Wireless Networks (2020) 26:2391–2402
https://doi.org/10.1007/s11276-019-02112-5

An enhanced security mechanism through blockchain for E-polling/counting process using IoT devices

R. Krishnamurthy[1] · Geetanjali Rathee[2] · Naveen Jaglan[3]

Published online: 10 August 2019

Abstract
One of the biggest challenges in political mayhem is visible during the election process where no stone is kept unturned in order to gain the power. Further, due to poll violence and waiting in the long queues to cast their votes, numbers of common citizens avoid the voting process completely in order to evade the chaos. In order to reduce these issues or to increase the voting rate, number of smart based or IoT enabled voting applications has been projected by various authors. However, IoT devices can be easily compromised or hacked by the experts (intruders) in order to gain their own access. Therefore, to ensure an enhanced secure and transparent polling process, Blockchain plays a vital role in ensuring the legit votes and their counting without their manipulation in any way. It is also needed in today's times where the world is available to people in their IoT or smart devices to also give them the opportunity to register their votes hassle free via their smart devices without having to worry about the system getting hacked. Therefore, in this paper, the proposed layout will be based on an enhanced security through Blockchain in E-voting application using IoT devices where the user will create an account with proper verification done via voter id and other biometric methods on a smart device. Every transaction done via this account which in this case will be registering vote will be validated by a miner. The proposed Blockchain mechanism for E-polling using IoT devices is again validated and verified through several parameters such as response time, resource utilization and request processed.

Keywords IoT devices · Blockchain · E-voting/polling · Blockchain voting · Voting threats

1 Introduction

One of the biggest challenges in political mayhem is visible during the election process where no stone is kept unturned in order to gain the power. The world, mostly democratic countries face various challenges on a daily basis which hinder country growth by involving a variety of illegal activities such as corruption and human rights violations etc. However, it is the common citizen who suffers most in terms of clarity as well as security when it comes to his/her vote. While some of them avoid the voting process completely in order to avoid the chaos and to wait in long queues to cast their votes [1]. This cannot be healthy for a democracy where the citizens are weary of the freedom to choose their leaders and don't have enough trust in the electoral process run by the administration. Therefore, it is needed more than ever in democracies across the globe to ensure a free and fair election and make it safer for voters to make a free willed decision. Voting is the process

✉ Naveen Jaglan
naveenjaglan1@gmail.com

R. Krishnamurthy
krishnamurthy.iisc@gmail.com

Geetanjali Rathee
geetanjali.rathee123@mail.com

[1] Department of Electronics and Communication Engineering, Sri Vasavi Engineering College, Tadepalligudem, Andhra Pradesh, India

[2] Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat, Solan 173234, H.P, India

[3] Department of Electronics and Communication, Jaypee University of Information Technology, Waknaghat, Solan 173234, H.P, India

through which most democracies choose their government and each citizen makes his/her choice by going to a polling booth and registering their vote. While there is a need to ensure the integrity of elections that does not get manipulated by providing safety and security of citizens during elections. Before the introduction of Electronic Voting Machines (EVMs), the Paper Ballot method was hugely assessed because of instances of fraudulent voting and booth capturing [2–4]. The EVMs came into being, which had tremendous benefits over paper ballots however the voter still has to go to a polling booth in order to cast their vote. Elections anywhere in the world are a very daunting affair where candidates use any and every kind of manipulation in order to gain seats in the office. Further, there is a huge amount of criminalization involved in today's electoral systems. During the polling process, some of the risks involving are voter manipulation, spreading of fake news, hacking and extreme cases of violence causing damage to life and property. Therefore, in order to ensure a secure voting process, EVMs must be secured or transparent using today's era of smart techniques [5, 6]. Smart technologies is the one where number of sensors, IoT devices involved during communication procedure by ensuring an easy, safe and effortless solution of any problem. However, a security breach in any phase of communication process such as data stealing, path modification or manipulation or compromised IoT devices may invite a huge risk of system performance [7–9].

1.1 Research objective

During online voting/counting processes, malicious activities such as Bogus voting and cost saving provides faster result however there is still room for improvement and more security. Further, a number of intruders may compromise smart or IoT devices by drastically affecting the polling or counting process in order to gain their own benefits. Therefore, there must be some security mechanisms that ensure a reliable poling and counting process. Though, number of security schemes such as cryptographic, biometric and hash based schemes for secure E-voting applications has been proposed by various authors. However, these mechanisms may further enhance the network complexity by issuing the computational, communication, storage and verification cost. Therefore, there is a need to further propose some enhanced security schemes or frameworks that promises a secure E-voting/counting process by avoiding the above mentioned issues.

Now days, Blockchain plays a very important role where users, IoT devices registering their votes are legit and the counting of votes is not manipulated in any way. Blockchain is a distributed ledger which stores data in the form of blocks where each block linked to the next via chain [10–12]. It is decentralized, distributed and immutable which makes it nearly impossible to tamper with any phase of voting process as depicted in Fig. 1. Blockchain when applied in the process of voting along with IoT devices further enhances the security among candidates and voters. The depicted Fig. 1 presents a secure E-voting process by ensuring the security through polling, counting and result declaration process using Blockchain technology. Here, the identities of all voters stored in a database that are further linked with Blockchain so that any single alteration in any phase of voting process can be easily traced and identifies by the authorities. Also, once every person has an application in their smart phones, it is not required to stand in long queues in the polling booths and fearing any kind of poll violence. It will provide a kind of transparency which will not let the results be questioned and will provide a new confidence to the voters. E-Voting by NirKshetri and Jeffrey Voas [13], have discussed how blockchain enabled E-voting namely BEV emphasized on voter transparency [14]. They have mentioned transparency, authentication and provability in the voting platform. Every country wants their citizens to be comfortable sitting in their homes and offices and be able to vote without having to worry about their votes being misused.

1.2 Motivation of the paper

Although the world is waking up to the possibility of using Blockchain for maintaining transparency, it has not yet been able to fully verify the fact that the transparency it claims to provide is in fact authentic. There are various ways to forge government issued documents that can be uploaded and used in order to create new identities for the same person. A person can have multiple voter ids for different states issued at different times in their lives. Most importantly to keep in mind the fact that people can forget their passwords or lose them and in worse cases share them. In our paper we will discuss these issues by ensuring a secure and transparent Blockchain based E-voting mechanism using IoT devices [15]. The polling and counting processes through smart devices such as laptops and smart phones not only reduces the voter's efforts to cast their votes but also ensures the increase of vote's rate at an exponential growth. However, the attacking or compromising techniques may further stop the organizations to gain the benefits of IoT devices. Therefore, a biometric based method may further enhance the identification and detection of malicious IoT devices.

The proposed layout of this manuscript will be based on a Blockchain technique that ensures a secure E-voting/counting process using IoT devices where user creates

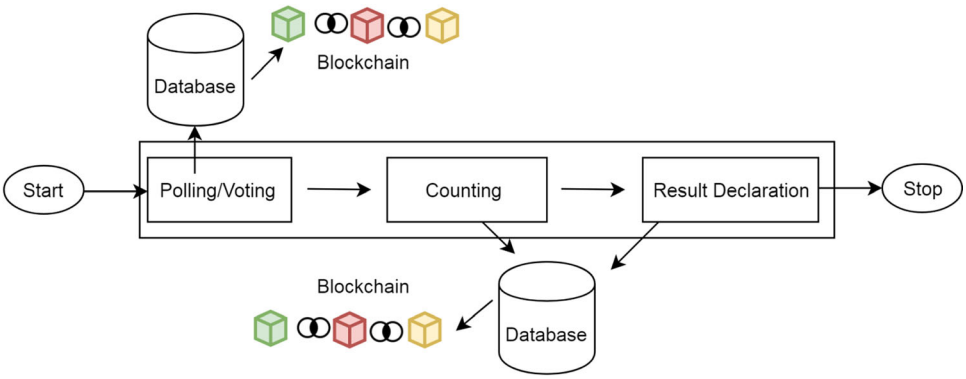

Fig. 1 Blockchain enabled E-voting polling and counting process

an account with proper verification done via voter id and other biometric methods. Every transaction done via this account will be registered and validated by some miner by taking into account the voter's permanent address based on voter id and thereby assigning that vote to a vote pool of that constituency. Every vote of a person will be done via biometric methods where the miner of Blockchain network will validate the authenticity of votes. Once the election date of the constituency has passed and there is any other vote registered, the miner will cancel the request. Similarly, if the biometric authentication has failed for the user, the request will be cancelled by the miner through this method same account holder will not be allowed to vote in multiple constituencies.

The remaining structure of the paper is organized as follows. The need of Blockchain technique in E-voting application for ensuring a secure polling/voting and counting process is briefly introduced in Sect. 1. The number of secure E-voting mechanisms or frameworks projected by various authors is illustrated in related work Sect. 2. A secure E-voting and counting framework using Blockchain technology is illustrated in Sect. 3. The performance analysis numerically simulated proposed framework against attack strength, accuracy and result processes in the network over traditional mechanism is detailed in Sect. 4. Finally, Sect. 5 concludes the paper by highlighting the future direction to further secure the E-voting pooling and counting mechanism.

2 Related work

There are various countries who have either implemented, experimented or are at least considering implementing blockchain based E-voting system. Estonia is a pioneer in E-governance and has already implemented E-Voting in their parliamentary elections. E-Voting is available for the days predating the Election Day. It is thoroughly convenient as well as safe for the citizens and keeps duplications in check. Further, South Korea has carried out their part of experiments pertaining to Blockchain E-Voting. It was first carried out in March 2018 by the country's Gyeonggi-do Province, where it was used to determine what community project to carry out first in the budget. Although this initiative was done on a small-scale with participants only numbering about 9000, officials believe this demonstrates the potential for Blockchain technology as a tool for online voting. Japan too is undertaking trials for Blockchain for voting. In this section, the number of Blockchain enabled techniques in E-voting applications reported by various researchers and scientists will be explained in detail.

Salahuddin et al. [16] have proposed a softwarized and agile infrastructure for flexible secure, cost effective and privacy deployment for IoT systems in smart healthcare services and applications. Kang et al. [17] have proposed a Blockchain based data sharing mechanisms among vehicles in Internet-of-Vehicles. By addressing the compromised vehicles challenge, Kang et al.have proposed two-stage security solution such as selection of miners and block verification. The author's have designed a reputation voting scheme by ensuring miner selection based upon their past interactions. The proposed mechanism has simulated the results for sharing the data in internet of vehicles. Wireless sensor networks have proposed a vital role in supporting IoT operations. However, organizations are afraid to adopt it properly because of their security issues. She et al. [18] have proposed a Blockchain trusted mechanism for detecting the malevolent node in sensor networks. The author's have proposed trusted framework by constructing Blockchain data structure to detect malevolent nodes. Finally, it realizes the malevolent node detection using sensor quadrilateral and Blockchain contracts. The simulated result projected the effectiveness of proposed framework by ensuring the tractability of detected process. In order to enhance the efficient and management levels, many gas and oil companies have shifted towards digitalization and intelligence by adopting Blockchain technique. Lu et al. [19] have reviewed the Blockchain technology in gas and oil industry in four different aspects such as management, trading, cyber security and supervision. The

author's have concluded the benefits of adopting Blockchain technology in gas and oil industry. Further, the author's have mentioned that though it is an initial stage because of its primarily technology, system and regulation transformations. Moreover, the author's have focused that Blockchain developments have moved to hybrid architectures, cross chains and hybrid mechanisms. The recent advancements in automotive industries and its adapting complexities, Industry 4.0 such as cyber physical system, augmented reality, robotics involving privacy, traceability, integrity, trustworthy, security. Lamas et al. [20] have reviewed the applications of Blockchain technology in automotive industries by emphasizing their security features. Furthermore, the author's have illustrated the use cases by creating business models and disrupting the car sharing economy. Furthermore, the author's have pointed the weakness, strengths, threat analysis, by recommending certain guidelines and companies in future resilient developments. Al-Jaroodi and Mohamed [21] have reviewed various industry applications where Blockchain can be adopted is discussed. Further, the paper has discussed various benefits, opportunities and challenges in various applications of Blockchain techniques. Moreover, the paper identified the requirements and implementations of Blockchain by revealing various opportunities for utilizing Blockchain in industries. Furthermore, the author's have addressed various utilization of Blockchain in industry. Hu et al. [22] have digital payment based on Blockchain for financial verification by deploying various proxy nodes connected to remote communities. Authors have proposed various probabilistic parameters to realize vigorous operations. Furthermore, authors have demonstrated the feasibility by growing Near Field Communication on Raspberry-Pis, mining nodes and mobile wallet application on off shelf computers. In order to reduce inconsistencies and redundancies in voting portal systems, E-voting has replaced the traditional both voting systems. However, over the time, electronic voting has not been successful adopted due to privacy and security flaws. Shahzad et al. [23] have proposed a Blockchain framework for ensuring the security of voted data. The proposed framework illustrates the utility of hashing algorithms, accumulation of data, polling processes, creation and sealing of blocks along with result declaration via adjusted Blockchain methods. The proposed framework claimed the management and security challenges by proving an improved digital voting scheme. Kshetri and Voas [24] have proposed e-voting Blockchain mechanism to reduce fraud by increasing the voter accesses. The eligible voters have casted the ballots via smart phones and computers anonymously in order to ensure the security using Blockchain. The author's have proposed an encrypted tamper proof identify of personals. The paper has proposed implementations by highlighting the challenges and benefits. Anjum et al. [25] have elaborated various applications of Blockchain in manufacturing, supply chain management, agriculture product tracking, internet of things, advertizing verifications, industries and healthcare. The progressive shift of healthcare services and data are limiting the access control and cryptographic methods by addressing the privacy and security concerns in cloud environments. Esposito have proposed the potential use of Blockchain for protecting the healthcare data hosted over the cloud. Further, the author's have illustrated the practical challenges along with future directions. Yavuz et al. [26] have proposed a Blockchain enabled E-voting application by emerging a cheap, safe, transparent and secure polling process. In order to avoid duplicate votes and ensure a consistency among the voting and counting process, authors have implemented a voting application as smart contract while using the solidity language. Further, the proposed framework validated and verified in terms of efficiency and reliability of Blockchain based voting process. Hjalmarsson et al. [27] have projected a novel E-voting scheme using Blockchain by addressing the limitation of existing approaches. The authors have evaluated the distributed ledger technique by discussing a case study of election process by implementing a Blockchain application with reduced host costing and improved security. Till now, numbers of researchers have projected the E-voting process using IoT devices and need of Blockchain technology in various applications or fields. However, none of the authors have discussed the issue of compromised IoT devices while casting the votes. Further, the need of Blockchain in E-voting process is still at its early stage. The goal of this manuscript is to project a Blockchain enabled E-voting process using IoT devices that ensure transparency and security among candidates and voters while polling or counting system using bio metric password protection.

3 Proposed solution

The proposed layout will be based on a smart contract, using Ethereum software to create an e-voting app where the user will create an account with proper verification done via voter id and other biometric methods. Every transaction done via this account will be registered vote that will be validated by a miner. The miner will take into account the voter's permanent address based on voter id and thereby assigning that vote to a vote pool of that constituency. There will be duration of few days when the option of registering the vote will be active. Every registered vote will be done via biometric methods where the miner will validate the authenticity of the vote. Once the

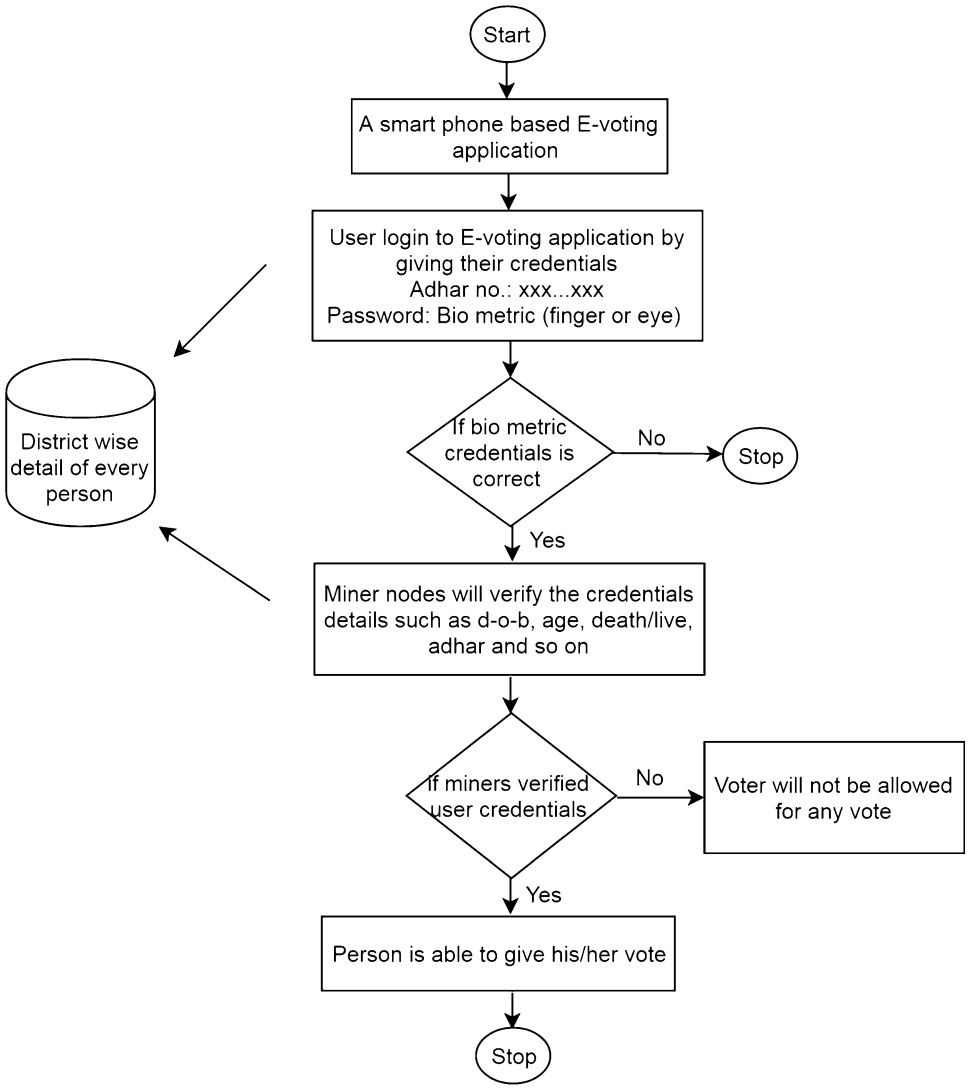

Fig. 2 Flowchart of proposed blockchain enabled E-voting process

election date of the constituency has passed and there is any other vote registered, the miner will cancel the request. Similarly, if the biometric authentication has failed for the user, the request will be cancelled by the miner. Same account holder will not be allowed to vote in multiple constituencies. Therefore, in order to save time as well as reduce the loss of security purposes, IoT devices must have been secured by projecting an efficient and reliable framework. The major case of document forgeries causing a single person to vote multiple times can be countered by introducing a biometric login system that will ensure that there is only a single entity associated with one vote. This biometric system can be installed in the same application as the electronic voting system. We would require separate ledgers for biometric data as well as the voter choices where each miner would have to check the data verification before validating the voting transaction.

The accounts in this case will not be document based or email based, they would be taking your physical data to create an account. The ledgers would also have to be in sync with the census and be updated on a daily basis on the number of deaths and citizens turning 18 (official age for voting in India). The physical data input can be verified via government records, police records and in cases of suspicion it can be verified in person at a government approved process. It is also a simpler approach for a large part of the Indian population who are not very well versed with the complications of technology for example the password reset and document updating options. These things can make people skip the whole voting process doing more damage than good. Therefore a single touch option taking them to the choices of their parties and another single touch option to seal their votes at the comfort of their homes seems like a much convenient option.

The depicted Fig. 2 details the flowchart of Blockchain E-voting process. Before ensuring a secure E-voting process using Blockchain technique, it is necessary to verify each person credentials such as name, age, date-of-birth

and address through his/her identity card such as adhar card, voter identity card, rashan card etc. As every person has a unique adhar number, therefore, no two persons would be able to take participate twice in the voting process or to do vote twice. Further, fake users who has stolen adhar number of another person or people participating in voting process in the name of another one who are dead can be successfully caught using this technique. Further, a single change or performing any type of malicious activity in the voting process, the remaining admin authorities would be able to immediately detect the intruders as per Blockchain feature. The depicted 2 presents a complete flowchart of Blockchain enabled E-voting process where the step explanation of every step is details as follows:

1. For reducing the time and effort while standing in a queue, a smart phone E-voting application would be very helpful that further enhances the voting percentage among the country.
2. After installing the E-voting application, every person who is eligible to do voting could be successfully login by filling the adhar number or password credentials. In order to ensure security and prevent from fake identities, a biometric password scheme is chosen where every person is recognized or verified through this eye scan or finger print identity.
3. If adhar number and corresponding password credentials matches with already stored database information

Then

Person is allowed for further process

Else

Person would not be permitted to participate in any E-voting process.

4. Blockchain network consist numbers of peer and miner nodes that are responsible to participate in voting process or verifying the participating nodes in the network
5. If miners have successfully verified the person credentials such as date-of-birth, adhar number, address and voting status

Then

Person is allowed to do vote

6. Else
7. Voter will be notified as fake user
8. Further, in order to prevent from repeat voting by single person, the record of voting is matched with database
9. If voting status is null

Then

Person is allowed to do vote

Else

An alert message will encounter as “you have already submitted your vote”

Further algorithm 1 presents the pseudo code of the proposed framework.

Algorithm 1: Authenticity of voter to cast their votes

Input: A smart phone with E-voting application

Output: User or voter has successfully casted their vote or not

Begin

Step 1: User will enter into polling process by entering his/her credentials such as adhar card and finger prints

If (voter adhar no. && finger prints ==voter's already stored information in the database)

Then

Voter is allowed to further proceed and to do the voting

Else

Voter or user will be blocked at initial stage

Step 2: The voter personal details such as date-of-birth, address proof, location will further verified by the miners nodes of Blockchain network. Miners M1, M2…Mn further verify the voters V1,V2…Vn personal details.

If (Miner nodes M1, M2…Mn verify voter's date-of-birth, address proof, location)

Then

System will check whether vote has already been casted by the voter or not

Else if (voter Vi voting status=No)

Then

Voter is allowed to cast their vote

Else if

Message will be displayed as voter has already casted its valuable vote

Else

Voter is not allowed to caste his/her vote

Now, suppose some of the intruders have compromised IoT devices and tries to cast the votes using fake identities. In that case, these fake identity voters can be easily caught during its initial phase where identity is done via bio metric password. Now, in case where intruders may successfully get rid from first step then it can be surely caught at second step where voter's identification is again done via miner nodes. The entire person's identity stored on a database in linked through Blockchain where miner node verifies each individual further to ensure a legit vote. After the completion of voting process, the next step in E-voting is to start counting the votes. Blockchain technology plays a vital role at step that actually prevents the E-voting process from any type of fraud or alterations during counting process. While counting the votes, there may be high chances of internal as well as external entities to alter the submitted record. In order to prevent from these security risks, Blockchain technique would be very beneficial by maintaining a transparency among the users. Any change or alteration of a single vote or record can be immediately identified or detected by remaining polling authorities and

can be immediately take the action corresponding to that station. Though, the smart based E-voting applications considered as smart devices where persons are identified or allowed to do their votes using the application can be early hacked by number of intruders, while Blockchain technique ensures a high level security in E-voting process. In order to understand the benefits of Blockchain in during polling or counting process, let us consider a scenario as depicted in Fig. 3.

The Blockchain hashes are very valuable when someone desires to recognize or detect any changes in the current blocks. According to Blockchain feature, a single alteration in any stored record such as vote counts or person identity within the block will modify the current hash. Each block contains the hash of current and prior blocks which effectively generates a chain of blocks by ensuring a secure Blockchain. To appreciate it in a better way in case of E-voting, let us consider where a 3-block chain sequence is worn. Each block point to casted vote, or total vote counts by the voters as depicted in Fig. 3. Every block has three elements such as voter information, its current hash, and hash of its succeeding block. Various authorities are appointed to keep track or store each votes counting through Blockchain. Now, assume an intruder or internal authority tries to tamper with the second block data present in the Blockchain. In such a case, once the data or vote information is stored, any change in the counting may change the hash of the all succeeding blocks. This causes current block hash alter as well as alteration of block 3 and all subsequent blocks irrationally since they no longer hoard of a valid hash of former block. Thus, altering a solitary chunk will leave all subsequent blocks unacceptable. The scope of this paper is to analyze the legitimately of IoT devices where intruders tried to compromise IoT devices to cast fake votes. The proposed framework is analyzed against certain networking parameters such as possibility of accuracy of proposed framework, attack strength and request processed by compromised IoT devices in the network by considered certain security concerns.

4 Performance analysis

4.1 System state

For ensuring the validation and verification of proposed E-voting framework, the simulation results are analyzed over NS2 software. The analyzed performance results are realized over various security measures such as of attack strength, accuracy and result processes in the network. Though, security measures over voting applications are considered to be a very challenging task. This paper has proposed a secured Blockchain voting scheme that not only guarantee security of nodes (devices) but also ensures a secure and transparent counting process during polling. In the projected E-voting frameworks, NS version 2.5 having predefined number of IoT devices or nodes is executed. 700 × 700 simulation area is created having 10, 25, 50, 75, 100 number of nodes as depicted in Table 1.

In the projected E-voting frameworks, NS version 2.5 having predefined number of IoT devices or nodes is executed. 700 * 700 simulation area is created having 10, 25, 50, 75, 100 number of nodes are generated. Moreover, for validating the security framework, devices metrics are analyzed where certain of them are compromised by various intruders. The malevolent nodes are added based on transmission probability by accomplishing the execution time of simulation for 1 min. Number of metrics such as attack strength, accuracy and result processes in the network are recorded on mentioned numerical set up. The depicted graphs show proposed mechanism over traditional approach against certain metrics. The depicted Fig. 4 shows the accuracy of the proposed scheme in the presence of malicious environment.

The accuracy is computed in terms of time where in how much time the proposed mechanism is able to actual predict the legitimate devices over predicted amount of time. The difference among actual and predicted time can be easily identified the accuracy of proposed phenomenon. As depicted in Fig. 4, proposed framework close to 81% accuracy against malevolent environment. Furthermore, it is alleged the attack strength of proposed framework as depicted in Fig. 5 augments better results than existing

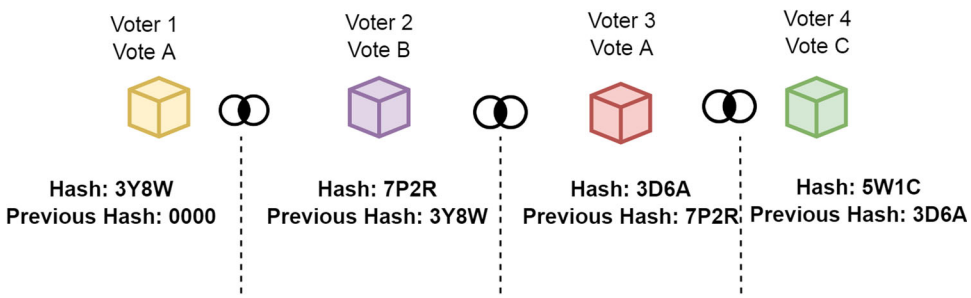

Fig. 3 Formation of blockchain corresponding to product

Table 1 Analysis details of proposed framework

Metrics	Values
Network size	700 × 700
Simulator	NS2
Data size	256 byte
MAC	802.11
Number of nodes	10, 25, 50, 75, 100
Simulation time	60 s

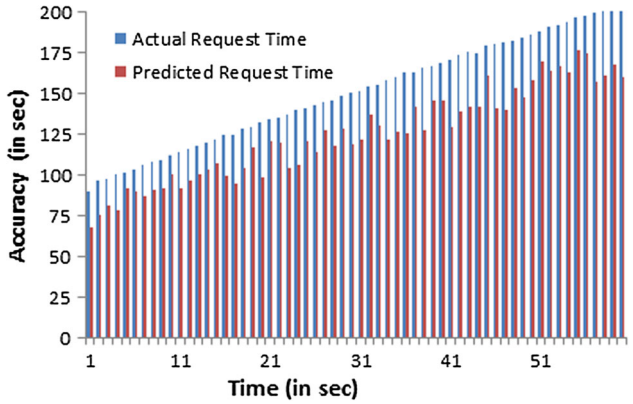

Fig. 4 Accuracy comparison for prediction of malicious nodes

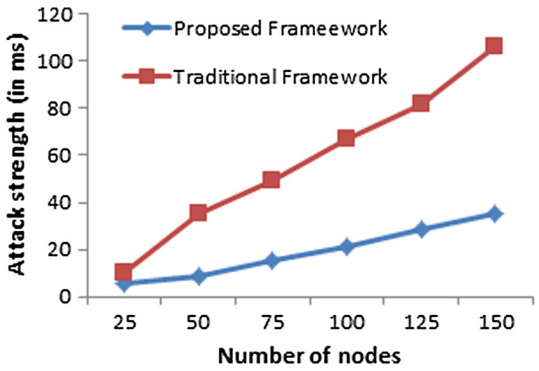

Fig. 5 Attack possibility against number of nodes

mechanisms. Existing schemes are not able to successfully ensure transparent environment that may further paves way to reduce the attack possibility by involving the fake identities or modifying the stored record in the network by voters and vote counts. While proposed framework is based on Blockchain technique is successfully able to identify and remove the malicious activities of stored record alteration and devices. Further, the transparent feature of Blockchain ensures the trust among voting/polling procedures. Figure 6 shows the number of processed request against linear trend over varying number of nodes. All the mentioned graphs clearly pragmatic that the nodes augmentation is linear, the number of processed requests also augments linearly.

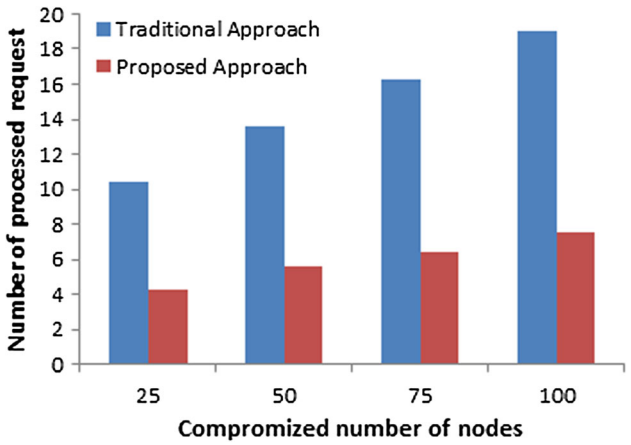

Fig. 6 Number of request processed over compromised number of nodes

Here, existing system is when malicious devices are not identified using trust and are not able to remove from the system that further leads to increase in attack strength and accuracy reduction of the existing system. However, in proposed scheme that detects any malevolent device and able to immediately remove it from the system so that it does not hamper the system performance. Moreover, Fig. 6 presents the number of requests processed by the proposed framework with respect to linear trend for all networks. It can be clearly pragmatic that as the augment in device number is linear the number of processed requests also augments linearly.

Further, Figs. 7 and 8 analyzed against certain attacks and authentication processes. Figure 7 depicts the outperformance of proposed mechanism over basic approach where number of intruders compromised several legitimate

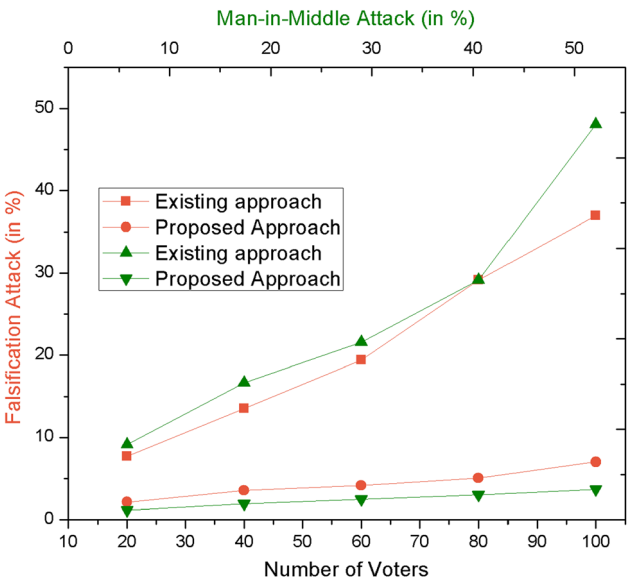

Fig. 7 Falsification and man-in-middle attack

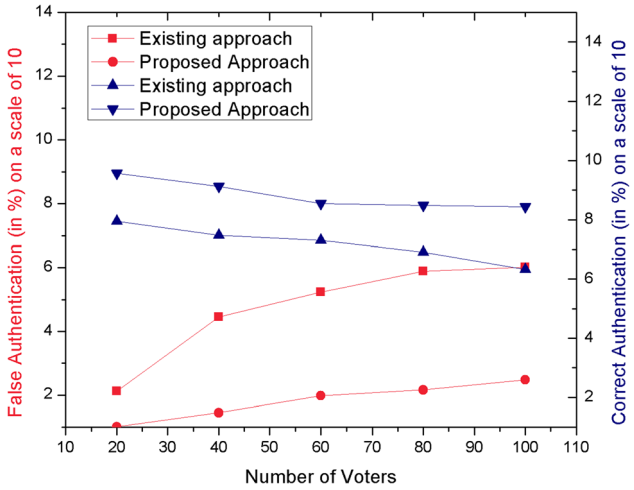

Fig. 8 False and correct authentication delay

nodes by introducing falsification and man-in-middle attack. Falsification attack is the one where nodes are compromised by the nodes and successfully able to perform malicious activities while congesting the traffic, increasing the cost and consuming the network resources. However, man-in-middle attack is the one where intruders are successful to see the ongoing message among the communicating entities. During the validation process, proposed framework is less affected by the compromised nodes because of two stage verification of Blockchain framework. Similarly, in case authentication validation, proposed and basic approaches are measured against false and correct authentication scenarios. Correct authentication means projected approach is able to successfully identify the difference among legitimate and compromised users. In addition, false authentication occurs where compromised voters or nodes are successfully able to do malicious activities in the network. The depicted Fig. 8 presents the success rate where intruders are successful to compromise the voters and able to do malicious activities in the network. The proposed mechanism is validated against two authentication schemes such as false authentication where servers have identified the compromised nodes as legitimate where correct authentication means where node is legitimate and server has also identified it legitimate node. In this scenario, the proposed scheme successfully outperforms as compare to existing approach because of its two stage security using bio metric and blockchain technology.

4.2 Traditional (existing) approach

For validating the proposed trust framework, the mechanism is compared against existing security technique proposed by Yavuz et al. [26]. They have proposed a Blockchain enabled E-voting application by emerging a cheap, safe, transparent and secure polling process. In order to avoid duplicate votes and ensure a consistency among the voting and counting process, authors have implemented a voting application as smart contract while using the solidity language. Further, the proposed framework validated and verified in terms of efficiency and reliability of Blockchain based voting process. However, in our proposed mechanism, the E-voting security is further enhanced in two different aspects such as providing the security from compromised IoT devices by verifying the votes through bio metric password scheme and identification and alteration of a single alteration in stored record using Blockchain technique.

4.3 Discussion on evaluated results

Traditional voting mechanisms and proposed Blockchain enabled voting procedures have been appraised over various nodes by projecting a personalized numerical setup. The proposed mechanism efficiently identified the malicious activities done by compromised IoT devices. Further, the transparency among candidates and voters can be easily maintained through Blockchain technique that identifies a single alteration in any phase of voting process by the intruder in the network. In addition, the identified malicious device and modified record can be permanently blocked or punished and cancelled depending upon the change of modification. The evaluation of simulation conduction was victorious where numbers of concerned results against several parameters were recorded. The system state and evaluated metrics values were offered in both the previous subsections. The proposed voting mechanism behaves as desired having optimized evaluated metrics against traditional voting procedures. In addition, the accuracy of Blockchain enabled framework reached to 81% that can be further recovered and enhanced over period of time. Furthermore, remaining parameters such as attack strength, accuracy and result processes in the network during malicious environment ensures better results. The detection and removal of malicious nodes in proposed framework is entirely based upon Blockchain process that ensures a transparent environment among all the nodes. Any change of alteration in polling system may immediately alert the remaining polling stations and authorized persons.

5 Conclusion

This paper has proposed an enhanced security E-voting/counting framework using IoT devices based on Blockchain technique. The proposed framework ensures

the security by capturing and intimating each and every legal and illegal activity of the voters during polling and counting process in E-voting. The proposed framework is validated against various compromised IoT devices that can be further analyzed through biometric and blockchain mechanisms. The proposed Blockchain E-voting framework has significantly outperform against various numerically simulated results such asattack strength, accuracy and result processes in the network against traditional mechanisms in the presence of malevolent nodes/devices. Furthermore, the simulated results of proposed framework enhanced the E-voting security by showing 81% accuracy compared to traditional E-voting procedures that further encourages the organization to use Blockchain technique. Moreover, the real time application on a dataset where E-voting can immediately identify the malicious activity of IoT devices and detect the alteration of record stored on Blockchain database will be reported in future communication.

References

1. Liu, F. H. F., & Hai, H. L. (2005). The voting analytic hierarchy process method for selecting supplier. *International Journal of Production Economics, 97*(3), 308–317.
2. Christian Schaupp, L., & Carter, L. (2005). E-voting: From apathy to adoption. *Journal of Enterprise Information Management, 18*(5), 586–601.
3. Zissis, D., & Lekkas, D. (2011). Securing e-Government and e-voting with an open cloud computing architecture. *Government Information Quarterly, 28*(2), 239–251.
4. Barr, E., Bishop, M., & Gondree, M. (2007). Fixing federal e-voting standards. *Communications of the ACM, 50,* 19–24.
5. Zissis, D., & Lekkas, D. (2011). Securing e-Government and e-voting with an open cloud computing architecture. *Government Information Quarterly, 28*(2), 239–251.
6. Khasawneh, M., Malkawi, M., Al-Jarrah, O., Barakat, L., Hayajneh, T. S., & Ebaid, M. S. (2008). A biometric-secure e-voting system for election processes. In *2008 5th international symposium on mechatronics and its applications* (pp. 1–8). IEEE.
7. Singh, M., Rajan, M. A., Shivraj, V. L., & Balamuralidhar, P. (2015). Secure mqtt for internet of things (iot). In *2015 fifth international conference on communication systems and network technologies* (pp. 746–751). IEEE.
8. Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems, 78,* 964–975.
9. Marin, L., Pawlowski, M., & Jara, A. (2015). Optimized ECC implementation for secure communication between heterogeneous IoT devices. *Sensors, 15*(9), 21478–21499.
10. Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review, 95*(1), 118–127.
11. Rathee, G., Sharma, A., Kumar, R., & Iqbal, R. (2019). A secure communicating things network framework for industrial IoT using blockchain technology. *Ad Hoc Networks, 94,* 101933.
12. Rathee, G., Sharma, A., Saini, H., Kumar, R., & Iqbal, R. (2019). A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-019-07835-3.
13. Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. *IEEE Software, 35*(4), 95–99.
14. Ayed, A. B. (2017). A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security and Its Applications, 9*(3), 01–09.
15. Osgood, R. (2016). The future of democracy: Blockchain voting. In *COMP116: Information security* (pp. 1–21).
16. Salahuddin, M. A., Al-Fuqaha, A., Guizani, M., Shuaib, K., & Sallabi, F. (2018). Softwarization of internet of things infrastructure for secure and smart healthcare. arXiv preprint arXiv:1805.11011.
17. Kang, J., Xiong, Z., Niyato, D., Ye, D., Kim, D. I., & Zhao, J. (2019). Towards secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory. *IEEE Transactions on Vehicular Technology, 68,* 2906–2920.
18. She, W., Liu, Q., Tian, Z., Chen, J. S., Wang, B., & Liu, W. (2019). Blockchain trust model for malicious node detection in wireless sensor networks. *IEEE Access, 7,* 38947–38956.
19. Lu, H., Huang, K., Azimi, M., & Guo, L. (2019). Blockchain technology in the oil and gas industry: A review of applications, opportunities, challenges, and risks. *IEEE Access, 7,* 41426–41444.
20. Fraga-Lamas, P., & Fernández-Caramés, T. M. (2019). A review on blockchain technologies for an advanced and cyber-resilient automotive industry. *IEEE Access, 7,* 17578–17598.
21. Al-Jaroodi, J., & Mohamed, N. (2019). Blockchain in industries: A survey. *IEEE Access, 7,* 36500–36515.
22. Hu, Y., Manzoor, A., Ekparinya, P., Liyanage, M., Thilakarathna, K., Jourjon, G., et al. (2019). A delay-tolerant payment scheme based on the ethereum blockchain. *IEEE Access, 7,* 33159–33172.
23. Shahzad, B., & Crowcroft, J. (2019). Trustworthy electronic voting using adjusted blockchain technology. *IEEE Access, 7,* 24477–24488.
24. Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. *IEEE Software, 35*(4), 95–99.
25. Anjum, A., Sporny, M., & Sill, A. (2017). Blockchain standards for compliance and trust. *IEEE Cloud Computing, 4*(4), 84–90.
26. Yavuz, E., Koc, A. K., Cabuk, U. C., & Dalkılıc, G. (2018). Towards secure e-voting using ethereum blockchain. In *IEEE 6th international symposium on digital forensic and security (ISDFS)* (pp. 1–7).
27. Hjalmarsson, F.P., Hreioarsson, G.K., Hamdaqa, M., & Hjalmtysson, G. (2018). Blockchain-based e-voting system. In *IEEE 11th international conference on cloud computing (CLOUD)* (pp. 983–986).

R. Krishnamurthy was born in Tamil Nadu, India. He received B.E. degree from the St.Peter's Engineering College, Chennai, India and M.E. degree in Telecommunication Engineering from the Indian Institute of Science, Bangalore, India in 2005 and 2010 respectively. He received Ph.D. from the Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore in June 2015. His research interest includes PLIs-aware RWA Algorithms, PLIs-aware survivable networks, flexible-grid optical networks, and cross-layer planning of optical networks.

Geetanjali Rathee is currently working as an Assistant Professor in Computer Science and Engineering Department in Jaypee University, Waknaghat, Solan. She has received B.Tech. Degree in Computer Science and Engineering from Bhagwan Mahavir Institute of Engineering and Technology (BMIET), Haryana in the year 2011. She has completed her M.Tech. in Computer Science and Engineering from Jaypee University, Waknaghat, Solan in the year 2014. She has done her Ph.D. from Jaypee University, Waknaghat, Solan in the year 2017. Her research interest include resiliency in wireless mesh network, routing protocols, network protocols and security in next generation communication systems, security aspects in cognitive radio network.

Naveen Jaglan was born in 1989, obtained B.Tech. (Hons.) and M.Tech. (Hons.) degrees in Electronics and Communication Engineering from Kurukshetra University, Kurukshetra, India in 2009 and 2011 respectively. He obtained his Ph.D. dissertation entitled "Design and Development of Microstrip Antennas integrated with Electromagnetic Band Gap structures" from Jaypee Institute of Information Technology, Sec-62, Noida, U.P., India in June 2017. He has authored/co-authored several research papers in referred international journals and conferences. His research has included microwave communications, planar and conformal microstrip antennas including array mutual coupling, artificial materials (metamorphic, metamaterials), EBG, PBG, FSS, DGS, novel antennas, UWB antennas, MIMO systems, numerical methods in electromagnetics, Composite Right/Left Handed (CRLH) transmissions and High-k dielectrics. His skill includes modelling of antenna and RF circuits with Ansoft HFSS/CST Microwave Studio/ADS Momentum, measurements using Vector Network Analyzer and Anechoic Chamber.