International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/211629 Volume 9, Issue 1, January – February (2022)

RESEARCH ARTICLE

Blockchain Powered Mutual Authentication and Access Control Protocol

Geeta Kakarla
Department of Computer Science and Engineering, Sreenidhi Institute of Science and Technology, GITAM (Deemed To Be University), Hyderabad, Telangana, India
geetavemula333@gmail.com

S. Phani Kumar
Department of Computer Science and Engineering, GITAM (Deemed To Be University), Hyderabad, Telangana, India
phanikumar.s@gmail.com

Received: 16 December 2021 / Revised: 17 January 2022 / Accepted: 01 February 2022 / Published: 28 February 2022

Abstract – With the advancement in the network connectivity, services can be subscribed for limited period of time. Subscribing for certain services is always an economic option rather than owning them. Implementing adequate procedures in the establishments, meeting the access control policies is challenging. Although the essential procedures are implemented using the centralized scheme where the single central server cater to the access control requests and the authorization mechanisms with the help of the stored identifiable attributes of the workstations in the web. In our article, we are proposing a blockchain powered lightweight, decentralized and secure framework for mutually authenticating the participating entities and levy the access control model among them. In our protocol, the device administrators (DA) can maintain their signed device policies for any of its services in the blockchain network which increases its visibility to more subscribers and at the same time, DAs can get rid of tedious job of authenticating each and every user/subscriber. On the other hand, users can also come to know about the wide range of services provided by different service providers and can avail appropriate service with the optimal constraints. We used elliptic curve cryptography (ECC) to transmit the secret sign parameters which makes our protocol lightweight. Secret sign parameters are used to verify the signature of any entity at the other end.

Index Terms – Blockchain, Mutual Authentication, Elliptic Curve Cryptography, Access Control, Digital Signatures, Confidentiality, Integrity.

1. INTRODUCTION

With high usage of the Internet of Things (IoT) technology and its assimilation in the various applications for offering the qualitative services to the mankind has brought in the wide range of challenges [1]. Prominent among them remain the security aspect which can be catastrophic if not handled in the appropriate manner. In October 2016, the Dyn service provider had faced the Mirai Botnet attack which is confirmed as the largest ever launched DDoS attack. The vulnerabilities in the IoT devices must be plugged meticulously with the state of the art security mechanisms which are light-weight and robust to counter the attacks. The threats on the IoT devices can be classified as arising internally from the networked other devices in the premises or staged by an external entity. The first step towards implementing the security procedure is to institute the authentication mechanism among the interconnected devices to establish the certified exchange of information. The identity of the participating entity in the communication must be established before initiating the information transmission.

The popular mechanism used in the authentication models used earlier is based on the Public Key Cryptosystem (PKC) which needs a principal authority to determine the mutual authentication of the communicating parties. The trustworthiness and deterrence of the central server is a matter of concern owing to the breaches and sophisticated attacks staged. In our paper, blockchain administrator (BCA) is the liable entity which initiates and records each and every transaction carried out with it. The Blockchain is working on the principle of distributed and decentralized ledger [2] among a set of interconnected nodes. The data stored in the form of transactions in the ledger among the computing machines are immutable in nature and offer a range of desirable features [3]. Data remains at the helm of the blockchain network which is accessible by any party in the most trustworthy environment.

The promising features of the blockchain network are immutable nature of the data stored, verifiability of the records, data security, effective expansion and operational management of the stored data thus paving way for the effective interoperable information systems. The scenarios which demand information exchange among the differently

RESEARCH ARTICLE

configured networks and involving different players accessing and updating the data are in greater need of the mutual trustworthy environment to rely on. Health-care ecosystem, financial institutions, logistics, legal enforcements and likewise are few such scenarios for the introduction of the blockchain networks. Health-care ecosystem can tap the potential of the blockchain powered IoT system in various ways. A mobile recommender system is suggested in the [4] which offer more appropriate routes to the people having chronic health conditions. Zhenget.et al. [5] discussed several challenges and opportunities the blockchain can offer other than crypto currencies. The blockchain provide a trustworthy system [6] in which the nodes can store, access, transfer and update the data securely with no conflicts.

The consensus algorithm play a pivotal role in updating the transacted records unlike the conventional databases which manage the susceptible data centrally and individually using applications. Blockchain is an innovative design for digitizing official documents/policies which must be agreed upon by all the parties involved in any official transactions. In our paper, we are assigning the responsibility of authentication and access control to the blockchain administrator (BCA). BCA accepts the signed device policies from DAs for their services. After verifying digital signatures, BCA uploads all device policies to the blockchain. BCA also makes sure; whatever user wants to use the service must agree and sign the device policy of the device given by DA earlier. After verifying user's request, BCA disseminate the tokens to both DA and the user. When the user presents the token, DA allows the user to use the service for some stipulated time. Here the DAs need not authenticates each and every user and the tedious and complex task of record keeping of all the transactions are reduced up to great extent.

Blockchain technology conceptually describe chain of blocks, with each block holding a finite set of transactional records similar as conventional public ledger [7] and demonstrating the following key features enlisted here under:

- Persistent Data Availability: The transactional data stored in the form of records can be validated and availed quickly by the stakeholders. Using the concepts of proof of stake (PoS) or proof of work (PoW), or other related mechanisms, the miners compute hash value and validate the data prior to storing in the blocks and disallow the invalidated data. The data updating and/or deletion is strictly followed on executing the consensus algorithm among the participating stakeholders, given the basic feature of the blockchain of its immutable nature. The consistent availability of the data proves to be one of the desirable features.
- Decentralized Data Management. Unlike in the conventional information systems, where data is validated by the centrally staged trusted agency, data in the blockchain is managed in the decentralized format. The conventional data management systems, like centralized financial institutions, give rise to the cost and performance bottlenecks as the entire responsibility of validating the data lies with the central server. Improvement of such bottlenecks can be attained by introducing the third party agencies, albeit leaving the system vulnerable owing to its cost and security facets. In contrary, the introduction of the blockchain technology along with consensus algorithms in place provide much needed decentralization feature as well as reinstating the trust among the data owners and the users.
- Anonymous User's Identity. The users partaking into the blockchain network can avail the services of storing and accessing the data without revealing their real identity. The users access the data with the help of the identity address in the form the public key. Moreover, transactions being easily verifiable and traceable provide effective data maintenance.

In this paper, we are using the elliptic curve cryptography to convey the secret sign parameter used for verification purpose as well as for disseminating tokens to both user and the DAs. When user presents the token, DA verifies the token and allows the user to avail its services. [8], [9] Koblitz and Miller introduced Elliptic curve cryptography, in 1980s, Diffie-Hellman key exchange[10] and ElGamal signature was introduced as an efficient replacement for cryptographic mechanisms which uses discrete logarithmic problem in the finite fields. One of the public key cryptosystems is the Elliptic Curve Cryptography, which works efficiently with much smaller key sizes than RSA. ECC provides similar level of security with 163 bit key size as compared to RSA which uses 1024 bit key size. ECC keys are based on elliptic curve equations and not on large prime numbers.

ECC is based on the equation created from the elliptic curve and a mathematical group. If a point resides on the elliptic curve and of the mathematical group, then multiplying it with any random value gives other point on the curve and also the part of the same mathematical group. Even though the initial point and resultant point is known, it is nearly impossible to find the random value with which it was multiplied [12]. Because of its smaller key size, ECC is widely used for securing mobile applications. The basic ECC is followed by "The Elliptic Curve Digital Signature Algorithm" and "Key Agreement and Key Transport Using Elliptic Curve Cryptography". Several mobile manufacturers incorporated ECC into their products to make them safe and secure against latest cyber-attacks. The "Standards for Efficient Cryptography" [13] has also documented the standards used in ECC.

Our next sections are ordered in the following manner: in Section 2, the related works pertaining to the authentication

RESEARCH ARTICLE

protocols are described. In Section 3, the network architecture is presented and in Section 4, a detailed description of the proposed protocol for mutually authenticating the stakeholders and access control policies are made. In Section 5 and 6, security analysis is demonstrated using both, the BAN logic as well as AVISPA tool to prove the verifiability and strength of the protocol, in section 7, informal security analysis and finally made conclusions with future Scope in Section 8.

2. RELATED WORKS

The blockchain was primarily developed with intent of generating the crypto-currencies, aka bitcoin. With the development of the technology over the time, the blockchain is sought-after in the applications where there is a need of reinstating the cost-effective and trust-worthy system which is capable of storing transactional records of the parties [14]. Few of the illustrative scenarios are mentioned above for reference. Many industries like power-grid, educational, government disbursement systems and real estate, medium and large, are studying and adopting the blockchain technology thus providing an alternative authentication model. Besides this, the security features of anonymity and immutability offer a sought after technology.

In [15], the authors proposed a framework involving blockchain and access regulator features for the IoT architecture but the same protocol is not efficient if the data is stored in cloud or in the network system. Decentralized Docker Trust (DDT) solution is detailed in the [16] which is a solution based on blockchain. The mechanism used in DDT gives signature validation and verification services for docker images and greatly minimizes the risks involved in the DoS attacks. However, since this is completely based on decentralized system, it is difficult to maintain and manage. In [17], a new model is proposed for efficiently mitigating the DDoS attacks across multiple domains using blockchain and smart contracts. But this scheme can only block the traffic coming from static IPs and hence cannot handle the attacks posing from the advanced systems capable of generating dynamic IPs.

In [18],the blockchain acts as an automatic access control manager for managing the personal data in the decentralized way and ensuring that owners of the data owns the data in the rightful manner, thus getting rid of third party. In [19], the authors also suggested a new design with the help of the smart contracts of blockchain for proficient Distributed Denial of Service moderation solutions. In Lee B et al. [20], blockchain technology is used in modeling a new firmware management scheme testing the firmware, securely and effectively. As well as the features like verifying the firmware and transferring the right firmware of the implanted device are also accompanied. A new security model to guarantee the legitimacy and consistency of password authentication data is developed using the blockchain network in Moinet A. [21]. Apart from blockchain technologies, ECC is widely used in security systems. In [22], the authors suggested the ECC centered verification protocol for RFID with two schemes, one with storage of distinct key material for each genuine tag and the other is deprived of storage of single key material at the reader's side. The authors of [23] used ECC for developing authentication protocol for health observing system. The authors of [24] proposed a easy end-to-end authentication scheme which is ECC-based for Wireless Body Area Networks. However, it has been found that the scheme is susceptible from the clock synchronization problem and known session based information attack.

In [25], an anonymous authentication scheme is well demonstrated and validated using AVISPA simulation in the wireless medical sensor network. However, it was found and proved through cryptanalysis in [26] in the year 2017 that [25] embedded the vulnerability of de-synchronization, posing a threat of stolen mobile device attack and exposing sensor key. With time, several variants of the authentication schemes have been proposed. To mention few, [27] is body motion based using wearable, three factor authentication mechanism is detailed [28], authentication based on cloud server in [29] etc. Along the same lines, in [30], a lightweight authentication scheme is articulated which was basically meant for wearable devices. Similar to this, in [31], the design for authentication for WBANs is presented using lightweight ECC principles. But the scheme is prone to DoS attack and also to impersonation attack.

3. NETWORK ARCHITECTURE

The network architecture as shown in Figure 1 comprises of service providers, managed by device administrators (DAs), users and a blockchain network, managed by blockchain gateway administrator (BCA). The DAs can register with the blockchain network by exchanging authentication data. Upon receiving the signed documents and verification, the BCA pushes the device policies into the blockchain network. The authenticated and authorized device policies are up and are visible to the users. If any user needs device's service, it has to acquire the respective device policy from BCA, sign it and send back to the BCA. Upon receiving the signed device policy from the user and verification, the BCA generates the tokens for both user and DAs. When the user produces the token to the DA in order to avail the service, the DA verifies the token and allows the user to avail the service.

BCA – BlockChain Administrator

DA – Device Administrator

S_B -- BCA's private key

PK_{BCA} – BCA's Public key

RESEARCH ARTICLE

MSK_{u_i} – Master secret key for user i

MSK_{d_j} – Master secret key for device j

ID_{u_i} – Indentity of user i

ID_{d_j}—Identity of device j

SG_{D_j} – Signature for device j

SG_{U_i} – Signature for user i

SSP_{D_j} – Secret signature parameter for device j

SSP_{U_i} – Secret signature parameter for user i

r_{B_1} – Secret random numbers selected by blockchain for device j

r_{D_j} –Secret random numbers selected by device j

x_{D_j} –Time based secret random numbers selected by device j

r_{U_i} –Secret random numbers arbitrated by user i

x_{U_i} –Time based secret random numbers chosen by user i

r_{B_2} –Secret random numbers chosen by blockchain for user i

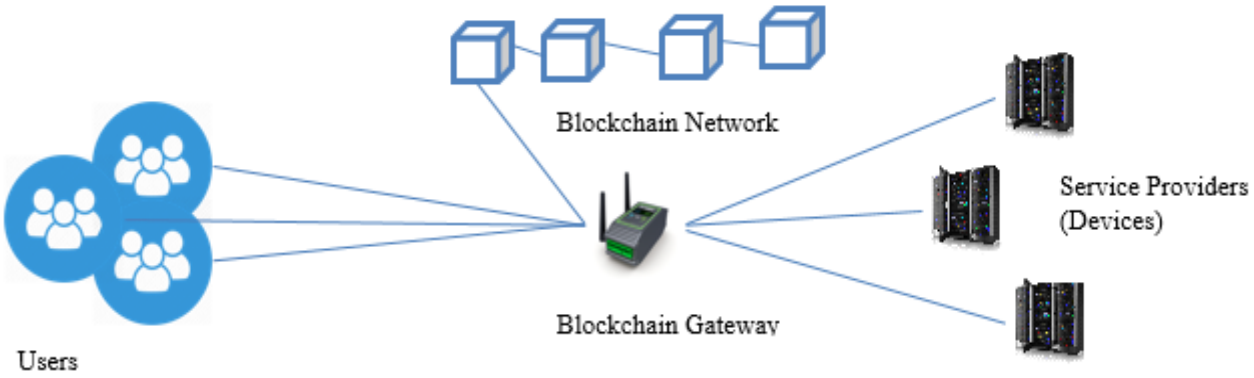

Figure 1 Network Architecture

4. PROPOSED PROTOCOL

In the proposed protocol, we assimilate the ECDHP [32], and ECDLP detailed in [33-34] qualities and effectiveness offered in the security as well as in strength and authentication under the varied context and the invertible hash functions and xor computations. ECDHP mainly offer insolvability existing in calculating the $d_i d_j \Psi$ assuming that $d_i \Psi$, $d_j \Psi \in E_\Psi(a,b)$ on an Elliptic Curve E_Ψ is given.

4.1. Initialization Phase

In this, all the entities (users and devices) in the network submit their entities to the Blockchain Administrator (BCA) so that they can be the part of the network. BCA generates the master secret keys (MSK) for each and every user and device and handover via secure channel. BCA also maintains the list of MSKs with their corresponding IDs.

First and foremost, a finite field F_p is selected by the BCA over a wide range such that $p > 2^{160}$and an elliptic curve $E_p(a,b)$ is generated by the central principle:

$y^2 \ mod \ p \ \ (x^3 + ax + b) mod \ p$

Where $(a,b) \in F_p$ and $4a^3 + 27b^2 \ mod \ p \neq 0$ with order n over F_p.

4.2. Device Registration phase

Each device, in this phase, can register itself in the blockchain with the help of BCA. The conversation between BCA and device administrator is depicted in the following steps for the fair loading of device policies into the blockchain network. This phase starts when device administrator requests the BCA to upload its device policies in the blockchain network. The user has to agree the uploaded device policy to avail any services from the device.

Step 1 (DA → BCA): - The device administrator requests BCA to upload the device policy into blockchain network by send its ID ID_{D_j}

Step 2 (BCA → DA):- BCA asks the device administrator to send the signed device policy. BCA selects the random number r_{B_1} as shown in equation 2, and generates $h1_{D_j}$ shown in equation 1 as follows:

$$h1_{D_j} = H_1(ID_{D_j} \mid MSK_{D_j} | R_{B_1} | PK_{BCA}) \quad (1)$$

RESEARCH ARTICLE

$$R_{B_1} = r_{B_1} \cdot P \bmod Q \quad (2)$$

$$PK_{BCA} = S_B \cdot P \bmod Q \quad (3)$$

Equation 3 depicts the generation of public key PK_{BCA} by BCA. BCA sends $(R_{B_1} | h1_{D_j})$ to the device administrator.

Step 3 (DA → BCA):- When device administrator receives the message from BCA, device administrator performs the following computations.

DA computes $h1_{D_j}$ and verifies that the calculated $h1_{D_j}$ is same as received $h1_{D_j}$. If it is same, DA generates its signature, signs its device policy and send it to BCA, otherwise it discards the message and again initiates the conversation from beginning.

DA generates its signature SG_{D_j} shown in equation 5 as follows.

DA selects two random numbers x_{D_j} and r_{D_j} and calculates R_{D_j} shown in equation 4. x_{D_j} is the temporary secret parameter used to calculate signature SG_{D_j}. x_{D_j} is conveyed to BCA as elliptic curve point shown in equation 6.

$$R_{D_j} = r_{D_j} \cdot P \bmod Q \quad (4)$$

$$SG_{D_j} = (MSK_{D_j} \cdot x_{D_j} \cdot R_{B_1}) \cdot P \bmod Q \quad (5)$$

$$SSP_{D_j} = (R_{D_j}, x_{D_j} + r_{D_j}.PK_{BCA}) \quad (6)$$

$$DP_{SD} = ID_{D_j} || DP || SG_{D_j} || SSP_{D_j} \quad (7)$$

Device sends the signed device policy DP_{SD} generated in equation 7 to BCA. BCA, at its end calculates and verifies the device's signature. If verified, BCA uploads the device policy in its network.

4.3. Access Request Phase

Step 1 (User → BCA): - When i^{th}user want to acquire j^{th} device service, it sends its request to BCA by sending its own ID and device ID as shown in equation 8,

$$U_i = ID_{D_j} || ID_{U_i} \quad (8)$$

Step 2 (BCA → User):- BCA asks the user to send the signed request. BCA selects the random number r_{B_2} (equation 10) and generates $h1_{D_j}$ (equation 9) as follows

$$h1_{U_i} = H_1(ID_{U_i} | MSK_{U_i} | R_{B_2} | PK_{BCA}) \quad (9)$$

$$R_{B_2} = r_{B_2} \cdot P \bmod Q \quad (10)$$

BCA sends $(R_{B_2} || h1_{U_i} || DP)$ to the user.

Step 3 (User→ BCA):- Upon receiving the message from BCA, user performs the following computations.

User computes $h1_{U_i}$ and verifies that the calculated $h1_{U_i}$ is same as received $h1_{U_i}$. If it is same, User generates its signature, signs the device policy and sends it to BCA, otherwise it discards the message and again initiates the conversation from beginning.

User generates its signature SG_{U_i} as shown in equation 12.

User selects two random numbers x_{U_i} and r_{U_i} and calculates R_{U_i} (equation 11). x_{U_i} is the temporary secret parameter used to calculate signature . x_{U_i} is conveyed to BCA as elliptic curve point (equation 13). The equations are as follows

$$R_{U_i} = r_{U_i} \cdot P \bmod Q \quad (11)$$

$$SG_{U_i} = (MSK_{U_i} \cdot x_{U_i} \cdot R_{B_2}) \cdot P \bmod Q \quad (12)$$

$$SSP_{U_i} = (R_{U_i}, x_{U_i} + r_{U_i}.PK_{BCA}) \quad (13)$$

$$DP_{SU} = ID_{U_i} || DP || SG_{U_i} || SSP_{U_i} \quad (14)$$

User sends the signed device policy DP_{SU} (equation 14) to BCA. BCA, at its end calculates and verifies the device's signature. If verified, BCA proceeds with the access confirm phase.

4.4. Access Confirm Phase

Once the BCA receives the device policy signed by the user, the BCA will generate tokens $T_{UD_{ij}}$ and handover to the user as well as the device (equations 15 and 16). When the user presents the token to DA, it allows the user to avail its services. BCA handover the tokens as elliptic curve points.

a. BCA → DA

$$Token_{UD_{ij}} = (R_{B_1}, T_{UD_{ij}} + r_{B_1}.R_{D_j}) \quad (15)$$

b. BCA → User

$$Token_{UD_{ij}} = (R_{B_2}, T_{UD_{ij}} + r_{B_2}.R_{U_i}) \quad (16)$$

The proposed protocol conversations are depicted in the Figure 2.

5. FORMAL SECURITY ANALYSIS

Here we use of Burrows–Abadi–Needham logic, popularly known as BAN logic, to verify our authentication protocol.

5.1. BAN Logic Notations

1. Message Meaning

$$\frac{P| \equiv Q \leftarrow K \rightarrow P, P \lhd (X)_K}{P| \equiv Q | \sim X}$$

RESEARCH ARTICLE

2. Nonce Verification

$$\frac{P| \equiv \#(X), P| \equiv Q| \sim X}{P| \equiv Q| \equiv X}$$

3. Jurisdiction

$$\frac{P| \equiv Q \Rightarrow X, P| \equiv Q| \equiv X}{P| \equiv X}$$

4. Decomposition rule

$$\frac{P| \equiv (X, Y)}{P| \equiv X}$$

$$\frac{P| \equiv Q| \sim (X, Y)}{P| \equiv Q| \sim X}$$

5. Conjunction rule

$$\frac{P| \equiv (X), P| \equiv (Y)}{P| \equiv (X, Y)}$$

5.2. Our Assumptions in the Proposed Protocol

1. BCA$| \equiv PK_{BCA}, R_{B_1}, MSK_{D_j}, R_{B_2}, MSK_{U_i}$
2. DA$| \equiv R_{D_j}, X_{D_j}, MSK_{D_j}$
3. DA$| \equiv \#(h_{1D_j})$
4. DA$| \equiv$ BCA $\Rightarrow PK_{BCA}$,
5. DA$| \equiv \#(h_{1U_i})$
6. User$| \equiv R_{U_i}, X_{U_i}, MSK_{U_i}$
7. User$| \equiv$ BCA $\Rightarrow PK_{BCA}$,

5.3. Goals

A. DA$| \equiv Token_{UD_{ij}}$

B. User$| \equiv Token_{UD_{ij}}$

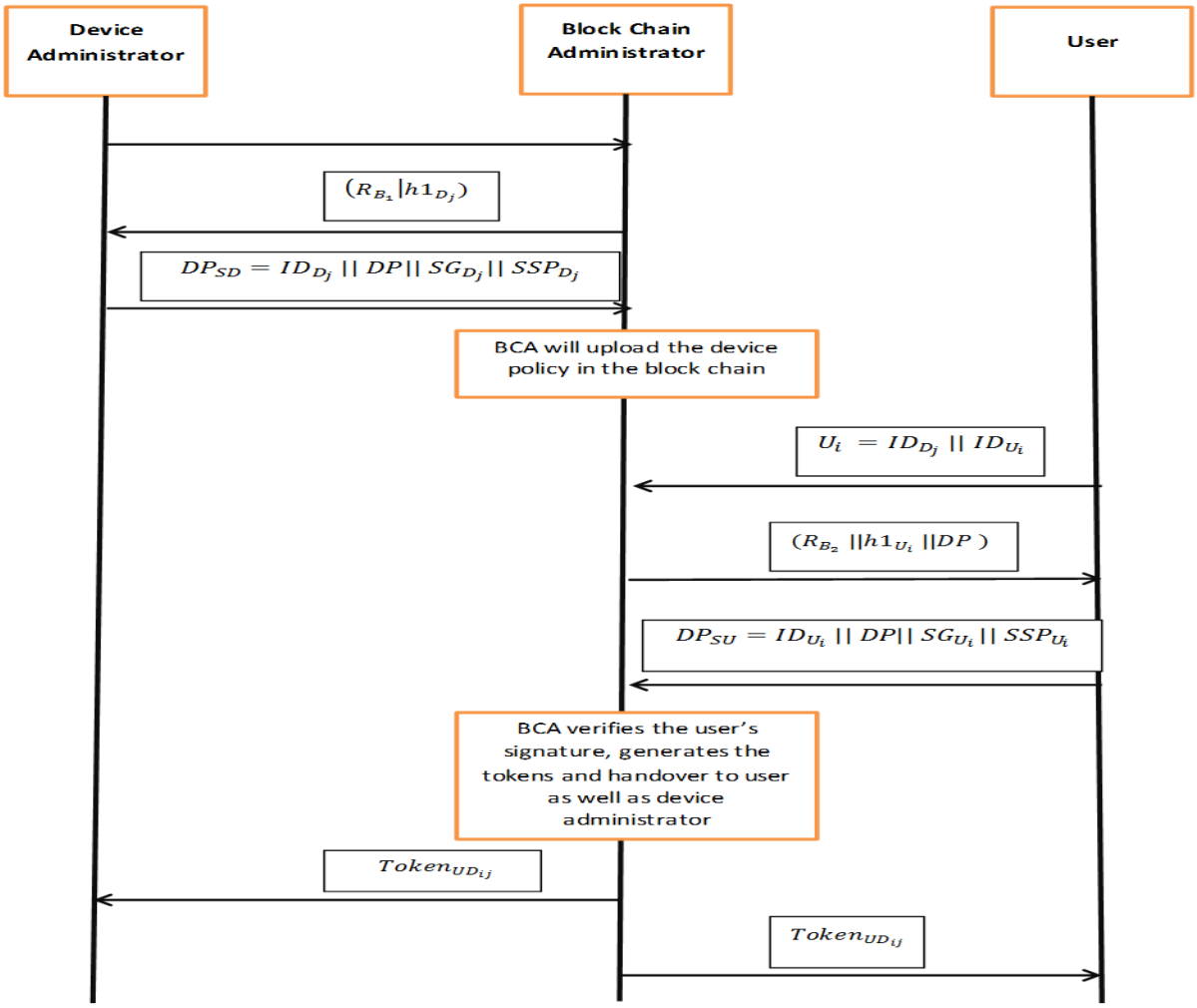

Figure 2 Flow Diagram for Registration, Access Request and Access Confirm Phases

RESEARCH ARTICLE

5.4. Proof for Goal A

5.4.1. Device Registration Phase

1. BCA ◁ $(\mathrm{ID})_{\mathrm{D_j}}$
2. $BCA \mid\sim \left(R_{B_1} \middle| h1_{D_j}\right)$
3. DA ◁ $(R_{B_1} | h1_{D_j})$

DA ◁ $(R_{B_1} | h1_{D_j})$

$h_{1D_j} = H_1(ID_{D_j} \mid MSK_{D_j} | R_{B_1} | PK_{BCA})$

According to 2nd (Nonce verification rule), 3rd assumption, and 2nd statement we get

4. DA| ≡ BCA | ≡ $h1_{D_j}$

According to 3rd (jurisdiction) rule, 4th assumption, and4th statement, we get,

5. DA| ≡ $h1_{D_j}$

According to 4th (decomposition) rule, 5th statement, we get,

6. DA| ≡ R_{B_1}

Now we have ,

7. BCA ◁ $ID_{U_i} || DP || SG_{U_i} || SSP_{U_i}$ (BCA ◁ DP_{SD})
8. $SG_{D_j} = (MSK_{D_j} \cdot x_{D_j} \cdot R_{B_1}) \cdot P \bmod Q$
9. $SSP_{D_j} = (R_{D_j}, x_{D_j} + r_{D_j}.PK_{BCA})$

From message meaning rule we get,

BCA| ≡ DA | ~ DP_S

From 1st assumption and decomposition rule we get

10. BCA| ≡ R_{D_j} ,
11. BCA| ≡ x_{D_j} ,
12. BCA| ≡ SG_{D_j} and hence
13. BCA| ≡ DP_S

5.4.2. In Access Confirm Phase

14. DA ◁ $(Token_{UD_{ij}} = (R_{B_1}, T_{UD_{ij}} + r_{B_1}.R_{D_j}))$

From statement 6, assumption 2 and decomposition rule we get,

15. DA| ≡ $T_{UD_{ij}}$
16. From statement 15 and conjunction rule we get,

DA| ≡ $(Token_{UD_{ij}})$ { Here our 1st goal is proved}

5.5. Proof for Goal B

User ◁ $(R_{B_2} | h1_{U_i})$

1. BCA ◁ $ID_{D_j} || ID_{U_i}$
2. $BCA \mid\sim (R_{B_2} || h_{1U_i} || DP)$
3. User ◁ $(R_{B_2} || h_{1U_i} || DP)$

$h_{1U_i} = H_1(ID_{U_i} \mid MSK_{U_i} | R_{B_2} | PK_{BCA})$

According to 2nd (Nonce verification rule), 5th assumption, and 2nd statement we get

4. User| ≡ BCA | ≡ h_{1U_i}

According to 3rd (jurisdiction) rule, 7th assumption, and4th statement, we get,

5. User| ≡ h_{1U_i}

According to 4th (decomposition) rule, 5th statement, we get,

6. User | ≡ R_{B_2}

Now we have ,

7. BCA ◁ $ID_{U_i} || DP || SG_{U_i} || SSP_{U_i}$ (BCA ◁ DP_{SU})
8. $SG_{U_i} = (MSK_{U_i} \cdot x_{U_i} \cdot R_{B_2}) \cdot P \bmod Q$
9. $SSP_{U_i} = (R_{U_i}, x_{U_i} + r_{U_i}.PK_{BCA})$

From message meaning rule we get,

BCA| ≡ DA | ~ DP_S

From 1st assumption and decomposition rule we get

10. BCA| ≡ R_{U_i} ,
11. BCA| ≡ X_{U_i} ,
12. BCA| ≡ SG_{U_i} and hence
13. BCA| ≡ DP_{SU}

5.5.1. In Access Confirm Phase

14. User ◁ $\left(Token_{UD_{ij}} = \left(R_{B_2}, T_{UD_{ij}} + r_{B_2}.R_{U_i}\right)\right)$
15. From statement 6, assumption 2 and decomposition rule we get,
16. User| ≡ $T_{UD_{ij}}$

From statement 15 and conjunction rule we get,

RESEARCH ARTICLE

User| ≡ ($Token_{UD_{ij}}$) { Here our 2nd goal is proved}

6. USAGE OF AVISPA FOR FORMAL SECURITY ANALYSIS

The other widely used tool in case of security protocol models is AVISPA, abbreviated from Automated Validation of Internet Security Protocols and Applications. The models intended for usage in the internet communication are tested for their authenticating strength. AVISPA is acclaimed to be used for proving authentication feature officially, of the models.

```
role bca (BCA,DA: agent, P:text, KDF,MUL,H1,ADD,SUB :
hash_func, K1: symmetric_key, Snd, Rcv:channel (dy))
played_by BCA
def=
local State:nat,
DDA,IDBCA,Sbca,Ubca,Uda,RB1,Rb1,XDj,Xdj,H11,SGDj,
SSPDj,RDj,Rdj,DPs:text
const success,sec1,sec2,dps1: protocol_id
init State := 0
transition
1. State = 0 /\ Rcv(IDDA') =|> State' := 1
/\ IDBCA' := new()
/\ Sbca' := new()
/\ Rb1' := new()
/\K1':=new()
/\ Ubca' := MUL(Sbca',P)
/\RB1' := MUL(Rb1',P)
/\H11' := H1(IDDA'.K1'.RB1'.Ubca')
/\ Snd(H11'.RB1')
/\ secret({Sbca},sec1,{BCA})
/\secret({K1},sec2,{BCA,DA})
2. State = 1 /\ Rcv(IDDA'.DPs'.SGDj'.SSPDj')
/\Xdj' =
SUB(ADD(Xdj',MUL(Rdj',Ubca')),MUL(RDj',Sbca'))
/\SGDj' = MUL(K1',Xdj',RB1',P') =|> State' := 2
/\Snd(success)
/\witness(DA,dps1,BCA)
/\request(DA,dps1,BCA)
end role
```

AVISPA Code 1 HLPSL Code for Role BCA

```
role da(BCA,DA:agen, P :text, KDF,MUL,H1,ADD,SUB:
hash_func, K1 : symmetric_key, Snd,Rcv:channel(dy))
played_by DA
def=
   local State : nat,
       IDDA,IDBCA,IDUSER,
RDj,Rdj,XDj,Xdj,SGDj,SSPDj,DPs,Ubca,DP,H11,RB1:text
 const success,sec1,sec2,dps1 : protocol_id
 init State := 0
 transition
1. State = 0 /\ Rcv(start) =|> State' := 1
/\IDDA' :=new()
/\Snd(IDDA')
2. State = 1 /\Rcv(H11'.RB1')
/\H11 = H1(IDDA.K1'.RB1'.Ubca) =|> State' := 2
/\Rdj' := new()
/\Xdj' := new()
/\DP' := new()
/\RDj' := MUL(Rdj,P)
/\XDj' := MUL(Xdj,P)
/\SGDj' := MUL(K1,Xdj',RB1',P)
/\SSPDj' := (RDj'.ADD(Xdj',MUL(Rdj,Ubca)))
/\DPs' := (IDDA.DP'.SGDj'.SSPDj')
/\Snd(DPs')
/\witness(DA,dps1,BCA)
/\request(DA,dps1,BCA)
/\secret({Rdj,Xdj},sec1,{DA})
/\secret({K1},sec2,{BCA,DA})
end role
```

AVISPA Code 2 HLPSL Code for Role DA

```
goal
secrecy_of sec1
secrecy_of sec2
authentication_on dps1
end goal
```

AVISPA Code 3 HLPSL Code for Goal

```
role user(BCA,USER:agent, P
:text,KDF,MUL,H1,ADD,SUB: hash_func,K1 :
symmetric_key,Snd,Rcv:channel(dy))
played_by USER
def=
local State : nat,
IDDA,IDBCA,IDUSER,
RUj,Ruj,XUj,Xuj,SGUj,SSPUj,DPs,Ubca,DP,H11,RB2:text
const success,sec1,sec2,dps1 : protocol_id
init State := 0
transition
1. State = 0 /\ Rcv(start) =|> State' := 1
/\IDUSER' :=new()
/\Snd(IDUSER')
2. State = 1 /\Rcv(H11'.RB2')
/\H11 = H1(IDUSER.K1'.RB2'.Ubca) =|> State' := 2
```

RESEARCH ARTICLE

```
/\RUj' := new()
/\Xuj' := new()
/\DP' := new()
/\RUj' := MUL(Ruj,P)
/\XUj' := MUL(Xuj,P)
/\SGUj' := MUL(K1,Xuj',RB2',P)
/\SSPUj' := (RUj'.ADD(Xuj',MUL(Ruj,Ubca)))
/\DPs' := (IDUSER.DP'.SGUj'.SSPUj')
/\Snd(DPs')
/\witness(USER,dps1,BCA)
/\request(USER,dps1,BCA)
/\secret({RUj,Xuj},sec1,{USER})
/\secret({K1},sec2,{BCA,USER})
end role
```

AVISPA Code 4 HLPSL Code for Role User

```
% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/span/span/testsuite/results/MyAuthBC93.if
GOAL
as_specified
BACKEND
OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 12.45s
visitedNodes: 29 nodes
depth: 12 plies
```

AVISPA Code 5 OFMC Output

```
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
TYPED_MODEL
PROTOCOL
/home/span/span/testsuite/results/GRP_AKA999.if
GOAL
As Specified
BACKEND
CL-AtSe
STATISTICS
Analysed  : 0 states
Reachable  : 0 states
Translation: 0.09 seconds
Computation: 0.00 seconds
```

AVISPA Code 6 CL-AtSe Output

For agreeing the protocol to be certified, AVISPA provides HLPSL module, treated as a role-based language. In the HLPSL program, every node is represented as a role during protocol execution and joins over the uncertain public channel with the additional roles of the network. The HLPSL program is interpreted into intermediate form (IF), a lower level code is produced by hlpsl2if translator and unswervingly read by the AVISPA back-ends: OFMC, CLAtSe, SATMC, and TA4SP. The impostor is shown as one of the roles holding adequate knowledge of the traffic transferring through the channel of the interactive parties.

The proposed protocol description is authenticated using the mentioned back-ends: CLAtSe and OFMC; the goals stated in Code 3, and the algorithms correspondingly for the roles involved in the network, as stated in the AVISPA Code 1 for the Blockchain Administrator (BCA), Code 2 for Data Administrator (DA), Code 4 for User. Finally, both the back-ends' simulation results of proposed protocol are shown in the Code 5 and Code 6, respectively.

7. INFORMAL SECURITY ANALYSIS

7.1. Man-in-the-Middle (MITM) Attack

In the network architecture, some intruder, say I may steal the message $Token_{UD_{ij}}$ while being transmitted over transmission lines. Even though, it tries to extract the actual token, it cannot do so, as it is been sent as a point on the elliptic curve. To extract it, it has to derive the key using random number of the legitimate user. But this random number was never transmitted over transmission line and hence we can say our projected protocol can survive the MITM attack.

7.2. User/ Device Impersonation Attack

In impersonation attack, the adversary I, can impersonate as genuine user and send the request to access the service. The BCA is also tricked to assume and the request received is genuine. The BCA then sends the device policy to the adversary I (assuming it's the genuine user). The user has to sign the device policy and must send to the BCA for verification. At this point, the adversary I is unable to generate correct signature as it does not possess pre shared master key which is used as one of the parameter in the signature. Hence we can say our protocol withstand user impersonation attack. The same is true for the device impersonation attack as well.

7.3. Replay Attack

In replay attacks, the adversary I can steal the user's signature while being transmitted over the channel, and can use it to avail services from the resources later. But our proposed protocol uses time based parameter in generating the signature. The BCA will check the time based parameter .If it is within the accepted time, the BCA will consider that

RESEARCH ARTICLE

signature, otherwise discard it. Hence we can say our proposed protocol withstands replay attacks.

8. CONCLUSION AND FUTURE SCOPE

In our paper we suggested a blockchain centred authentication and access control protocol. In this, block chain administrator is responsible for authenticating and authorizing every user on behalf of service providers. Here the service provider is getting rid of authenticating each and every request approaching it for some service. We have also analysed the proposed protocol formally with BAN logic and AVISPA and established the goals needed in order to validate the authentication protocol. Further we would like to implement this protocol using any blockchain platform like Ethereum or hyperledger.

REFERENCES

[1] Dongxing Li, Wei Peng, Wenping Deng, FangyuGai, "A Blockchain-based Authentication and Security Mechanism for IoT", 2018 27th International Conference on Computer Communication and Networks (ICCCN). doi:10.1109/icccn.2018.8487449.

[2] Muhammad Tahir, Muhammad Sardaraz, Shakoor Muhammad, Muhammad Saud Khan, "A Lightweight Authentication and Authorization Framework for Blockchain-Enabled IoT Network in Health-Informatics",Sustainability 2020, 12, 6960; doi:10.3390/su12176960.

[3] Bennett, B. HIE Overview: A Framework for Healthcare Interoperability. Telehealth Med. Today 2017, 2, 1–6.

[4] Casino, F.; Patsakis, C.; Batista, E.; Borràs, F.; Martínez-Ballesté, A. Healthy routes in the smart city: A context-aware mobile recommender. IEEE Softw. 2017, 34, 42–47.

[5] Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. Int. J. Web Grid Serv. 2018, 14, 352–375.

[6] Udokwu, C.; Kormiltsyn, A.; Thangalimodzi, K.; Norta, A. The state of the art for blockchain-enabled smart-contract applications in the organization. In Proceedings of the 2018 IvannikovIspras Open Conference (ISPRAS), Tokyo, Japan, 22–23 November 2018; pp. 137–144.

[7] ZibinZheng, ShaoanXie, Hongning Dai, Xiangping Chen, and HuaiminWang,"An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends",2017 IEEE 6th International Congress on Big Data,978-1-5386-1996-4/17 DOI .1109/BigDataCongress.2017.85

[8] Sharad Kumar Verma, D.B. Ojha, "A Discussion on Elliptic Curve Cryptography and Its Applications", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, January 2012.

[9] Victor S. Miller. Use of elliptic curves in cryptography. In H.C. Williams, editor, Advances in Cryptology CRYPTO'85, vol. 218 of Lecture Notes in Computer Science, pp. 417-426.Springer-Verlag, 1986.

[10] Whitfield Diffie and Martin E. Hellman. New directions in cryptography, IEEE Transactions of Information Theory, 22(6):644-654, 1976.

[11] TaherElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory 31(4):469- 472, 1985.

[12] http://en.wikipedia.org/wiki/Elliptic_curve_cryptography.

[13] Certicom, Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography, Version 1.0, September 2000.

[14] Zhao J L, Fan S, Yan J. Overview of business innovations and research opportunities in blockchain and introduction to the special issue. Financial Innovation, 2016, 2(1):28.

[15] Ouaddah A, AbouElkalam A, AitOuahman A. FairAccess: a new Blockchain based access control framework for the Internet of Things. Security & Communication Networks, 2017, 9.

[16] Xu Q, Jin C, Rasid M F B M, et al. Blockchain-based decentralized content trust for docker images. Multimedia Tools & Applications, 2017(239):1-26.

[17] Rodrigues B, Bocek T, Lareida A, et al. A Blockchain-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts[C]// IFIP International Conference on Autonomous Infrastructure, Management, and Security. Springer, Cham, 2017:16-29.

[18] Zyskind G, Nathan O, Alex. Decentralizing Privacy: Using Blockchain to Protect Personal Data[C]// IEEE Security and Privacy Workshops. IEEE Computer Society, 2015:180-18.

[19] Kumari S, Karuppiah M, Das A K, et al. A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers[J]. Journal of Supercomputing, 2017(4):1-26.

[20] Lee B, Lee J H. Blockchain-based secure firmware update for embedded devices in an Internet of Things environment[J]. Journal of Supercomputing, 2017, 73(3):1-16.

[21] Moinet A, Darties B, Baril J L. Blockchain based trust &authentication for decentralized sensor networks[J]. 2017.

[22] LamraniAlaoui, Hasnae, El Ghazi, Abdellatif, Zbakh, Mustapha, Touhafi, Abdellah, Braeken An. "A Highly Efficient ECC-Based Authentication Protocol for RFID", . Journal of Sensors, Hindawi, 2021, 10.1155/2021/8876766.

[23] K. Sowjanya, M. Dasgupta, and S. Ray, "An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems," International Journal of Information Security, vol. 19, no. 1, pp. 129–146, 2020

[24] Zhao, Z.: An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem. J.Med. Syst. 38(2), 1–7 (2014). https://doi.org/10.1007/s10916014-0013-5

[25] Amin, R., Islam, S .K .H.,Biswas, G., Khan, M .K., Kumar, N.: A robust and anonymous patient monitoring system using wireless medical sensor networks. FutureGener. Comput. Syst. 80(C), 483 495 (2016). https://doi.org/10.1016/j.future.2016.05.032

[26] Jiang, Q., Ma, J., Yang, C., Ma, X., Shen, J., Chaudhry, S .A.: Efficient end-to-end authentication protocol for wearable health monitoring systems. Comput. Electr. Eng. 63(C), 182–195 (2017).https://doi.org/10.1016/j.compeleceng.2017.03.016

[27] Yessad, N., Bouchelaghem, S., Ouada, F .S., Omar, M.: Secure and reliable patient body motion based authentication approach for medical body area networks. Pervasive Mob. Comput. 42(C), 351–370 (2017). https://doi.org/10.1016/j.pmcj.2017.06.009

[28] Li, X., Niu, J., Kumari, S., Wu, F., Sangaiah, A .K.,Choo, K .K .R.: A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. J. Netw. Comput. Appl. 103(C), 194–204 (2018). https://doi.org/10.1016/j.jnca.2017.07.001

[29] Wu, F., Li, X., Xu, L., Kumari, S., Karuppiah, M., Shen, J.: A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server. Comput. Electr. Eng. 63(C), 168–181 (2017). https://doi.org/10.1016/j.compeleceng. 2017.04.012 21.

[30] Das, A.K., Zeadally, S., Wazid, M.: Lightweight authentication protocols for wearable Computer Electrical Engineering, https://doi.org/10.1016/j.compeleceng.2017.03.008

[31] Liu, J., Zhang, L., Sun, R.: 1-RAAP: an efficient 1-round anonymous authentication protocol for wireless body area networks. Sensors (2016) https://doi.org/10.3390/ s16050728.

[32] Menezes, A.J. Elliptic Curve Public Key Cryptosystems; Kluwer Academic Publishers: Boston, MA, USA, 1993.

[33] Hankerson D., Menezes A., Elliptic Curve Discrete Logarithm Problem. In: van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA, 2011.

RESEARCH ARTICLE

[34] Junichi Yarimizu1 , Yukihiro Uchida1 and Shigenori Uchiyama, "The elliptic curve Diffie-Hellman problem and an equivalent hard problem for elliptic divisibility sequences", JSIAM Letters Vol.6 pp.5–7 2014.

Authors

Geeta Kakarla, done B.E in Computer Technology from KITS, Ramtek, Nagpur University and M.Tech in Software Engineering from JNTUH, Hyderabad. She possess 12 years of experience in academic and has guided many UG students. Currently she is working as Assistant Professor at Sreenidhi Institute of Science and Technology, Hyderabad. Her areas of interest include IoT, Web Technologies, Information Security, IoT and Network Security.

Dr. S. Phani Kumar, working as Professor & Head, Department of Computer Science & Engineering, School of Technology, GITAM Deemed to be University, Hyderabad. He completed his B.E.(Computer Science & Engineering) from VTU, Belgaum, M.Tech.(Software Engineering) and Ph.D. from Bharath University, Chennai. He has 30 research papers in reputed peer reviewed journals in addition to 12 papers in International Conferences to his credit. He has co-authored 7 book chapters (05 springer series, 01 CRC press and 01 IGI Global). He is Life member of ISTE, member of CSI, member of Indian Science Congress Association. His research interests are software safety, safety critical systems, Machine Intelligence, Wireless Sensor Networks and IoT Security.

How to cite this article:

Geeta Kakarla, S. Phani Kumar, "Blockchain Powered Mutual Authentication and Access Control Protocol", International Journal of Computer Networks and Applications (IJCNA), 9(1), PP: 103-113, 2022, DOI: 10.22247/ijcna/2022/211629.