IEEE Open Journal of the Communications Society

Received XX Month, XXXX; revised XX Month, XXXX; accepted XX Month, XXXX; Date of publication XX Month, XXXX; date of current version XX Month, XXXX.

Digital Object Identifier 10.1109/OJCOMS.2022.1234567

ECC-EXONUM-eVOTING: A Novel Signature-based e-Voting Scheme using Blockchain and Zero Knowledge Property

Suman Majumder, Sangram Ray (Senior Member, IEEE), Dipanwita Sadhukhan, Mou Dasgupta (Senior Member, IEEE), Ashok Kumar Das (Senior Member, IEEE), AND Youngho Park (Member, IEEE)

[1]National Institute of Technology Sikkim, Ravangla, Sikkim-737139, India
[2]National Institute of Technology Sikkim, Ravangla, Sikkim-737139, India
[3]National Institute of Technology Sikkim, Ravangla, Sikkim-737139, India
[4]National Institute of Technology Raipur, Raipur-492010, India
[5]International Institute of Information Technology, Hyderabad, 500032, India
[6]School of Electronics Engineering, Kyungpook National University, Daegu 41566, Republic of Korea

Sangram Ray and Youngho Park (e-mail:sangram.ism@gmail.com and parkyh@knu.ac.kr)

The research work is supported by Ministry of Education, Govt. of India. This work is also supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant 2020R1I1A3058605.

ABSTRACT Traditional voting systems mainly comprise of paper polling, electronic ballot system (EVM), mechanical devices, etc., and demand the physical presence of the voters. In the new age of digitization, the electronic voting system has come up with a unique facility to cast votes from any discreet place. However, the e-voting system has to face several challenges regarding security and privacy. To overcome such obstructions, blockchain is introduced in e-voting applications that preserve anonymity, security, and consistency of voter-related information with the help of Merkle tree and hash digest. Hence, any discrepancy can immediately be detected whenever the hash values of the respective block have been modified and consequently, the whole block is discarded. In this research, a novel e-voting scheme is proposed following the decentralized service-oriented architecture of Exonum private blockchain, hybrid consensus algorithm, and Elliptic Curve Diffie-Helmen (ECDH) protocol to agree upon a secure session key among different participants. Moreover, the proposed scheme (ECC-EXONUM-eVOTING) employs a zero-knowledge protocol and is customized to work over idemix technologies with a blind signature scheme. Numerous well-known cryptographic attacks are analyzed formally using the probabilistic random oracle model and informally for validating the security strength of ECC-EXONUM-eVOTING. As a result, it is found that the proposed scheme is well-defended against all potential security concerns. Furthermore, the scheme is simulated using both Automated Validation of Internet Security Protocols and Applications (AVISPA) and Scyther tools to demonstrate the proposed scheme is not prone to any security attacks. Finally, it is concluded that the proposed scheme is well-suited for secure e-voting applications.

INDEX TERMS Distributed Ledger Technology (DLT), Elliptic Curve Discrete Logarithm Problem (ECDLP), Practical Byzantine Fault Tolerant (PBFT).

I. INTRODUCTION

BLOCKCHAIN technology was first invented and used as a peer-to-peer payment system using Bitcoin by Mr. Satoshi Nakamoto in 2008 [1, 2]. Then, it this concept is incorporated into various applications such as digital voting, health care applications, e-voting systems, etc. [2-4]. Fundamentally, blockchain is a type of Distributed Ledger Technology (DLT) that follows a decentralized, permissionless, distributed ledger for a public blockchain and a permission-integrated, decentralized, or distributed ledger for private

blockchain applications [3,4]. In blockchain, information is shared among the contributory nodes described as peers. Each transaction is confirmed by a consensus mechanism, a technique that is supported by the majority of the peer nodes [5-9]. However, the distributed architecture expresses some restrictions imposed by the peer nodes, and any changes committed by a single node must be conveyed to all other nodes in the blockchain network on an urgent basis. Peer nodes are solely responsible for adding a new block to the chain and validating the block. After successful validation, if the majority of the nodes agree to add the block, then only the respective block is added to the blockchain. Hence, the peer nodes acquire the entire liability to make any decision regarding the alteration or modification of the blockchain rather than using any third-party centralized system [9]. Depending upon the maintenance and working functionality of the blockchain, the consensus mechanism is divided into– (i) competitive and (ii) non-competitive consensus. In competitive consensus, only one consensus algorithm is accepted by all the nodes in the network and participating nodes must obey the identical consensus rule to maintain an agreement. Various competitive consensus algorithms are - Proof–of–Work (PoW), Proof–of–Stake (PoS), Delegated–Stake (DPoS), etc. However, a competitive consensus system faces double voting or double payment problems for the same block. It also incurs uncertainty and performance issues [9]. On the other hand, the non-competitive consensus peer agreement and policy are changed based on time but it works in a trusted environment. So, all the peer nodes can confirm and reply instantly to the agreement. Various non-competitive consensus algorithms include Paxos, Raft Practical Byzantine Fault Tolerance (PFBT), etc. However, the problem of uncertainty and performance issues of a competitive consensus system can be solved using the PFBT consensus algorithm [9, 11].

The e-voting is an electronic voting system where the voters are allowed to cast their votes electronically through a secret ballot mechanism from any remote place, and the voting result is tabulated electronically. On the other hand, the cast votes are stored in the database or ledger so that the result can be recounted as per the situation demands and avoid hazards such as the queue for the voting process, the illegal behavior of voters and maintain reliability, transparency of voting process and production of accurate result [2,11-13].

A. Related Works

In this section, some related e-voting schemes mainly implementing blockchain technology are discussed along with their security robustness and vulnerabilities.

In 2018, Casado-Vara and Corchado [2] recommended a blockchain scheme to overcome the drawbacks of the conventional digital voting system since it mainly consists of the paper ballot or associated mechanical appliances such as EVM ballot system. They have proposed a digital voting system that is constructed using electronic polling devices basically into two verities: I-voting and E-voting. However, such a type of system faces various limitations like high bandwidth requirements, inflexible Internet and server connectivity, poor security, etc. [2]. In the same year, Kotsiuba et al. [5] proposed a decentralized e-health service platform based on a private and permission Exonum blockchain for storing and further accessing real-time medical documentation. In the same year, Yanovich et al. [6] proposed a fast consensus algorithm using Exonum and byzantine fault-tolerant protocol depending upon timestamp information. Hence, the transaction has no specific Merkle-proof structure. However, both the schemes mentioned in [5] and [6] suffer from vital security breaches such as insider attack, impersonation attack, etc. due to the lack of implementation of encryption/decryption mechanisms and failure to preserve user anonymity.

In 2019, Anyshchenko et al. [7] proposed a crypto token-based application using the Exonum blockchain. In this scheme, the traditional binary serialization format is utilized for communication between nodes of Exonum and used Tendermint consensus algorithm to avoid the mining process [7]. However, the Tendermint consensus algorithm provides poor service as compared to PBFT [8].

In the year 2020, Dhulavvagol et al. proposed [9] a digital e-voting system using the decentralized application blockchain, smart contract (SC), fingerprint-oriented hashing technique and Markle tree-based internal output generated system to solve various issues such as – authenticity, privacy, and confidentiality for the voters, voting information integrity, etc. In the same year, Sadia et al. [10] proposed, a biometric and blockchain-based e-voting scheme where eligible voters are given a specific time to cast their votes digitally after successful validation. Later, Shah et al. [15] enhanced the previous scheme [11] for an online e-voting arrangement using an Android application with the help of a unique key/one-time password. To maintain the security, both 128-bit AES encryption and SHA-256 hashing mechanisms are utilized. However, any adversary still becomes able to acquire the consensus mechanism of such a scheme. Roh and Lee [12] developed an e-voting system using the PBFT algorithm and private permission blockchain network. Due to the use of a permission mechanism, this scheme preserves confidentiality, security, and availability in access control. However, it suffers from biased key management, improper session management, and unprotected against DoS attack.

Jain et al. in 2021 [14], proposed a scheme “MATDAAN” utilizing Ethereum blockchain technology to set up a secure e-voting system since Ethereum is fast, reliable, open source application, cost-effective, and achieves anonymity. In this scheme, a unique QR code is generated as per the credentials provided by the user utilizing a one-time password. Unfortunately, this scheme [13,14] suffers from 51% attack. In 2021, Waheed et al. [15] proposed a novel ECC-based anonymous signcryption scheme for e-voting applications where only legitimate voters communicate with the polling server to cast

their votes as a signcryption structure. Though this scheme mitigates the limitations of unlinkability, forward secrecy, anonymity, and untraceability properties compared to other recent schemes, still it faces limitations of secure key distribution and implementations in a decentralized architecture.
In 2022, Jumaa et al. [16] proposed a lightweight elliptic curve cryptography(ECC) based e-voting scheme using public blockchain to enhance security mechanisms in Iraq by implementing biometric registration mechanism, QR code, synchronized e-voting models, SHA-256 hashing, PoW consensus, and efficient mining schemes with two or three leading zeroes. However, this scheme is still unable to mitigate 51% attack, high energy consumption, and double voting problems.
Recently, in 2023, Niloy et al. [17] proposed a U.S based secure and transparent e-voting system using a state-based blockchain scheme, reusable smart contract, web 3.0, and AI-based multilayer authentication and verification mechanism to mitigate 'double voting' and accelerated voter turnouts. However, voter details are stored in an SQL database, and state-based and wallet transactions are stored in a blockchain database which increases the overheads, storage cost, and complexity of maintenance of this scheme.
The above discussion about the previous related schemes is briefly summarized into a tabular format in table1 for easy understanding. The same reveals a need for an efficient, lightweight, and robust e-voting scheme that can enable remote users to cast their votes securely and anonymously.

TABLE 1. Description of Related Schemes

Schemes	Advantages	Limitations
Niloy et al. [17] 2023	Proposed a secure and transparent e-voting system using a state-based blockchain scheme to mitigate 'double voting' problems	Incurs huge computation and storage overhead
Jumaa et al. [16] 2022	Proposed a lightweight ECC-based e-Voting scheme using public blockchain	Unable to mitigate 51% attack and double voting problems
Waheed et al. [15] 2021	Proposed a novel ECC-based anonymous e-voting application, that mitigates the limitations of unlinkability, forward secrecy, anonymity, and untraceability	Insecure key distribution incurs huge communication overhead due to implementations of decentralized architecture
Zaghloul et al. [24] 2021	blockchain-based e-voting system for communication with IoT devices	Incurs huge communication and computation cost
Jain et al. [14] 2021	Proposed an e-Voting scheme "MATDAAN" utilizing Ethereum blockchain	Unable to mitigate 51% attack and double voting problems
Roh and Lee [12] 2020	Proposed an e-Voting system using the PBFT algorithm and private permission blockchain	Complex key management and session management, suffers from DoS attack
Sadia et al.[10] 2020	Proposed a biometric and blockchain- based e-voting decentralized system	Suffers from the double voting problem
Dhulavvagol et al. 2020	Proposed a digital e-Voting system using decentralized application	Suffers from key leakage problem

B. Motivation and contribution of the Research

From the above discussion in the literature review section, it is concluded that each of the existing e-voting schemes is either suffering from some security attacks or facing several security issues regarding the key management and failing to establish any secure e-voting transactions. On the other hand, some of the existing schemes are not competent considering communication and computation overheads.
The above-stated limitations motivate us to design a novel signature-based e-voting scheme that incorporates exonum blockchain using an ECC cryptosystem. The major contributions of the proposed scheme are summarized below:

i The limitations mentioned above motivate us to design an ECC-based novel e-voting application using a smart contract and Exonum private blockchain scheme.
ii The proposed scheme uses a secure hybrid consensus algorithm, a combination of both RAFT and PBFT algorithms.
iii The scheme ensures the confidentiality and authenticity of the votes using the zero-knowledge protocol, idemix scheme, and anonymity mechanisms.
iv In this application, a lightweight e-voting scheme is proposed using both ECC and one-way hash functions.
v This scheme considerably reduces communication and computation overheads and enhances the security strength using a private blockchain.

After analyzing all the previous e-voting schemes, it is seen that all the previous schemes either suffer from security defects or incur huge overheads. Key management, key distribution, anonymity, and confidentiality preservation are some other issues that must be achieved to execute secure e-voting from remote places. Then only traditional voting using EVM or other paper ballot voting can be replaced with this smart, digital, and secure e-voting system. The blockchain is one of the major one-stop solutions for all the above issues and can provide a huge advantage to society. This research work proposes a novel e-voting scheme using the private Exonum blockchain and reusable smart contracts to move towards an optimal solution to robust and secure e-voting.

C. Organization of the Paper

The remaining part of this paper is organized as: Section 2 illustrates a detailed discussion regarding preliminaries such

as brief functionality of Exonum blockchain technology and idemix technology for a better understanding of the scheme whereas in Section 3, different models and related security frameworks are discussed. Section 4, describes the proposed ECC-EXONUM-eVOTING scheme and its working procedure in detail. In Section 5 and Section 6, security analysis of the proposed scheme using the Random Oracle Model and simulation results using both AVISPA and Scyther simulation tools are demonstrated, respectively. Section 7 shows the comparative discussion of the performance analysis of the scheme concerning other existing e-voting schemes and finally, section 8 concludes this paper.

II. PRELIMINARIES

In this section, both the architecture as well as the functionality of Exonum blockchain and idexmix technology are illustrated.

A. Architecture and Functionality of Exonum Blockchain

Exonum blockchain is a type of private or consortium permission blockchain [5-7, 12, 22]. The fundamental features of this architecture are depicted in figure 1 and briefly described below.

a. It is an open-source application and contains full nodes connected through a peer-to-peer network and lightweight client [5,6]. It communicates with peer nodes through middleware and also maintains proper consensus mechanisms.
b. Full nodes make a copy of all stored information from the blockchain, construct a replica, and allocate the replica to the distributed database for accessing purposes [23].
c. The full nodes also maintain an authentication and data privacy mechanism communicating with Blockchain Storage DLT considering Exonum MerkleDB using the public key.
d. Full nodes are divided into two additional peers - validators and auditors. The validators create or append new blocks in the blockchain using Byzantine Fault Tolerant (BFT) whereas the auditor maintains the consistency of the whole blockchain.
e. The functionality of Exonum generally depends on the Service Oriented Architecture (SOA) and consists of three different components: Service, Lightweight client, and Middleware shown in Figure1.
f. Service incorporates main business logic, transaction rules, and service states. Clients are the main initiators who perform various key management activities. Middleware application provides interoperability between the service application and the lightweight client.

B. Idemix (Identity Mixture) Technology

Idemix is a technology that supports a cryptographic protocol suite developed by IBM Switzerland to provide some

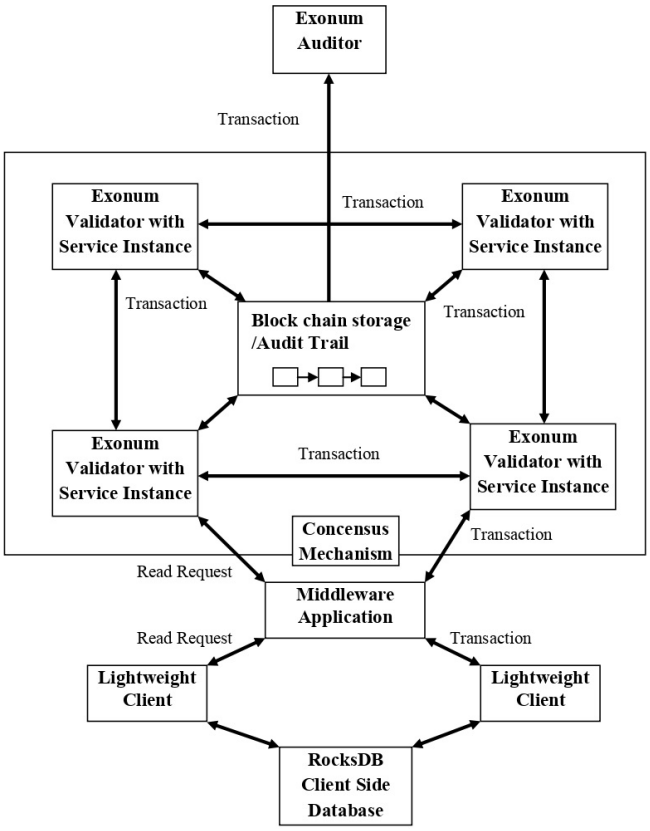

FIGURE 1. Functional Model of Exonum Blockchain

eminent features; which are – (i) unlinkability, which is a property that a single identity can launch several transactions without disclosing the identity of the user, (ii) anonymity, it is a privacy-preserving property by which the initiator of the transaction can complete the transaction without revealing the necessary details [18,19, 22]. This technology is built on an efficient Zero Knowledge protocol (ZPK) and blind signature scheme [19].

C. Communication Model

ECC-EXONUM-eVOTING adopts a communication model to perform secure transactions among the lightweight decentralized client application (Dapp), validator attached with service interface and auditor. The communication model is depicted in Figure 2. In the diagram, the solid lines indicate that the communication is performed through an insecure path and an invalid transaction mechanism.

a. Participating candidates: They are registered and valid candidates in the e-voting process.
b. Participating voters: They are registered and valid voters as per the voter list used in the e-voting process.
c. Validator with service instance: For the generation of the new block, it validates each transaction and includes them in the new block to be added to the blockchain.

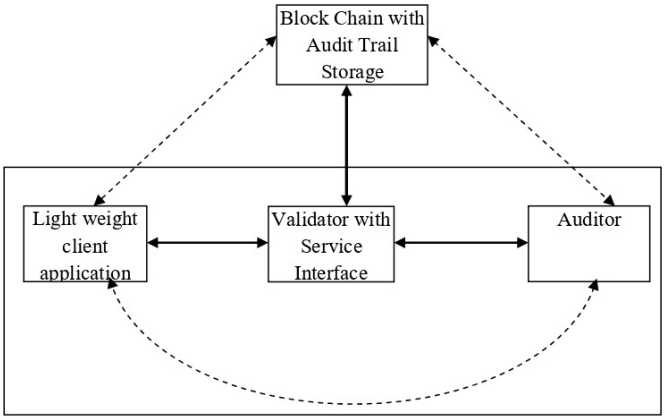

FIGURE 2. **Communication model using Exonum**

d. Auditor: It checks the consistency of the whole blockchain used in the e-voting scheme and also maintains an absolute copy of the whole blockchain.

D. Blockchain as a Service (BaaS) Model

BaaS model provides a security restriction against the outsourcing of the related information for backend applications by business clients or users who are generally authenticated and authorized for access to the frontend application and also provides remote updating, database and cloud server storage management, hosting services, push notifications, etc. for various mobile applications. Many reputed worldwide organizations follow this model such as IBM BaaS model, Microsoft Azure BaaS model, Amazon BaaS model Oracle blockchain cloud hosting BaaS model, etc. However, in the ECC-EXONUM-eVOTING scheme, the IBM BaaS model is considered for providing security restrictions for backend services [23].

E. Threat Model

A situation is considered where several transactions are carried out through an insecure channel that is directed by a challenger $\mathcal{A}$ and the whole transactions are compromised. In this situation, the de-facto standard model - Dolav-Yao (DY) threat model [25] is considered like other related authentication and key management schemes [2,5,7-14]. Moreover, we have incorporated the recent security model, i.e., Canetti and Krawczyk's adversary model (CK adversary model) [26] in ECC-EXONUM-eVOTING. If a situation is considered where one of the session-specific random credentials is compromised by $\mathcal{A}$ from any previous sessions, the session key is eventually compromised. This is called a session-specific random information attack.

III. PROPOSED SCHEME

In this scheme, a novel e-Voting protocol is proposed using the service-oriented decentralized architecture of Exonum private blockchain using a secure elliptic curve cryptosystem,

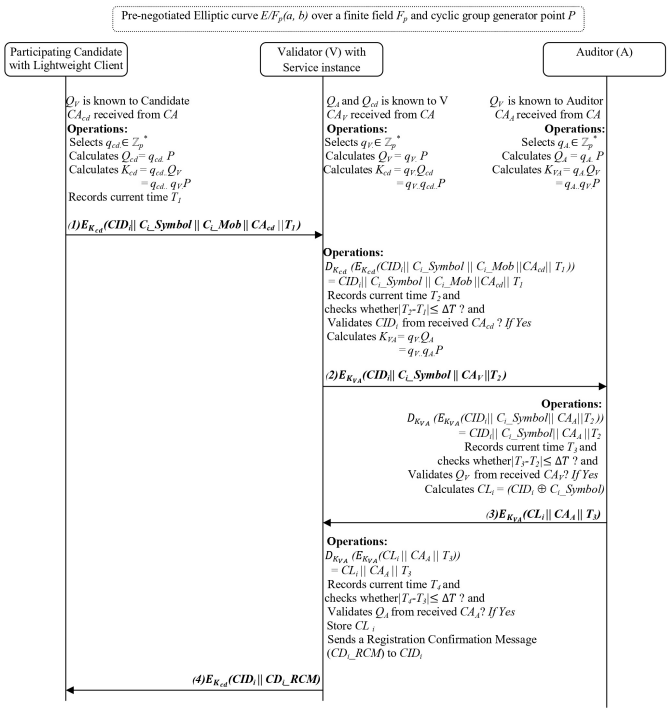

FIGURE 3. **Candidate Registration Phase**

hybrid consensus algorithm (combining both PBFT and RAFT), secure contributory public and session keys generated by using ECDH operations and shared public information among the participants using public key certificates (CA_{cd}, CA_V and CA_A) received from the certificate authorities. A major part of the e-voting process is maintained by the validator with Service instance and among the other entities of Exonum - lightweight client (Dapp), middleware, and auditors. ECC-EXONUM-eVOTING is mainly designed for e-Voting application for space-limited constraint devices using a lightweight client application (Dapp) to validate and establish secure sessions valid for small time duration (ΔT) used for transactions among registered candidates, registered voters, validators, and auditors. This scheme consists of four different phases - i) the Candidate registration phase, ii) the Voter registration phase, iii) the Voter authentication and vote casting phase, and iv) the Blockchain creation and vote counting phase. For an overall understanding of the functionalities of the ECC-EXONUM-eVOTING scheme, different phases of the system are described below and the notations used in this protocol are exhibited in Table2. Different figures of diverse phases are expressed below where $S \rightarrow R : TM$ signifies that the sender S forwards a TM (transaction message for communication) to the receiver R.

A. Candidate Registration Phase

This phase is performed among the candidate, the validator, and the auditor. The same is depicted in Figure 3.

TABLE 2. Description Of Individual Notations

Notation	Description
C,P,V,A	Participating candidate, participating voter, validator and auditor
F_g	A large prime finite field over *g*
$E_g(a,b)$, *G*	An elliptic curve, based on prime finite field and generator is defined over the elliptic curve of order *n*
CID_i	Identity of the registered candidate in e-Voting
C_i*_Symbol*	Symbol of the registered candidate
C_i*_Mob*	Mobile number of the registered candidate
H_{PV}	Anonymous identity of the registered voter
F_p	Biometric fingerprint information of the participating registered voter
CA_{cd}	Public key certificate of candidate
CA_V	Public key certificate of validator
CA_A	Public key certificate of auditor
CL_i	Valid list of participating registered candidates
VL_i	Valid list of participating registered voter
SK	Dynamic session key shared between the validator and participating voter
T_{SK_V}	Session key generation time by the validator that is valid for a small time duration
TS	Transactional message communication
h(.)	Secure one way hash function for instance *SHA1*
E/D	Algorithm based on symmetric encryption/decryption process
(q_{cd}, Q_{cd})	Participating candidate's public-private key pair
(q_V, Q_V)	Participating validator's public-private key pair
(q_A, Q_A)	Participating auditor's public-private key pair
(q_{PV}, Q_{PV})	Participating auditors public-private key pair Q_{PV}= $q_{PV}.P$
BLK_i	Voter wise generated block for e-Voting process.
Blk_Chn_i	Final blockchain generated by the validator
Blk_Chn_{i-1}	Previous blockchain where more blocks are required to be added by the validator
$\|\|$	Concatenation operator for different parameters of the communicated messages.

***Step 1*: C→ V:** $E_{K_{cd}}(CID_i||C_i\_Symbol \,||\, C_i\_Mob \,||\, CA_{cd} \,||\, T_1)$
In this phase, (shown in Figure 3 the participating candidates have to be registered to the validator for participating in the e-Voting process using ECC-based point multiplication and hash operation. The following operations are performed in this phase -i) Generate Q_{cd}= q_{cd}.P, and K_{cd} = $q_{cd}.Q_V$ = $q_{cd}.q_V.P$ ii) records the current time T_1 for further communication using contributory symmetric key K_{cd} among the validator. The public key Q_V is pre-shared with the candidate by the validator. Later, participating candidates forward their encrypted registration messages - $E_{K_{cd}}(CID_i||\, C_i\_Symbol \,||\, C_i\_Mob \,||\, CA_{cd}||\, T_1)$ along with the voting symbols C_i*_Symbol* and CA_{cd} of the candidate to validator.
***Step 2*:V→ A:** $E_{K_{VA}}(CID_i||\, C_i\_Symbol \,||CA_V \,||T_2)$
In step 2, the validator also generates the symmetric key K_{cd} using pre-shared public key Q_{cd} by the participating candidate and K_{cd} is calculated using ECDH based point multiplication as K_{cd} = $q_{cd.}.Q_V$ = $q_{cd}.q_{V.}.P$. Later on, the validator decrypts the message and gets the candidate's identity, public key certificate, and participating symbol, along with the mobile number. Further, it validates the current time stamp ΔT as well as CID_i received from CA_{cd}. Based on successful validation, validators calculate K_{VA}= $q_V.Q_A$ = $q_{V.}.q_A.P$ using the public key Q_A which is pre-shared with the validator. Finally, validators encrypt the message with generated public key $E_{K_{VA}}(CID_i||\, C_i\_Symbol \,||\, CA_V \,||T_2\,)$ and forwards it to the auditor.
***Step 3*:A→V:** $E_{K_{VA}}(CL_i \,||\, CA_A \,||\, T_3)$
In step 3, the auditor generates i) symmetric key K_{VA}= $q_A.Q_V$= $q_A.q_{V.}.P$ using the pre-shared public key Q_V of the validator, ii) decrypts the received message and acquires the candidate identity and participating symbol CID_i, C_i*_Symbol,* CA_A and T_2, iii) records current time T_3 and validates whether $|T_3\text{-}T_2| \leq \Delta$T, iv) validates Q_V from received CA_V and v) based on successful validation, the auditor generates the list of participating valid candidate CL_i = *(*$CID_i \oplus C_i$*_Symbol)* for further voting purpose and forwards the same CL_i to the auditor along with the current time T_3 as an encrypted format $E_{K_{VA}}(CL_i \,||\, CA_A \,||\, T_3)$.
***Step 4*: V →C:** $E_{K_{cd}}(CID_i \,||\, CD_i\_RCM)$
In step 4, the validator decrypts the received message with the contributory symmetric key K_{VA} and obtains *i)* CL_i , CA_A and T_3, *ii)* records current time T_4 and validates whether $|T_4\text{-}T_3| \leq \Delta\ T$, iii) validates Q_A from received CA_A and *iv)* forwards the registration confirmation message CD_i*_RCM* along with the identity of the candidate as an encrypted format $E_{K_{cd}}(CID_i \,||\, CD_i\_RCM)$ to the participating candidate.

B. Voter Registration Phase

This phase is performed between the voter, the validator, and the auditor. This phase is depicted in Figure 4.
***Step 1*: P →V:** $E_{K_{PV}}(H_{PV} \,||\, R_{PV} \,||F_p \,||\, T_5)$
In this phase (shown in Figure 4), using both ECC-based point multiplication and hash operation, participating voters have to register themselves to the validator to participate in the e-Voting process using *i)* Q_{PV}= $q_{PV}.P$, *ii)* K_{PV} = $q_{PV}.Q_V$ = q_{PV} .$q_V.P$, *(iii)* R_{PV} = $r_{PV}.q_{PV}.Q_A$ = $r_{PV}.q_{PV}.q_A.P$ and *(iv)* H_{PV} = *h (*$R_{PV} \,||\, K_{PV}$*)*. Later, the voter records the current time T_5, communicate the message $E_{K_{PV}}(H_{PV} \,||\, R_{PV} \,||F_p \,||\, T_5)$ using contributory symmetric key K_{PV} to the validator in Step 1 where the public keys Q_V and Q_A are shared previously with voter by the validator and anonymity of the voter is preserved.
***Step 2*: V →A:** $E_{K_{VA}}(H_{PV} \,||\, R_{PV} \,||F_p \,||\, V_1||\, CA_V \,||\, T_6)$
In Step 2, the symmetric key K_{PV} is also generated by the validator using the public key Q_{PV} that is pre-shared with validator. Further, K_{PV} is calculated using ECDH based point multiplication as K_{PV} = $q_V.Q_{PV}$ = $q_V.q_{PV}.P$. Later

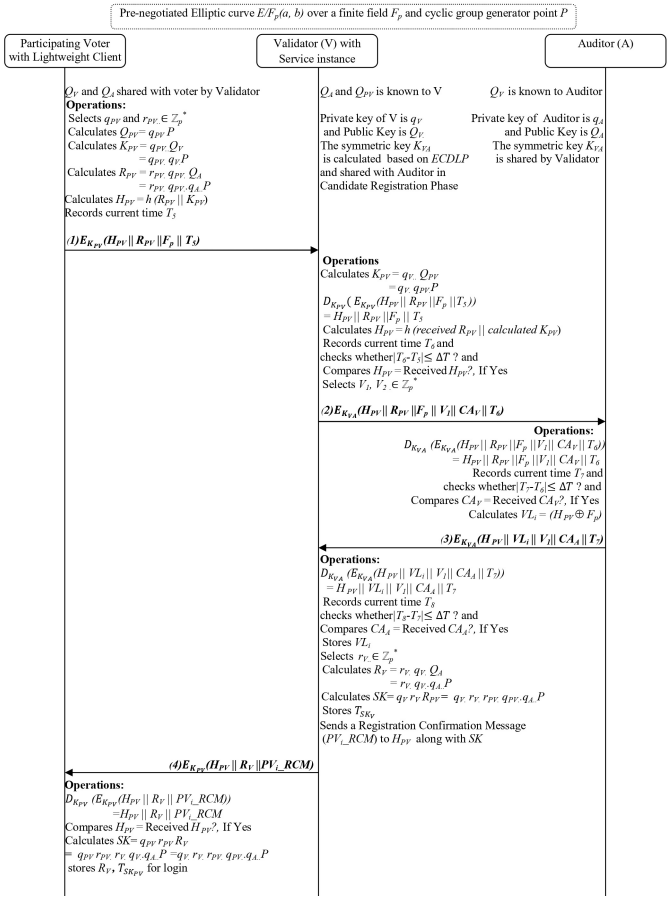

FIGURE 4. Voter Registration Phase

on, validator decrypts the message $D_{K_{PV}}(\ E_{K_{PV}}(H_{PV}\ ||\ R_{PV}\ ||F_p\ ||T_5\ ))$, obtains the anonymous identity H_{PV} and random generated value R_{PV} of the respective voter, finger print F_p along with current time T_5 . Further, validator calculates *i)* H_{PV} = *h (received* R_{PV} || *calculated* K_{PV}), *(ii)* validates the H_{PV} with received H_{PV}, *(iii)* records current time T_6, *(iv)* validates the $|T_6\text{-}T_5| \leq \Delta T$ and *(v)* compares H_{PV} = received H_{PV}. Based on successful verification, validator randomly selects two variables V_1 and V_2 for further communication. Later, validator, encrypts the message with generated public key $E_{K_{VA}}(H_{PV}\ ||\ R_{PV}\ ||F_p\ ||\ V_1||\ CA_V\ ||\ T_6\ )$ and forwards the same to auditor for further communication.

***Step 3*: $A \rightarrow V$: $E_{K_{VA}}(H_{\ PV}\ ||\ VL_i\ ||\ V_1||\ CA_A\ ||\ T_7)$**

In step 3, auditor decrypts the message received from auditor with the symmetric key K_{VA} generated based ECDH and gets the anonymous identity H_{PV} of participating voter, finger print (F_p), public key certificate (CA_V), current time stamp T_6 and other secret information. Later, it validates (i) duration of the time stamp ΔT i.e $|T_7\text{-}T_6| \leq \Delta T$, (ii) public key certificate (CA_V) of the validator with the previously stored information and (iii) based on successful validation, auditor further generates voter list $VL_i = (H_{\ PV} \oplus F_p)$ and forwards VL_i to validator along with the current time T_7,

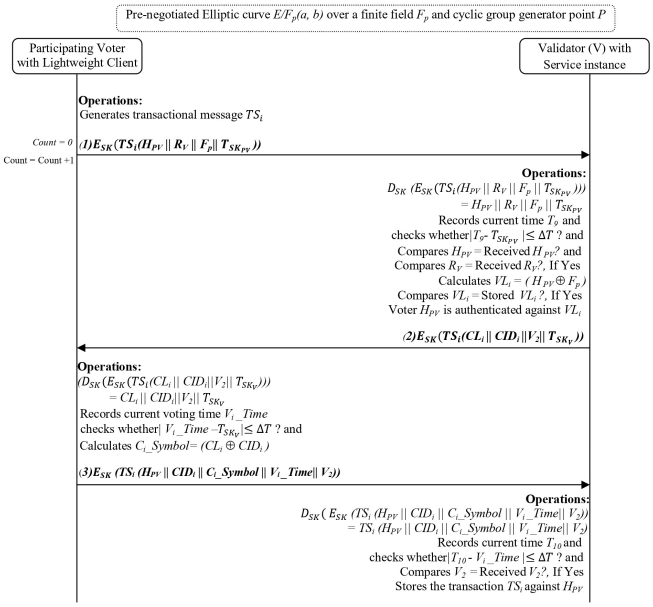

FIGURE 5. Voter Authentication and Vote Casting Phase

H_{PV} , public key certificate (CA_A) of auditor and other secret information as an encrypted format using K_{VA}.

***Step 4*: $V \rightarrow P$: $E_{K_{PV}}(H_{PV}\ ||\ R_V\ ||PV_i\_RCM)$**

In step 4, the validator decrypts the encrypted message with the contributory symmetric key K_{VA} and obtains the information of (i) the specific voter from the anonymous identity H_{PV}, (ii) voter list VL_i and (iii) public key certificate (CA_A). Later, the validator verifies the CA_A and time stamp duration to validate the authenticity of the auditor and accordingly accepts as well as stores the voter list VL_i or rejects it. Further, validator generates the arbitrary random value (i) $R_V = r_V.q_V.Q_A = r_V.q_V.q_A.P$ and (ii) contributory session key $SK = q_V.r_V.R_{PV} = q_V.r_V.r_{PV}.q_{PV}.q_A.P$ based on ECDLP using private key components and secret random values. Moreover, validator achieves the session key generation time (T_{SK_V}) for further communication and generates Registration Confirmation Message (PV_i*_RCM)* of validator and forwards the encrypted message $E_{K_{PV}}(H_{PV}$ || *SK*|| R_V ||PV_i*_RCM)* to participating voter.

After receiving the message from the validator, the participating voter decrypts the message using K_{PV} and validates the anonymous identity H_{PV} with received one and generates the contributory session key $SK = q_{PV}\ r_{PV}\ R_V = q_V.\ r_V.\ r_{PV}.\ q_{PV}.q_A.P$. Later, the voter stores the session key generation time of the voter ($T_{SK_{PV}}$) along with R_V for further login purposes.

C. Voter Authentication and Vote Casting Phase

During this phase, only transactions are communicated between participating voters and validators as shown in Figure 5.

***Step 1*: $P \rightarrow V$: $E_{SK}(TS_i(H_{PV}\ ||\ R_V\ ||\ F_p||\ T_{SK_{PV}}\ ))$**

In step 1, the voter forwards the voting authentication message encrypted using *SK* that contains i) the anonymous identity of the voter H_{PV}, ii) arbitrary random message R_V generated by the validator, iii) biometric information F_p of the voter and (iv) session key generation time of the participating voter.

***Step 2*: $V \rightarrow P$: $E_{SK}(TS_i(CL_i \mid\mid CID_i \mid\mid V_2 \mid\mid T_{SK_V}))$**

In this round, validator first decrypts the authentication messages and obtains several components – i) H_{PV}, *ii)* R_V, *(iii)* F_p and *(iv)* $T_{SK_{PV}}$. Now, it records current time T_9 and validates whether $|T_9 - T_{SK_V}| \leq \Delta T$, where ΔT is the permissible period. Moreover, the validator also authenticates the anonymous identity of the voter H_{PV} and random messages R_V are identical one or not. If the validation is true then i) the validator computes the voter list with the anonymous identity $VL_i = (H_{PV} \oplus F_p)$ (ii) verifies it with the previously stored one. Derived from successful validation of VL_i, the voter H_{PV} is authenticated against VL_i and forwards the transaction $E_{SK}(TS_i(CL_i \mid\mid CID_i \mid\mid V_2 \mid\mid T_{SK_V}))$ to the voter. The message contains (i) participated candidate list CL_i, ii) identities of the candidates CID_i to obtain the vote casting symbol, and iii) session key generation time of the validator.

Step 3*: $P \rightarrow V$: E_{SK} *(*TS_i *(*$H_{PV} \mid\mid CID_i \mid\mid C_i$*_Symbol* $\mid\mid V_i$ *_Time*$\mid\mid V_2$*))

In step 3, voter first i) records the current voting time V_i *_Time*, ii) verifies the validity of the session by $|V_i$*_Time* $- T_{SK_V}| \leq \Delta T$. Accordingly, the voter selects the suitable candidate with symbol C_i*_Symbol= (*$CL_i \oplus CID_i$ *)* and casts his/her vote along with i) anonymous identity H_{PV}, ii) the suitable candidate's identity CID_i, iii) symbol for vote casting C_i*_Symbol*, iv) vote casting time V_i *_Time* and v) secret variable V_2 that is sent by the validator in Step 2 as a proof for further authentication. Later, voter encrypts the voting transaction message with *SK* and forwards the transaction E_{SK} *(*TS_i *(*$H_{PV} \mid\mid CID_i \mid\mid C_i$*_Symbol* $\mid\mid V_i$ *_Time*$\mid\mid V_2$*))* to the validator. In this case, a variable *count* is initialized to 0 and enhanced next to 1 for each unsuccessful transaction and permitted up to three different attempts otherwise the communication is terminated. After receiving the voting transaction, validator i) records the current time T_9, *ii)* validates the duration of the transaction i.e. whether $|T_9 - T_{SK_{PV}}| \leq \Delta T$ iii) certifies the transaction based on the validation of the variable V_2 and stores the voting information against anonymous identity H_{PV}.

D. Blockchain Creation and Vote Counting Phase

In this phase, separate blocks are generated based on the provided voting information received from the respective voter containing the anonymous identity H_{PV} along with the candidate symbol and other information used for the voting purpose. The phase is depicted in Figure 6. Later, each block is appended to the blockchain based on the proper validation mechanism. Finally, the voting results are counted and displayed accordingly.

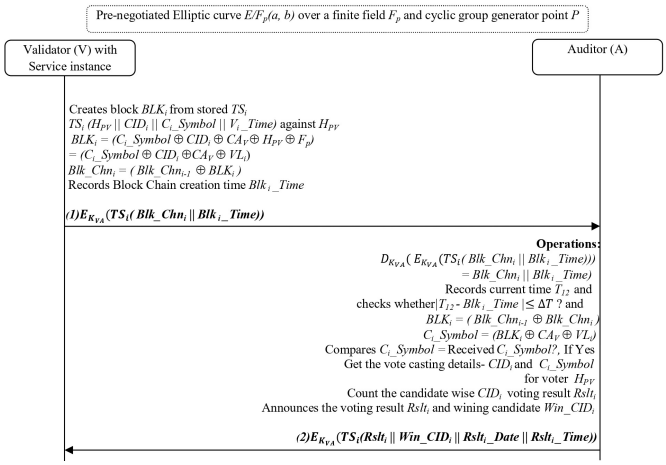

FIGURE 6. Blockchain Creation and Vote Counting Phase

***Step1*: V $\rightarrow$ A: $E_{K_{VA}}(TS_i($** *Blk_Chn*$_i \mid\mid$ *Blk* $_i$ *_Time))*

In Step 1, block BLK_i is generated by the validator using the following information for vote casting transaction TS_i received from the anonymous voter H_{PV} .

$BLK_i = (C_i$*_Symbol* $\oplus$ $CID_i \oplus CA_V \oplus H_{PV} \oplus F_p) = (C_i$*_Symbol* $\oplus$ $CID_i \oplus CA_V \oplus VL_i)$ and *Blk_Chn*$_i$ *= (* *Blk_Chn*$_{i-1} \oplus BLK_i$ *)*

Later, validator appends the newly generated block BLK_i to the existing blockchain *Blk_Chn*$_i$ that contains the voting information of the anonymous voter H_{PV}.

Further, validator records the generation time of the blockchain *Blk*$_i$ *_Time* and forwards the encrypted transactional message of blockchain $E_{K_{VA}}(TS_i($ *Blk_Chn*$_i \mid\mid$ *Blk* $_i$ *_Time))* to auditor for validation and counting the e-Voting result.

Step 2*:A $\rightarrow$ V: $E_{K_{VA}}(TS_i($Rslt***$_i \mid\mid$ *WinCID*$_i \mid\mid$***Rslt***$_i$ *_Date* $\mid\mid$ ***Rslt***$_i$ *_Time))*

In step 2, auditors decrypt the encrypted message to obtain the blockchain *Blk_Chn*$_i$ as well as blockchain creation time *Blk*$_i$*_Time* and records the current time T_{12} to ensure whether $|T_{12}$ - *Blk* $_i$ *_Time* $| \leq \Delta T$. Based on successful validation, auditors extract the vote-casting symbol of the voter C_i*_Symbol = (*$BLK_i \oplus CA_V \oplus VL_i$*)* and compare the symbol with the casted vote. Accordingly, get the details of the casting vote against the anonymous voter H_{PV}. Later, the auditor counts the candidate wise CID_i voting result $Rslt_i$, announces the voting result $Rslt_i$ and wining candidate Win_CID_i. Finally, forwards the encrypted message $E_{K_{VA}}(TS_i($***Rslt***$_i \mid\mid$ *Win_CID*$_i \mid\mid$ ***Rslt***$_i$ *_Date*$\mid\mid$ ***Rslt***$_i$ *_Time))* to the validator.

In this scheme, we have considered a persistent storage location using the concept of Exonum MerkleDB (as shown in Figure 1 as Blockchain storage) that supports a merklized structure (as shown in Figure 6) like a shared digital ledger (DLT) that allows participants(Voters/Candidates) to record transactions and share information securely, tamper-resistant way in the distributed network but only has restricted access permission for Validators and Auditors for data storage and

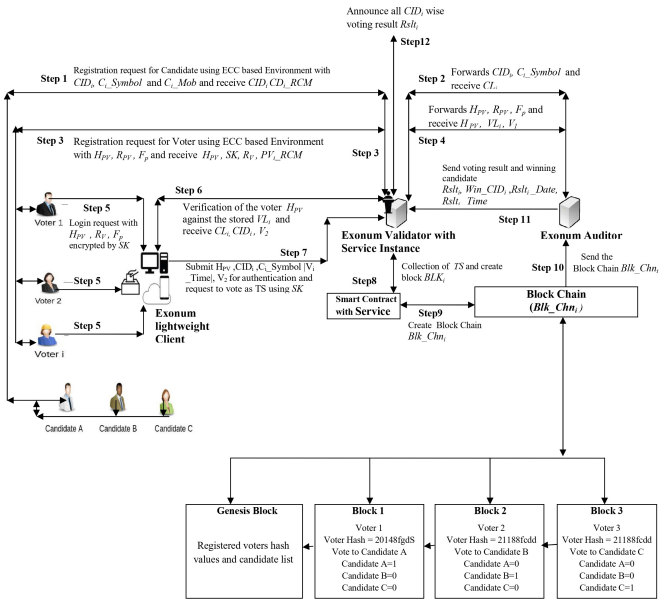

FIGURE 7. **Overall Procedure of the Proposed System**

retrieval. Moreover, Auditors have access to verify and recover the shared information communication with the shared DLT.

IV. SECURITY ANALYSIS

This section mostly deals with the analysis of different security features and ascertains the robustness of the ECC-EXONUM-eVOTING system. To investigate the security strength of the e-voting scheme, generally, two different types of security analysis have been performed for any scheme- I) formal security analysis with ROM (Random Oracle Model) and II) informal security analysis. Both AVISPA and Scyther simulation tools are used for establishing our claim about the security robustness of the proposed scheme. This section demonstrates that the proposed scheme is robust and secure against all possible security attacks with the help of formal and informal security analysis.

A. Formal Security Analysis using Random Oracle Model

ROM was proposed by Phillip Rogaway, Bellare, and Mihir in 1993 as a turning machine that works as a probabilistic polynomial time (PPTTM) [27] and is utilized to test the security-related limitations of various authentication protocols where a game is played between the adversary $\mathcal{A}$ and the challenger C. The working procedure of ROM is also based on the Real-Or-Random (ROR) model, which works on the security issues of session keys [28, 29].

An analysis is performed using ROM for two major phases of ECC-EXONUM-eVOTING: i) voter authentication and vote casting phase; and ii) blockchain creation and vote counting phase. It consists of four participants: candidates, participating voters, validators, and auditors.

The verification of semantic security of ECC-EXONUM-eVOTING is described in Theorem 1 using the Real-or-Random model, where it is presumed that the adversary $\mathcal{A}$ runs an e-Voting transaction against the ECC-EXONUM-eVOTING scheme at polynomial time *tm* to rupture the semantic-related security and acquire the benefit in the ROM model.

The advantage function of the adversary $\mathcal{A}$ is given in theorem 1 which proves that the advantage of the adversary is less than the probability of breaking the security of the scheme.

Theorem 1

$$Advr_{\mathrm{ECC-Exonum-eVoting}}{}^{ASKE}(tm) \leq$$

$$\frac{q_h^2}{|Hash|}+\frac{q_{send}}{2^{r-1}.|U|}+2.Advt_{\mathrm{ECC-Exonum-eVoting}}{}^{ECDLP}(tm)$$

A thorough description of the random oracle model and the proof of the Theorem 1 is discussed in Appendix 1. Additionally, the details of the proof of ROM for the ECC-EXONUM-eVOTING scheme are described in detail in a separate file *Appendix* under section *Appendix1*. According to the final deduction in equation no. 11, it is concluded that the theorem is proved, and correspondingly, it is concluded that the advantage of the adversary in compromising the proposed protocol in polynomial time is insignificant.

B. Informal Security Analysis

This section demonstrates the informal security analysis of the ECC-EXONUM-eVOTING scheme using arithmetical practices with the consideration of a realistic hypothesis.

Man-in-the-Middle Attack

Suppose a challenger $\mathcal{A}$ is surreptitiously listening the e-Voting transaction, intercepts the initial transactions those contain $E_{K_{cd}}(CID_i||\ C_i\_Symbol\ ||\ C_i\_Mob\ ||\ CA_{cd}\ ||T_1\ )$, $E_{K_{VA}}(CID_i||\ C_i\_Symbol\ ||\ CA_V\ ||T_2\ )$, $E_{K_{VA}}(CL_i\ ||\ CA_A\ ||\ T_3)$ and $E_{K_{cd}}(CID_i\ ||\ CD_i\_RCM)$ and intends to modify those transactions in such a way that such transactions look as if approaching from a legitimate participant but with the substituted values of CA_{cd}, CA_V *or* CA_A of the adversary. Though, each participating entity computes the contributory symmetric keys, $K_{cd} = q_{cd.}.Q_V = q_{cd.}.q_V.P$ and $K_{VA} = q_{V.}.Q_A = q_{V.}.q_A.P$ using ECDH scheme. Further, using the symmetric keys, validator or participating voters computes $H_{PV} = h\ (R_{PV}\ ||\ K_{PV})$, where R_{PV} is calculated $R_{PV} = r_{PV}.\ q_{PV}\ .Q_A = r_{PV}.\ q_{PV.}.q_{A.}.\ P$ and $R_V = r_{V.}.\ q_{V.}.\ Q_A = r_{V.}.\ q_{V.}\ q_{A.}.\ P$ and validates the anonymous identity H_{PV}, with the obtained transaction. Based on the failed affirmation, such transactional communication will be discarded. Furthermore, if $\tilde{A}$ attempts to amend the contents R_{PV} or R_V, s/he will not be able to execute the same due to using point multiplication using ECDLP that is inflexible to forge within polynomial instances. Hence, the ECC-EXONUM-eVOTING scheme is strong in the case of such an attack.

Denial of Service Attack (DoS)

In the voter authentication and vote casting phase of ECC-EXONUM-eVOTING**,** both the voter and validator convey their transactional messages within a precise time limit ΔT, and each voter is allowed to authenticate himself within three different numbers of attempts; otherwise, the participating voter will be immobilized for a specific duration. In this regard, a variable *count* is initialized with an initial value of 0 and increased to 1 for every unsuccessful e-Voting transaction; otherwise, the entity is not allowed to participate anymore in e-Voting transactions for the specific session. Hence, $\tilde{A}$ will be unable to assemble the e-voting mechanism available. Thus ECC-EXONUM-eVOTING manages the DoS attack

Distributed Denial of Service Attack (DDoS)

It is also a type of DoS attack, but numerous attackers or diverse nodes are used to flood targeted resources. So, it has occurred from multiple remote locations or peer nodes. In the voter authentication and vote-casting phases, each voter is allowed to authenticate within three attempts; otherwise, the participating voter will be deactivated for a specific duration. On the other hand, session key generation times ($T_{SK_{PV}}$ and T_{SK_V}) for both the voter and validator are also remain operative for small time duration ($\Delta\ T$ only, and the whole e-Voting process has to be completed within the specific time. Moreover, for the authentication as a valid voter, every adversary $\tilde{A}$ has to provide the anonymous identity (H_{PV}) as well as random message (R_V) those are generated based on robust ECDLP scheme and biometric information (F_p) and all those information will be validated by the validator with the pre-stored information. The whole authentication transaction is encrypted by contributory session key $SK = q_{V.}.r_{V..}.r_{PV.}.q_{PV.}.q_{A.}.P$ that is generated on ECDH based robust scheme, private keys and random values. Hence, $\tilde{A}$ will be unable to break *SK* because of the rigidity of ECDLP and get the necessary information for authentication purposes. So, this scheme handles DDoS attack.

51 % and 34% Attacks

In ECC-EXONUM-eVOTING, participating candidates or voters have to be registered first to gain access to the e-Voting scheme after successfully satisfying the proper authentication mechanism. For the candidate registration, several messages are communicated between the candidate, validator, and auditor using contributory public keys: $E_{K_{cd}}$ or $E_{K_{VA}}$ those are generated using the ECDH scheme and public key certificates generated by certificate authorities based on *PKI* validation rule. Later, validator generates a registration confirmation message (CD_i*_RCM*) for the valid candidate CID_i. On the other hand, auditors also generate a valid candidate list CL_i and forward it to the validator for validation of the voting outcomes. Alternatively, during voter registration, some messages are also communicated between the voter, validator and auditor using ECDH-based contributory public keys $E_{K_{PV}}$ and $E_{K_{VA}}$ along with public key certificates, voter list VL_i and registration confirmation message (PV_i*_RCM*) and those are generated for valid anonymous voter $H_{PV.}$. After completion of registration process, a contributory session key $SK = q_{V.}.r_{V..}.r_{PV.}.q_{PV.}.q_{A.}.P$ is also generated using private keys ($q_{V.}$,$q_{PV.}$ and q_A) and random values ($r_{V.}$ and $r_{PV.}$) in a ECDH based environment for communication between the registered voter and validator using the session based communication that is valid for $\Delta\ T$ only. So, several authentication, authorization, validation, and robust ECDH-based keys are generated for both the participating voter and candidates to gain access in the ECC-EXONUM-eVOTING application and preserve the accessibility of Merkle tree and computing power of the 51 % or 34 % peer nodes from malicious access [16, 20, 21, 37, 38, 40, 41]. So it is capable of defending both 51 % and 34 % of attacks.

Double Voting Problems

To prevent this attack, the system must confirm that only one vote was cast by the specific voter [14, 40]. Suppose a contender $\tilde{A}$ assumes to be a certified authority related to the e-voting system. Further, $\tilde{A}$ imitates the broadcasted transaction of a specific voter, assembles the user voting credentials, and casts the vote in the e-Voting system for the specific voter to get the advantage of double voting for the specific voter. However, in the ECC-EXONUM-eVOTING scheme, the anonymous identity of voter H_{PV} is maintained based on the idemix technology where H_{PV} is generated using ECDLP point multiplication and one-way hash function. $H_{PV} = h\ (R_{PV}\ ||\ K_{PV})$, where $R_{PV} = r_{PV.}.q_{PV.}.q_{A.}.P$ and $K_{PV} = q_{PV.}.q_{V.}.P$. In this case both the public keys Q_V and Q_A are shared with voter by the validator. For the registration, voter authentication, and vote-casting phases, the voter generally uses anonymous identity H_{PV} and biometric fingerprint information F_p along with other secret credentials either for registration or vote-casting. So, this scheme is capable of defending against this attack.

Private Key Related Security Attack

This attack deals with mainly the confidential private key-related security issues [37, 44] that are used to generate the public keys and shared between the e-Voting participants. However, in the ECC-EXONUM-eVOTING scheme, only public keys (Q_{cd}, Q_V Q_A and Q_{PV}) are shared and those are generated ECDH based point multiplication environment as $Q_{cd} = q_{cd.}.P$, $Q_V = q_{V.}.P$, $Q_A = q_{A.}.P$ and $Q_{PV} = q_{PV}.P$ which is unfeasible to conciliate because of the rigidity of ECDLP. Later, using ECDH, symmetric contributory keys K_{cd}, K_{VA} and K_{PV} are also generated and those are used for further communication among the participants. Later, contributory session keys $SK = q_{V..}.r_{V..}.r_{PV.}.q_{PV.}.q_{A..}.P$ are also generated using private keys ($q_{V.}$,$q_{PV.}$ and q_A) and random values ($r_{V.}$ and $r_{PV.}$) in an ECDH based environment. Hence, ECC-EXONUM-eVOTING is harmless in case of such an attack.

Insider Attack

For authentication and vote-casting purposes, several transactions are communicated between the peers. In this scenario, if any one of the transactions is achieved by $\tilde{A}$, still s/he

is unable to state as an authentic validator of the e-Voting system because most of the transactions are communicated using shared public keys (Q_{cd}, Q_V , Q_A and Q_{PV}) those are generated using ECDLP which is unfeasible to conciliate due to rigidity of ECDLP. On the other hand, messages also contain anonymous identity of voter H_{PV} that is generated using ECDLP, public key certificates (CA_{cd}, $CA_{A,}$ CA_V) generated by the certificate authority based on proper PKI validation rule and time stamp validation in every step. Additionally, contributory session keys are also used and computed as $SK= q_{V..}.r_{V..}.r_{PV.}.q_{PV.}.q_{A.}.P$ using private keys ($q_{V.}$,$q_{PV.}$ and q_A) and random values ($r_{V.}$ and $r_{PV.}$) in an ECDH based environment. So, it is unfeasible in favor of $\tilde{A}$ to guess SK due to the rigidity of ECDH. Therefore, this proposed scheme is harmless in case of insider attack.

Transaction Privacy Linkage Attack

Blockchain technology uses transactional communication among the participating entities. So, security mechanisms or models must be followed to perform secure transactions [42] and avoid the chance of attacks on e-voting applications. Generally, various security mechanisms are considered nowadays, for secure transactions like zero-knowledge property, homomorphic cryptosystem, crypto note, etc. are used [43] for e-Voting purposes. However, for performing secure transactions for the ECC-EXONUM-eVOTING scheme, we have incorporated private blockchain, idemix technology, zero-knowledge property, blind signature scheme, and anonymous identity of voter H_{PV}. On the other hand, every transaction is encrypted with either contributory symmetric keys K_{cd} and K_{PV} or SK. However, SK is also generated using private keys ($q_{V.}$,$q_{PV.}$ and q_A) and random values ($r_{V.}$ and $r_{PV.}$) in an ECDH based environment. Hence, ECC-EXONUM-eVOTING is harmless in case of transaction privacy linkage attack.

Liveness Attack

In the ECC-EXONUM-eVOTING scheme, this type of attack is prevented using ECDH-based operation, symmetric contributory keys (K_{cd}, $K_{VA,}$ K_{PV}) and session keys SK those are generated and used for further transactional communication among the participants along with public key certificates (CA_{cd}, $CA_{A,}CA_V$) those are generated maintaining proper PKI validation rule. After completion of candidate registration, a registration confirmation message $E_{K_{cd}}(CID_i \,||\, CD_i\_RCM)$ is forwarded to the candidate and for voter registration, a voter registration confirmation message $E_{K_{PV}}(H_{PV} \,||\, SK|| \, R_V \,||PV_i\_RCM\,)$ is also conveyed by the validator to voter and in every step, the time stamp ΔT is also validated within which all transactions are required to be completed. On the other hand, session key generation and validation times ($T_{SK_V,}$ $T_{SK_{PV}}$ and ΔT) are also maintained to restrict the liveness attack. Alternatively, in the voter authentication and vote-casting phase, a variable *count* is initiated to 0 and incremented for each unsuccessful transaction, and beyond the three unsuccessful transactions, the communication is terminated. So, all the transactions along with necessary delay procedures are restricted by the validator [37, 44]. Hence, ECC-EXONUM-eVOTING is harmless in case of a liveness attack.

DAO Attack

In ECC-EXONUM-eVOTING, the communication path is maintained by validators or auditors and in every step, a transaction is communicated using both ECDH-based operation, symmetric contributory keys (K_{cd}, $K_{VA,}$ K_{PV}) and session key SK those are generated and further used for communication among the participating entities along with public key certificates (CA_{cd}, $CA_{A,}CA_V$). On the other hand, both private blockchain and hybrid consensus algorithm ($RAFT$ and $PBFT$) are the most efficient mechanisms used to control forwarding those transactions to the root or any specific node by malicious nodes [37,39, 44]. Hence, ECC-EXONUM-eVOTING restricts the occurrence of DAO attack.

Sybil Attack

In ECC-EXONUM-eVOTING, blocks (BLK_i) are generated and maintained by validators only and further generate the blockchain after completion of proper validation procedures. Each block is generated using the anonymous identity H_{PV} and fingerprint (F_p) of the registered voter, public key certificate of the validator CA_V, identity CID_i and participating symbol C_i_Symbol of the registered candidate participating in the e-Voting process. So, the identity of the validator is also authenticated [37,40]. Further the recently generated BLK_i is appended to the existing blockchain and generates the whole blockchain by the validator only and forwards the entire blockchain to the auditor for validation purposes. The auditor validates each block of the blockchain and the identity of the validator using the public key certificate CA_V. So, all the entities are authenticated and authorized in the e-voting process. On the other hand, if Ã change the Blk_i_Time' and forwards the transaction $TS_i(Blk\_Chn_i \,||\, Blk_i\_Time')$ to auditor. However, at the time of validation, auditor will track the time stamp duration with current time $|T_{12} - Blk_i\_Time'| \leq \Delta T$ and it will differs. So, this scheme is capable of defending against this attack.

Eclipse Attack

In ECC-EXONUM-eVOTING, the attacker $\tilde{A}$ is not able to acquire the control of a participating node or entity in the e-Voting transactions to generate the unnecessary computing power for the blockchain network [37,44]. However, for protecting various transactional communications of ECC-EXONUM-eVOTING scheme, private blockchain, idemix technology, zero-knowledge property, blind signature scheme and anonymous identity of voter H_{PV} are utilized. On the other hand, every transaction is encrypted with either ECDH-based contributory symmetric keys K_{cd} , K_{PV} or contributory session key SK. The session key is also generated based on private keys ($q_{V.}$,$q_{PV.}$ and q_A) and random values ($r_{V.}$ and $r_{PV.}$) in an ECDH based environment. Hence, ECC-EXONUM-eVOTING is harmless in case of an Eclipse attack.

Phising Attack

In the ECC-EXONUM-eVOTING scheme, voters afford their relevant documentation to the validator guessing that the validator is dependable [44]. But after acquiring some influential credentials, any insider or the validator can perform as a challenger $\tilde{A}$. In this scenario, if all the sensitive information like H_{PV}, R_V and F_p are acquired by $\tilde{A}$, still s/he is incapable to endorse like a legitimate participant. Since H_{PV} or R_V is computed and further verified with the validator. Afterwards, contributory session keys $SK = q_{V..}.r_{V..}.r_{PV.}.q_{PV.}.q_{A.}..P$ is also generated based on private keys ($q_{V.}$,$q_{PV.}$ and q_A) and random values ($r_{V.}$ and $r_{PV.}$) in an ECDH based environment. Hence, ECC-EXONUM-eVOTING is harmless for phishing attack.

Replay Attack

In voter authentication and vote casting phase of ECC-EXONUM-eVOTING scheme, the transaction $E_{SK}(TS_i(H_{PV} \,||\, R_V \,||\, F_p||\, T_{SK_{PV}}))$ is corresponded to validator by the registered voter. If $\tilde{A}$ obtains the transaction, tries to reply it to the validator just altering the identity of H_{PV} *to* $H_{PV}{}^{x}$ and transmits the transaction that contains $E_{SK}(TS_i(H_{PV}{}^{x} \,||\, R_V \,||\, F_p||\, T_{SK_{PV}}))$. After obtaining the transaction, validator compares pre-computed H_{PV} with the received $H_{PV}{}^{x}$, which will not be same as the received $H_{PV}{}^{x}$ and each of the components of H_{PV}, R_{PV} and K_{PV} is computed using ECDH scheme. Hence, the session will be deactivated. However, it will work out the validation of the time stamp difference with current time $|T_9 - T_{SK_{PV}}| \leq \Delta T$ that will not be similar to the presumed ΔT. Therefore the validator concludes the session. Hence, it is very much capable of defending against such attack.

Impersonation Attack

At the time of communication, a contender $\tilde{A}$ may intercept the registration-related communication messages) and tries to amend those messages in such a way that it appears as if coming from a valid participant but with the substituted values either for public key certificates CA^x_{cd}, CA^x_V and CA^x_A or the replaced timestamp values T^x_1, T^x_2 or T^x_3 by $\tilde{A}$. However, either the public key certificates or the timestamps are validated by the validators or auditors at every step of the scheme. On the other hand, after receiving communication messages, each participant computes the contributory symmetric keys $K_{cd} = q_{cd..}.q_{V.}.P$ and $K_{VA} = q_{V..}.q_{A.}.P$ using ECDH. Further, using the symmetric keys, both the validator or participating voters computes the anonymous identity $H_{PV} = h\,(R_{PV} \,||\, K_{PV})$, where R_{PV} is calculated as R_{PV} $r_{PV.}.q_{PV.}.q_A\,.P$ and validates H_{PV} with the received transactions. On the other hand, K_{PV} is computed by the voter as $K_{PV} = q_{PV.}.Q_V$ or by the validator as $K_{PV} = q_{V.}.Q_{PV}$ using ECDH. Furthermore, any amendment like K_{PV} as K^x_{PV} or R_{PV} as R^x_{PV} is performed by $\tilde{A}$ for the computation of H_{PV}, and based on the unsuccessful validation, the transactions will be terminated. Hence, ECC-EXONUM-eVOTING is competent to resist this attack.

Known Session Specific Temporary Attack

To control the incidence of such attack for ECC-EXONUM-eVOTING, a contributory session key $SK = q_{V..}.r_{V..}.r_{PV.}.q_{PV.}.q_{A.}..P$ is used for communication between validator and participating voter at the time of voter authentication and vote casting phase. This key is generated based on private keys ($q_{V.}$,$q_{PV.}$ and q_A) and random values ($r_{V.}$ and $r_{PV.}$) in an ECDH based environment. Hence, the ECC-EXONUM-eVOTING scheme is exempt from known session-specific temporary attack.

Session Key Computation Attack

To swap over the information among the valid participants in the e-Voting process and accomplish the e-Voting related information securely, ECC-EXONUM-eVOTING is represented in a manner that it pursues a top-secret contributory session $SK = q_{V..}.r_{V..}.r_{PV.}.q_{PV.}.q_{A.}..P$. Due to hardness of ECDH, this scheme is suggested for session key computation and ECC-EXONUM-eVOTING is very much defended and rigid to reconciliation. Alternatively, using three private keys (from voter, validator and auditor) and two random numbers (from both the voter and validator), session key SK is computed. So, the contender $\tilde{A}$ is unable to negotiate the inflexible key in polynomial time although any one of the secret components is uncovered to $\tilde{A}$. Hence, ECC-EXONUM-eVOTING is very much feasible to put off the session key for such an attack.

Efficient Mutual Authentication

A shared verification approach among candidates, voters, validators, and auditors has been proposed for the ECC-EXONUM-eVOTING scheme based on secret proposals mutually contributed among them. For candidate registration process, a registration request is forwarded and encrypted as a transaction $E_{K_{cd}}(CID_i|| \; C_i\_Symbol \,||\, C_i\_Mob \,||\, CA_{cd} \,||T_1\,)$ to validator. Based on the received transactions, validator further forwards the same to the auditor. Later, auditor generates a valid candidate list CL_i and conveys to the validator as an encrypted transaction $E_{K_{VA}}(CL_i \,||\, CA_A \,||\, T_3)$. Later, the validator forwards a registration confirmation message to the valid candidate $E_{K_{cd}}(CID_i \,||\, CD_i\_RCM)$ in an encrypted format. Using the same procedure, participating voter also transmits his/her registration request with anonymous identity H_{PV} and fingerprint (F_p) to validator that is further forwarded to auditor with additional inclusion of CA_V and successively auditor forwards a valid voter list VL_i along with CA_A to validator. After receiving this transaction, the validator further transmits a registration confirmation message to the valid voter and completes the registration. Using a proper validation methodology, a secure transaction is performed between the voter and auditor in addition to a contributory session key SK for authentication and secure voting purposes. Further, based on the received votes of the anonymous voter, a blockchain is generated and forwarded to the auditor for counting and announcement of results. Hence, from the aforesaid communications, secure

and mutual transactional communication is performed among the participants.

Non-repudiation

Using non-repudiation, a sender or any participants may oppose driving a transaction to the recipient. But in the ECC-EXONUM-eVOTING scheme, the candidate forwards their registration request as an encrypted transaction using $E_{K_{cd}}$ to the validator that contains the candidate's identity and public key certificate of the candidate. Further, the transaction is forwarded by the validator to the auditor with the additional inclusion of a public key certificate of the validator C_{AV} as encrypted format using $E_{K_{VA}}$. On the other hand, auditor also generates a valid candidate list C_{Li} and sends the encrypted message to validator $E_{K_{VA}}(C_{Li} \mid\mid C_{A_A} \mid\mid T_3)$ together with public key certificate of validator C_{A_A}. Using similar registration procedure, voters also send their registration request $E_{K_{PV}}(H_{PV} \mid\mid R_{PV} \mid\mid F_{F_p} \mid\mid T_5)$ to validator along with anonymous identity H_{PV} and biometric fingerprint F_p information. So, participation by each peer in the e-voting process, cannot be denied regarding the performing of e-voting transactions by relevant participants due to proper authentication and validation mechanisms maintained using their identities. Hence, this scheme encompasses non-repudiation.

Perfect Forward Secrecy

In ECC-EXONUM-eVOTING, if symmetric contributory keys K_{cd} or K_{PV} or contributory session key SK are exposed to any adversary, still s/he cannot compromise the whole e-voting process. The session key is also generated based on private keys ($q_{V.}$,$q_{PV.}$ and q_A) as well as random values ($r_{V.}$ and $r_{PV.}$) and contributory symmetric keys are also generated using confidential private keys. Hence, ECC-EXONUM-eVOTING defends against the effects of perfect forward secrecy.

Untraceability

A condition is considered where an antagonist $\tilde{A}$ can infer several transactions those enclose $E_{K_{PV}}(H_{PV} \mid\mid R_{PV} \mid\mid F_p \mid\mid T_5)$, $E_{K_{VA}}(H_{PV} \mid\mid R_{PV} \mid\mid F_p \mid\mid V_1 \mid\mid CA_V \mid\mid T_6)$ and $E_{K_{VA}}(H_{PV} \mid\mid VL_i \mid\mid V_1 \mid\mid CA_A \mid\mid T_7)$ in a vulnerable channel. As those communications are encrypted by the contributory symmetric keys $E_{K_{PV}}$ and $E_{K_{VA}}$ generated by means of ECDH, so it is impossible by $\tilde{A}$ to decrypt those communications. Alternatively, if the adversary $\tilde{A}$ somehow estimates the random message (R_{PV}), still s/he cannot get the anonymous identity of the voter H_{PV} that is computed using ECDH. Moreover, in any situation, $\tilde{A}$ somehow acquires the information details of K_{PV}, still s/he cannot be able to estimate the identity of the voter due to use of hashed information that is irreversible. Therefore, it is not possible to break the security due utilization of the pre-image resistance property of the hash function. Moreover, from those transactions $E_{SK}(TS_i(H_{PV} \mid\mid R_V \mid\mid F_p \mid\mid T_{SK_{PV}}))$ and $E_{SK}(TS_i(CL_i \mid\mid CID_i \mid\mid V_2 \mid\mid T_{SK_V}))$, if $\tilde{A}$ desires to deduce the identity and participating symbols of a candidate, still the adversary has to compute the contributory session key SK to decrypt those transactions. However, SK is also generated based on private keys ($q_{V.}$,$q_{PV.}$ and q_A) and random values ($r_{V.}$ and $r_{PV.}$). So, due use of ECDH, it is impossible to crack the key due to its robustness. Hence, ECC-EXONUM-eVOTING restricts such property.

Unlinkability

Using the voter authentication and vote casting phase, voter forwards an encrypted transaction to validator exploiting the transaction $E_{SK}(TS_i(H_{PV} \mid\mid R_V \mid\mid F_p \mid\mid T_{SK_{PV}}))$ Suppose, the voter forwards the same to validator using two transactions- $E_{SK}(TS_i(H^x_{PV} \mid\mid R^x_V \mid\mid F^x_P \mid\mid T^x_{SK_{PV}}))$ in session x and $E_{SK}(TS_i(H^y_{PV} \mid\mid R^y_V \mid\mid F^y_P \mid\mid T^y_{SK_{PV}}))$ in session y. However, in this case, the voter exercises two dissimilar assessments of the anonymous identity and random messages R_V of the voter H_{PV} in e-Voting process, H^x_{PV} and R^x_V in session x as well as H^y_{PV} and R^y_V in session y. But based on the birth day attack, likelihood of the two transactions $E_{SK}(TS_i(H^x_{PV} \mid\mid R^x_V \mid\mid F^x_P \mid\mid T^x_{SK_{PV}})) = E_{SK}(TS_i(H^y_{PV} \mid\mid R^y_V \mid\mid F^y_P \mid\mid T^y_{SK_{PV}}))$ is insignificant as $H^x_{PV} \neq H^y_{PV}$, $R^x_V \neq R^y_V$ and $T^x_{SK_{PV}} \neq T^y_{SK_{PV}}$. Likewise, validator also forwards two unlike transactions $E_{SK}(TS_i(CL^x_i \mid\mid CID^x_i \mid\mid V^x_2 \mid\mid T^x_{SK_V}))$ and $E_{SK}(TS_i(CL^y_i \mid\mid CID^y_i \mid\mid V^y_2 \mid\mid T^y_{SK_V}))$ to voter in two diverse sessions, in session x and y correspondingly and also holds an irrelevant possibility regarding both the transactions are equivalent. Hence, ECC-EXONUM-eVOTING restricts such property.

Information Leakage

$\mathcal{A}$ can interpret the transactions as discussed in initiation protocol those are exchanged in an insecure channel. However, all those transactions are encrypted using symmetric keys $E_{K_{cd}}$, $E_{K_{PV}}$ and $E_{K_{VA}}$ generated using ECDH. Most of those transactions used random values (R_{PV}, R_V) and created using ECDH. So, an attacker cannot gather sensitive information from those transactions. On the other hand, contributory session keys SK are used for communication between validator and participating voter for several e-Voting transactions and generated based on private keys ($q_{V.}$,$q_{PV.}$ and q_A) and random values ($r_{V.}$ and $r_{PV.}$) in an ECDH based circumstances. So it is unfeasible to evaluate due to the robustness of ECDH.

The above subsections, and security of the proposed ECC-EXONUM-eVOTING protocol are formally and informally analyzed. The formal analysis shows that the advantage of breaking the semantic security of this scheme in polynomial time is negligible. Additionally, the informal security analysis using a mathematical model demonstrates that the scheme resists all the known security threats.

V. Simulation of ECC-EXONUM-eVOTING

In this section, two different well-known simulation tools are used – i) AVISPA *(Automated Verification Internet Security Protocol and Applications)* and ii) Scyther. Both simulation tools are utilized for formal security verification of ECC-EXONUM-eVOTING to establish that the proposed protocol is safe against cryptographic attacks.

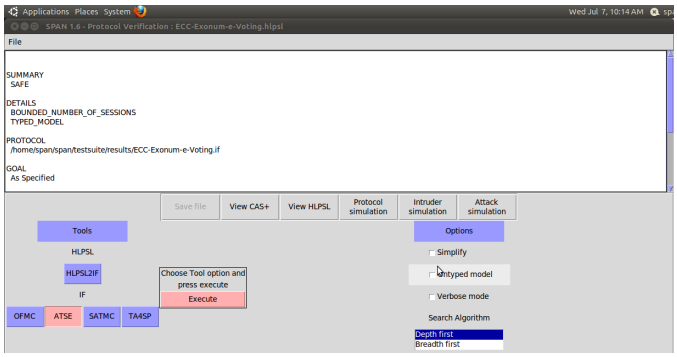

FIGURE 8. Result of AVISPA Simulation for Cl-AtSe Backend

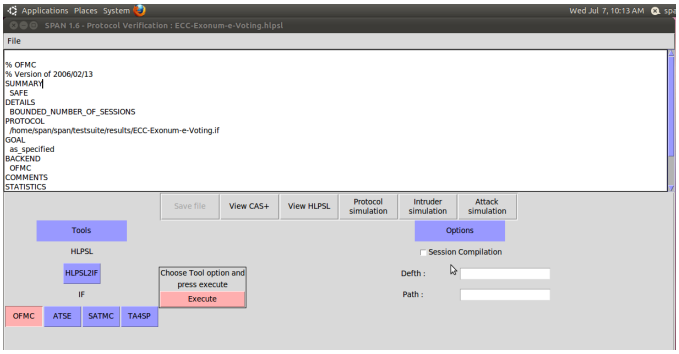

FIGURE 9. Result of AVISPA Simulation for OFMC Backend

A. Simulation Result Analysis using AVISPA

The simulation result of AVISPA simulation shown in Figures 8 and 9 under OFMC and Cl-AtSe backend is given in generates the output as 'SAFE' that denotes that all the roles are verified successfully and the protocol is well protected against all recent potential security threats and preserves necessary security goals according to AVISPA simulator. A detailed description of all the roles is given in appendix 2.

B. Simulation Result Analysis using Scyther

To display the result in 'Result window', using Scyther tool, it generates the outcomes either in 'Ok' or 'Fail' [35,36]. In our Syther simulation, the result window displays the output as "Ok" which denotes that the roles are verified successfully and resist all the active and passive attacks as depicted in Figure 10. A detailed description of Scyther is given in Appendix 2.

From the above discussion, it is concluded that the ECC-EXONUM-eVOTING protocol is well protected in e-voting applications.

VI. PERFORMANCE ANALYSIS OF THE PROPOSED SCHEME

Based on numerous earliest metrics like communication overhead, computation overhead, number of communicated messages for different transactions in e-Voting, security strength, and storage overhead are the on the whole appearance of ECC-EXONUM-eVOTING. Those metrics are

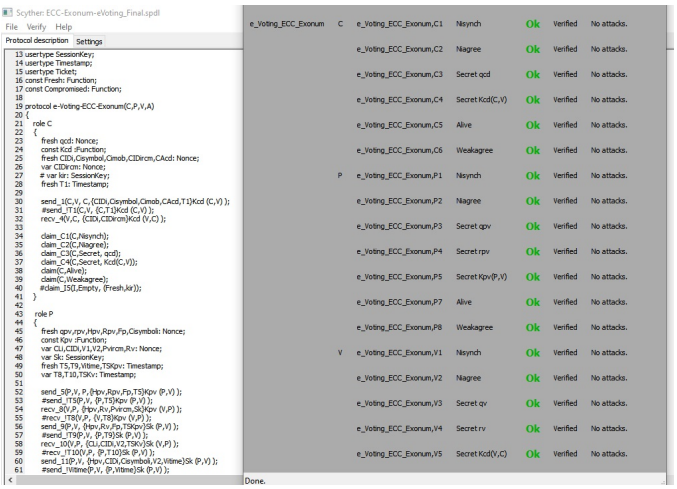

FIGURE 10. Result of Scyther simulation for description file (.spdl)

further verified within this segment using two different background working systems for diverse platforms- i) Intel (R) Core (TM) i-3- 5015U CPU, 4.00 GB of RAM, 2.10 GHz processor and Windows 10 and 64-bit operating system and ii) Intel Pentium Dual CPU E2200, 2048 MB of RAM, 2.20 GHz processor and Ubuntu 17.04.1 LTS 32 bit operating system to execute the protocol. On the other hand, for the successful installation of Scyther V1.1.3 version and proper functioning, some more additional software is required to be installed- Python 2.7.18 (64 bit), wxPython 2.8.12.1 for Python 2.7 and Graphviz. ECC-EXONUM-eVOTING is a novel scheme as still there is no existing work on ECC-based e-Voting applications using Exonum private blockchain. So, the whole voting process of ECC-EXONUM-eVOTING is compared with two recently proposed similar schemes -Waheed et al. [15] and Zaghloul et al. [24] scheme to evaluate the performance. The computations of different cryptographic operations are T_{ECPM} = *2.226 ms,* $T_{E/D(S)}$ = *3.85 ms*, T_h= *0.0046 ms,* T_{ECPA}= *0.0288 ms*, T_{EMod} = *3.85 ms* and T_{HMAC} = *0.0046 ms* where i) timing notation used for cryptographic hash operation- T_h , ii) timing notation used for encryption/decryption with symmetric key- $T_{E/D(S)}$, iii) timing notation used for elliptic curve point multiplication- T_{ECPM} , iv) timing notation used for elliptic curve point addition- T_{ECPA}, v) timing notation used for modular exponential operation- T_{EMod} and vi) timing notation used related to Fuzzy extractor operation for biometric information- T_F.

Among different participants of e-voting system, the communication overhead depends on the total number of bits transmitted during the exchange of information among the entities considering the number of transactions communicated and the network blockage that situation of the e-voting process. In ECC-EXONUM-eVOTING, different entities are taken in consideration like number of bits required for transaction such as time stamps (T_{SK_V}, $T_{SK_{PV}}$, T_9, T_{10}, V_i *_Time,*Blk_i *_Time,* T_{12}, $Rslt_i$ *_Time)* are extorted as

TABLE 3. Comparison Of Security Robustness

Security Feature	[12]	[15]	[17]	[24]	Proposed Scheme
MIMT attack	✓	×	✓	×	✓
DoS attack	✓	✓	✓	✓	✓
DDoS attack	✓	✓	✓	✓	✓
51% and 34 % attack	×	×	✓	×	✓
Double voting problem	✓	✓	✓	×	✓
Private key related security attack	✓	✓	✓	✓	✓
Insider Attack	✓	✓	✓	✓	✓
Transaction privacy linkage attack	×	×		×	✓
Liveness attack	✓	×	✓	×	✓
DAO attack	×	×	×	×	✓
Sybil attack	×	✓	✓	×	✓
Eclipse attack	×	×	×	×	✓
Resists Replay attack	✓	✓	✓	✓	✓
Impersonation attack	✓	✓	✓	×	✓
Known session-specific temporary attack	×	×	×	×	✓
Session key computation attack	×	×	×	×	✓
Efficient mutual authentication attack	✓	✓	✓	✓	✓
Non- repudiation	✓	✓	✓		✓
Perfect forward secrecy	×		×	×	✓
Untraceability	✓	✓	✓	✓	✓
Unlinkability	×	✓	✓	×	✓
Information leakage	✓	✓	✓	✓	✓
Phishing attack	✓	✓	✓	×	✓

TABLE 4. Comparison Of Computation Overhead

Schemes	Overheads	Execution Time (ms)
ECC-EXONUM-eVOTING	$\boldsymbol{4\,T_h + 6T_{ECPM} + 4T_{E/D(S)} + 6\,T_{EMod} + 2T_{FP}}$	**56.3264**
Neloy et al. [17]	$16\,T_h + 16T_{E/D(S)} + 2T_{Ran}$	63.7084
Waheed et al. [15]	$4T_h + 10T_{ECPM} + 4T_{E/D(S)} + 7\,T_{EMod}$	62.5944
Zaghloul et.al. [24]	$24T_{EMod} + 1T_{ECPM} + 6T_{E/D(S)} + 6T_{E/D(S)} + 6T_{Ran}$	120.9600

TABLE 5. Comparison Of Communication Overhead

Schemes	Communication Cost (bits)	Number of message communication
Proposed	**1760 bits**	**5 messages**
Neloy et al. [17]	1920 bits	10 messages
Waheed et al. [15]	1984 bits	4 messages
Zaghloul et al. [24]	2432 bits	6 messages

32 bits, identities of the participating entities (CID_i and H_{PVi}) are regarded as 64 bits, contributory symmetric or session keys (K_{VA}, K_{PV} and SK) are considered as 160 bits, different random messages or values (R_V and RP_V) are taken as 128 bits [30, 45,46] and Pseudo Random Number Generators ($PRNG$) are considered as 128 bits [19]. The comparison of computation overheads, communication overheads, and security features with other related schemes are demonstrated in Table4, Table5, and Table3 respectively.

VII. Conclusion

A novel ECC-based secure e-Voting protocol is proposed using Exonum private permission blockchain, hybrid consensus mechanism (PBFT and RAFT), idemix technology, zero-knowledge property, and blind signature scheme for secure voting transactions among different participants. In the ECC-EXONUM-eVOTING scheme, anonymous identity is utilized for the participating voters to preserve the confidentiality and integrity of the votes. The proposed scheme also follows the Exonum private blockchain applications where lightweight decentralized communication is established using Dapp. To validate the robustness, ECC-EXONUM-eVOTING is evaluated using mathematical models against significant cryptographic attacks. Additionally, using well-recognized AVISPA as well as Scyther simulation tools and the Random Oracle Model, the proposed scheme is formally assessed and found well secure. The performance analysis demonstrates that ECC-EXONUM-eVOTING is efficient for lightweight decentralized applications for private blockchain in terms of computation and communication overheads. Moreover, our scheme also works on a novel e-voting scheme.

In the future, we will consider and implement an advanced scheme using a verifiable data registry mechanism basically on the Hyperledger platform to reduce the distribution and maintenance overheads of certificates and generation, as well as maintenance of dynamic digital identities for each participant and verifier for anonymity and tracking purposes, and secure communication with DLT.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", *bitcoin.org*, 2008. *URL: https://bitcoin. org/bitcoin. pdf.*

[2] R. Casado-Vara and J.M. CoRCHaDo, "Blockchain for democratic voting: How blockchain could cast of voter fraud", *Oriental journal of computer science and technology*, Vol. 11, No. 03, 2018.

[3] T.A. Syed, A. Alzahrani, S. Jan, M.S. Siddiqui, A. Nadeem, and T. Alghamdi, "A comparative analysis of blockchain architecture and its applications", *Problems and recommendations, IEEE access*, Vol. 7, pp.176838-176869, *IEEE*, 2019.

[4] H.R. Hasan, K. Salah, R. Jayaraman, I. Yaqoob, M. Omar, and S. Ellahham, "COVID-19 Contact Tracing using Blockchain", *IEEE Access*, Vol. 9, pp.62956-62971, *IEEE*, 2021.

[5] I. Kotsiuba, A. Velvkzhanin, Y. Yanovich, I.S. Bandurova, Y. Dyachenko, and V. Zhygulin, "Decentralized e-Health architecture for boosting healthcare analytics", *in 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), IEEE*, 2018, pp. 113-118.

[6] Y. Yanovich, I. Ivashchenko, A. Ostrovsky, A. Shevchenko, and A. Sidorov, "Exonum: Byzantine fault tolerant protocol for blockchains", *bitfury. com*, pp.1-36, 2018.

[7] O. Anyshchenko, I. Bohuslavskyi, S. Kruglik, Y. Madhwal, A. Ostrovsky, and Y. Yanovich, "Building cryptotokens based on permissioned blockchain framework", in *Proceedings of 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, *IEEE*, 2019, pp. 1-5.

[8] R. Krishnamurthy, G. Rathee, and N. Jaglan, "An enhanced security mechanism through blockchain for E-polling/counting process using IoT devices", *Wireless Networks*, *Springer*, 2019.

[9] P. M. Dhulavvagol, V. H. Bhajantri, and S. G. Totad, "Blockchain Ethereum clients performance analysis considering e-voting application", Vol. 167, *Procedia Computer Science*, *Elsevier*, pp.2506-2515, 2020.

[10] K. Sadia, M. Masuduzzaman, R.K. Paul, and A. Islam, "Blockchain-based secure e-voting with the assistance of smart contract", in *Proceedings of IC-BCT 2019*, *Springer, Singapore*, 2020, pp. 161-176.

[11] A. Shah, N. Sodhia, S. Saha, S. Banerjee, and M. Chavan, "Blockchain Enabled Online-Voting System", *in Proceedings of ITM Web of Conferences, EDP Sciences,* Vol. 32, p. 03018, 2020.

[12] C.H. Roh, and I.Y. Lee, "A study on electronic voting system using private blockchain", *Journal of Information Processing Systems", Wiley*, Vol.16, No. 2, pp.421-434, 2020.

[13] S. Majumder, and S. Ray, "Usage of Blockchain Technology in e-Voting System Using Private Blockchain", *in Proceedings of Intelligent Data Engineering and Analytics, Springer*, 2022, pp. 51-61 .

[14] N. Jain, P. Upadhyay, P. Arora, and P. Chaurasia, "MATDAAN: A SECURE VOTING SYSTEM USING BLOCKCHAIN*", International Research Journal of Modernization in Engineering Technology and Science*, Vol. 03, 2021.

[15] A. Waheed, N. Din, A.I. Umar, R. Ullah, and U. Amin, "Novel blind signcryption scheme for e-voting system based on elliptic curves", *Mehran University Research Journal of Engineering & Technology*, Vol. 40, No.2, pp.314-322, 2021.

[16] Jumaa, M.H. and Shakir, A.C.,"Iraqi E-Voting System Based on Smart Contractusing Private Blockchain Technology", *International Journal of Computing and Informatics*, *Informatica,* Vol.46, No.6, 2022.

[17] M. N. Neloy, M. A. Wahab, S. Wasif, A. All Noman, M. Rahaman, T .H. Pranto, A.B. Haque, and R.M. Rahman, "A remote and cost-optimized voting system using blockchain and smart contract." *IET Blockchain, Wiley*, Vol.3, Issue 1, pp. 1-17, 2023.

[18] J. Camenisch, and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps*", in Annual international cryptology conference*, *Springer,* Berlin, Heidelberg, August, 2004, pp. 56-72.

[19] S. Sundaresan, R. Doss, and W. Zhou, "Zero knowledge grouping proof protocol for RFID EPC C1G2 tags", *IEEE Transactions on Computers*, *IEEE,* Vol.64, No.10, pp.2994-3008, 2015.

[20] H. Rui, L. Huan, H. Yang, and Z. Y. Hao, " Research on secure transmission and storage of energy IoT information based on Blockchain",*Peer-to-Peer Networking and Applications, Springer*, Vol.13, No.4, pp.1225-1235, 2020.

[21] K.L.S. Priya, and C. Rupa, "Blockchain Technology based Electoral Franchis*", in Proceedings of* 2^{nd} *International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), IEEE*, pp. 1-5, 2020.

[22] M.K. Mustafa, and S. Waheed, "An E-Voting Framework with Enterprise Blockchain", *in Proceedings of ICADCML: In Advances in Distributed Computing and Machine Learning", Springer*, pp. 135-145, 2021.

[23] S.V. Shinge, and U. Shrawankar. "An Efficient Technique for Improving Trust and Privacy in Blockchain as a Service (BaaS)." *in Proceedings of IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, *IEEE*, 2023, pp. 1-4.

[24] E. Zaghloul, T. Li, and J. Ren, "d-BAME: Distributed Blockchain-based Anonymous Mobile Electronic Voting", *IEEE Internet of Things Journal, IEEE,* 2021.

[25] D. Dolev, and A. Yao, "On the security of public key protocols", *IEEE Transactions on information theory*, *IEEE*, Vol.29, No.2, pp.198-208, 1983.

[26] R. Canetti, and H. Krawczyk, "Universally composable notions of key exchange and secure channels", *in International Conference on the Theory and Applications of Cryptographic Techniques*, *Springer, Berlin, Heidelberg*, 2002, pp. 337-351.

[27] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology", *revisited, Journal of the ACM (JACM),* Vol. 51 No.4, pp.557-594, 2004.

[28] J. Lee, S. Yu, M. Kim, Y. Park, and A.K. Das, "On the design of secure and efficient three-factor authentication protocol using honey list for wireless sensor networks", *IEEE Access, IEEE,* Vol.8, pp.107046-107062, 2020.

[29] S. Banerjee, V. Odelu, A. K. Das, J. Srinivas, N. Kumar, S. Chattopadhyay, and K.K.R. Choo, "A provably secure and lightweight anonymous user authenticated session key exchange scheme for internet of things deployment", *IEEE Internet of Things Journal, IEEE*, Vol. 6, No.5, pp.8739-8752, 2019.

[30] S. Majumder, S. Ray, S., D. Sadhukhan, M.K. Khan, and M. Dasgupta, "Ecc-coap: Elliptic curve cryptography based constraint application protocol for internet of things*", Wireless Personal Communications, Springer*, Vol.11, No.3, pp.1867-1896, 2021.

[31] S. Ray, and G.P. Biswas, "Design of mobile public key infrastructure (M-PKI) using elliptic curve cryptography", *International Journal on Cryptography and Information Security (IJCIS)*, Vol. 3, No.1, pp.25-37, 2013.

[32] Z. Chen, L. Xianhui, J. Dingding , and L. Bao, "Ind-cca security of kyber in the quantum random oracle model, revisited*." in Proceedings of International Conference on Information Security &Cryptology*, *Springer*, 2023. pp.148-166.

[33] S. Challa, A.K. Das, V. Odelu, N. Kumar, S. Kumari, M.K. Khan, and A.V. Vasilakos, "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks", *Computers & Electrical Engineering, Elsevier*, Vol. 69, pp.534-554, 2018.

[34] S. Majumder, S. Ray, D. Sadhukhan, M.K. Khan, and M. Dasgupta, "Esotp: ECC-based secure object tracking protocol for IoT communication", *International Journal of Communication Systems, Wiley,* Vol. 35, No.3, e5026, 2022.

[35] C. Cremers, "Scyther. Semantics and Verification of Security Protocols*", Thesis, University Press Eindhoven,* 2006.

[36] C. J. Cremers, "The Scyther Tool: Verification, falsification, and analysis of security protocols", *in Proceedings of International conference on computer aided verification, Springer,* 2008, pp. 414-418.

[37] S. Singh, A.S. Hosen, and B. Yoon, "Blockchain security attacks, challenges, and solutions for the future distributed iot network", *IEEE Access, IEEE*, Vol. 9, pp.13938-13959, 2021.

[38] S. Sayeed, and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack", *Applied Sciences, Multidisciplinary Digital Publishing Institute (MDPI)*, Vol. 9, No.9, p.1788, 2019.

[39] B. Ghaleb, A. Al-Dubai, E. Ekonomou, M. Qasem, I. Romdhani, and L. Mackenzie, "Addressing the DAO insider attack in RPL's Internet of Things networks", *IEEE Communications Letters*, *IEEE*, Vol.23, No.1, pp. 68-71, 2019.

[40] M. Iqbal, and R. Matulevičius, " Exploring Sybil and Double-Spending Risks in Blockchain Systems", *IEEE Access*, *IEEE*, Vol. 9, pp.76153-76177, 2021.

[41] M.R. Amin, "51% ATTACKS ON BLOCKCHAIN: A SOLUTION ARCHITECTURE FOR BLOCKCHAIN TO SECURE IOT WITH PROOF OF WORK", *Thesis, IUBAT (BCSE) International University of Business Agriculture and Technology*, 2020.

[42] Z. Wang, H. Jin, W. Dai, K.K.R. Choo, and D. Zou, "Ethereum smart contract security research: survey and future research opportunities", *Frontiers of Computer Science, Springer,* Vol. 15, No. 2, pp.1-18,2021.

[43] D. Rathore, and V. Ranga, "Secure Remote E-Voting using Blockchain", *in Proceedings of* 5^{th} *International Conference on Intelligent Computing and Control Systems (ICICCS), IEEE*, 2021, pp. 282-287.

[44] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems", *Future Generation Computer Systems, Elsevier*, Vol. 107, pp.841-853, 2020.

[45] H. H. Kilinc, and T. Yanik, "A survey of SIP authentication and key agreement schemes", *IEEE Communications Surveys & Tutorials, IEEE,* Vol.16, No.2, ,pp.1005-1023, 2013.

[46] D. Sadhukhan, S. Ray, M. Dasgupta, and J.J. Rodrigues, "claacs-iod: Certificate-embedded lightweight authentication and access control scheme for Internet of Drones", *Software: Practice and Experience, Wiley,* Volume 53, Issue 4, 2023.