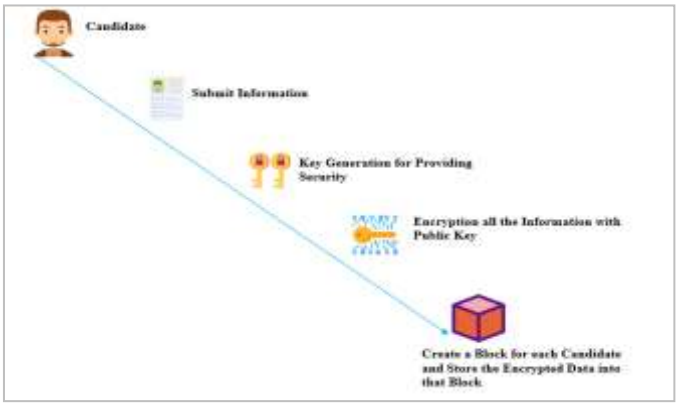

Fig -4: Architecture of Candidate Registration

Besides, each candidate has to be provided a candidate number including both their party symbol and seat number. For example:

XYZ is the candidate number of a candidate where,

X = Region of the nominated candidate
Y = Seat number of that region
Z = Party symbol number

2.3 VOTE CASTING PROCEDURE

After the completion of voter registration, a smart card will be provided. To cast a vote every voter has to perform the following steps:

- Voters need to use a smartphone to access the voting panel.
- A voter has to scan the smart card to verify his/her private key that is generated during the registration.
- Then a One Time Password (OTP) will be sent to his/her contact number given in the information and each voter has to verify themselves by submitting the OTP. If the OTP is incorrect then the process will be terminated.
- After successfully submitting the OTP, voters can able to access the voting panel and they will find the candidate list of his/her region.
- Then the voters will cast a vote to their desired candidate.
- Then the vote will be encrypted with the private key and added to the block. Every single block will be created for each vote.
- Each vote will be counted and shown in the result panel instantly while voting.

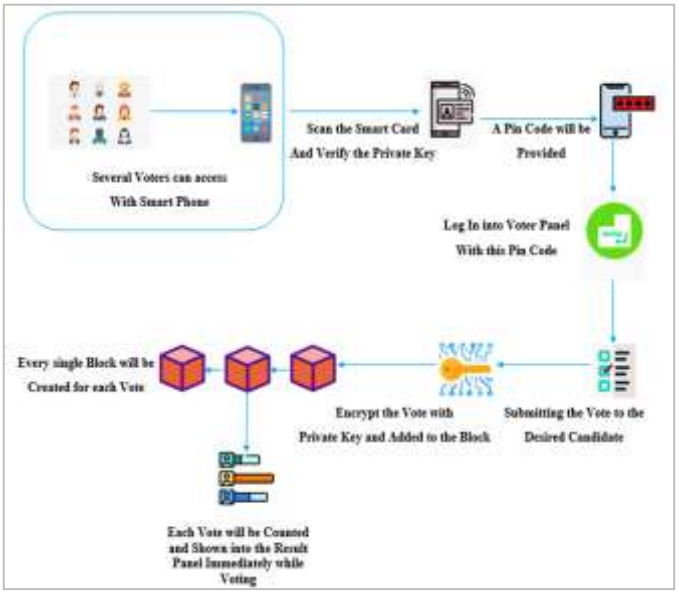

Fig -5: Architecture of vote casting procedure

2.4 RESULT PUBLICATION

After voting, every vote will form a block and add it to the chain. The vote will be counted instantaneously after the vote is submitted as there will be no risk of vote tampering and vote manipulation.

SEAT NUMBER	CANDIDATE of Z_1	CANDIDATE of Z_2	CANDIDATE of Z_3	WINNER
X_1-Y_1	5000	3000	1500	CANDIDATE- Z_1
X_1-Y_2	6000	7000	3000	CANDIDATE- Z_2
X_1-Y_3	8000	6000	2000	CANDIDATE- Z_1
X_2-Y_1	15000	12000	9000	CANDIDATE- Z_1
X_3-Y_1	8000	6000	9000	CANDIDATE- Z_3
X_3-Y_1	2000	6000	3000	CANDIDATE- Z_2
TOTAL EARNED SEAT	03	02	01	CANDIDATE-Z_1

Fig -6: Result Publication

3. METHODOLOGY

In our proposed system, as smartphones and smart cards are mandatory, so the necessity of providing security to keep the information of voters is the main concern. We will use an algorithm (ElGamal Cryptosystem) that can both generate a pair of keys and perform data encryption and decryption. We will also use the hash function (SHA-256) because the hash function is one of the main element of blockchain.

3.1 ALGORITHM

The ElGamal cryptosystem was first named by Taher Elgamal in 1985 and is a public-key cryptosystem. The proposed algorithm refers to the family of public-key cryptographic algorithms. Therefore it makes use of a key distributed into a public and a private part [15]. It uses asymmetric key encryption for communicating between two individuals and encrypting the message. The global components of Elgamal are a prime number q and, which is a primitive root of q. User A generates a private/public key pair as follows and here user B is Election Commission.

(1) Generate an arbitrary integer X_A, such that $1 < X_A < q - 1$.
(2) Compute $Y^A = \alpha^{X_A} \bmod q$.
(3) A's private key is X_A and A's public key is $\{q, \alpha, Y_A\}$.
User B that has access to A's public key can encrypt a message as follows:

(1) Express the message as an integer M in the range $0 < M < q - 1$. Longer messages are sent as a sequence of blocks, with every block being an integer less than q.
(2) Choose a random integer k such that $1 < k < q - 1$.
(3) Calculate a one-time-key $K = (Y_A)^k \bmod q$.
(4) Encrypt M as the set of integers (C_1, C_2) where

$C_1 = \alpha^k \bmod q$;
$C_2 = KM \bmod q$

User A recovers the plaintext as follows:
(1) Recover the key by calculating $K = (C_1)^{X_A} \bmod q$.
(2) Compute $M = (C_2 K^{-1}) \bmod q$.

3.2 HASH FUNCTION

Hash or hash function in the area of blockchain, it is usually expressed as the more precise form of the cryptographic hash function. The hash function, in general, is explained first and then its secure equivalent, the cryptographic hash function, as it is used as SHA-256 or SHA-3 in the blockchain sector. We use hash function because:

- **Fixed length output:** Hash function converts data of arbitrary length to a fixed value. This process is often associated with hashing the data.
- **Compression function:** In general, the hash is much smaller than the input data, hence hash functions are sometimes called compression function.
- **Digest:** Since a hash function is a smaller representation of a larger data, it is also referred to as a digest.
- **Fast operation ability:** Generally, for any hash function 'H' with input 'x', computation of H(x) is the first operation. Computationally hash functions are much more accelerated than symmetric encryption.

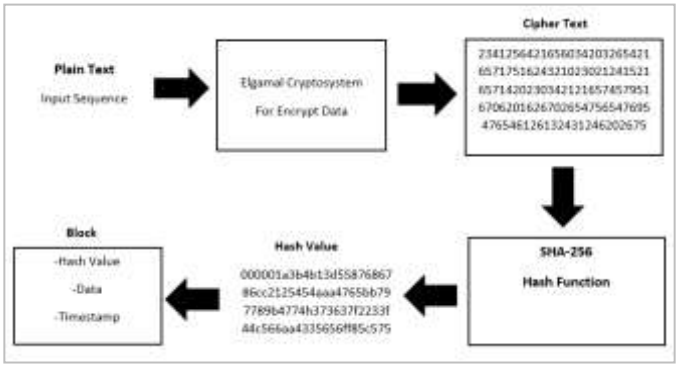

Fig -7: Representation of hash value

4. EXPECTED OUTCOME AND LIMITATIONS

As there are some limitations in existing systems, our proposed system will provide some benefits over the existing system that will help much to provide efficiency in the e-voting system.

- Every eligible voter will be able to cast vote from anywhere.
- An eligible voter will not be able to vote twice.
- The system will reduce the use of papers and EVM machines. So it will gradually reduce the cost of elections.
- The system will provide a high level of security.
- The system will reduce the risk of hacking and vote tampering.
- The system will ensure more voter participation.

However, blockchain-based e-voting still have a large room for improvement. Though the blockchain-based e-voting system is more secure and transparent there may be some drawbacks:

- If the internet connection is not available then it is almost impossible for the voters to cast vote.
- As it is a highly securable and busy process, so the system may work slowly sometimes due to workload.
- As most of the people of developing countries are lying under the poor literacy rate and having a lack of knowledge about technology, it can be a trouble for them to co-operate with this system.
- As the blockchain-based e-voting system is much secured and almost hack-proof, the strong political parties of some countries may not accept this system to retain their power continuously.

5. CONCLUSION

E-voting is still a controversial topic within both political and scientific circles. Despite the existence of a few very good examples, many more items were either failed to provide the security and privacy features of a traditional election or have serious usability and scalability issues. In current election systems voters must trust the vote records provided by the election authority and it is difficult for a single voter to prove that there is no fraud. On the contrary, the blockchain-based e-voting system has strong abilities to cope up with the situation. This paper has mainly explored the limitations of the traditional election system and introduced an electronic voting system that uses the blockchain to ensure the voters' rights and regain their trust and led the way to ensure a secure, reliable and trustworthy election system.

ACKNOWLEDGEMENT

This study is a part of a B.Sc Engineering thesis related to blockchain-based e-voting systems, conducted by the students and supervised by Mohammed Golam Sarwar Bhuyan, Associate Professor, Department of Computer Science and Engineering at Bangladesh Army University of Engineering and Technology.

REFERENCES

[1] Rifa Hanifatunnisa, Budi Rahardjo, "Blockchain Based E-Voting Recording System Design", School of Electrical Engineering and Informatics, Bandung Institute of Technology, Bandung, West Java, Indonesia.
[2] Yifan Wu, "An E-voting System based on Blockchain and Ring Signature", 2017 School of Computer Science, University of Birmingham.
[3] Ali KaanKoç, EmreYavuz, Umut Can Çabuk, GökhanDalkılıç, "Towards Secure E-Voting Using Ethereum Blockchain", Conference Paper · March 2018, DOI: 10.1109/ISDFS.2018.8355340.
[4] Ahmed Ben Ayed, "A CONCEPTUAL SECURE BLOCKCHAIN- BASED ELECTRONIC VOTING SYSTEM", 'International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2017'.
[5] Asad Ali Siyal, Aisha Zahid Junejo, Muhammad Zawish, Kainat Ahmed, Aiman Khalil, Georgia Soursou, "Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives", 'Received: 6 November 2018; Accepted: 26 December 2018; Published: 2 January 2019'.
[6] Mrs. Harsha V. Patil, Mrs. Kanchan G. Rathi, Mrs. MalatiV.Tribhuwan, "A Study on Decentralized E-Voting System Using BlockchainTechnology", 'International Research Journal of Engineering and Technology (IRJET)', Volume: 05 Issue: 11 | Nov 2018.
[7] Lee, Kibin; James, Joshua I.; Ejeta, Tekachew G.; and Kim, Hyoung J. (2016) "Electronic Voting Service Using Block-Chain," Journal of Digital Forensics, Security and Law: Vol. 11: No. 2, Article 8.
[8] SyedaAfrasheem Begum, Geeta Hanji, "Study of Existing Indian Voting System and Implementation of Hybrid Design using Biometric Security in Voting Authentication Process", 'International Journal of Computer Applications (0975 – 8887), Volume 177 – No.4, November 2017'.
[9] Lauretta O. Osho, Muhammad B. Abdullahi, OluwafemiOsho,"Framework for an E-Voting System Applicable in Developing Economies", International Journal of Information Engineering and Electronic Business (IJIEEB), Vol.8, No.6, pp.9-21, 2016. DOI: 10.5815/ijieeb.2016.06.02.
[10] The Risk of e-Voting, Thomas W. Lauer School of Business Administration, Oakland University, Rochester, USA.
[11] Srivastav G., Dwivedi A. and Singh R., "Crypto-democracy: A Decentralized Voting Scheme using Blockchain Technology", DOI: 10.5220/0006881905080513, In Proceedings of the 15th International Joint Conference on e-Business and Telecommunications (ICETE 2018) - Volume 2: SECRYPT, pages 508-513.
[12] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis, "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy", ISG-SCC, Royal Holloway, University of London, Egham, United Kingdom.
[13] Saman Shojae Chaeikar, Mohammadreza Jafari, Hamed Taherdoost, Nakisa Shojae Chaei kar, "Definitions and Criteria of CIA Security Triangle in Electronic Voting System", International Journal of Advanced Computer Science and Information Technology (IJACSIT), Vol. 1, No.1, October 2012, Page: 14-24, ISSN: 2296-1739.
[14] Kshetri, Nir and Voas, J. (2018)." Blockchain-Enabled E-voting ", IEEE Software 35(4), 95-99.
[15] Andreas V. Meier, "The ElGamal Cryptosystem", June 8, 2005.

BIOGRAPHIES

Md. Shahriare Arnob
B.Sc. Engineering in Computer Science and Engineering, Bangladesh Army University of Engineering and technology.

Niloy Sarker
B.Sc. Engineering in Computer Science and Engineering, Bangladesh Army University of Engineering and technology.

Md. Inzamam-Ul Haque
B.Sc. Engineering in Computer Science and Engineering, Bangladesh Army University of Engineering and technology.

Mohammed Golam Sarwar Bhuyan, Associate Professor, Dept. of Computer Science and Engineering, Bangladesh Army University of Engineering and technology.