International Journal for Multidisciplinary Research (IJFMR)

E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Wireless Sensor Network with Blockchain Technology Using Elliptic Curve Discrete Logarithm Problem and Its Applications

Gulab Das[1], B.P. Tripathi[2]

[1]Research Scholar, Department of Mathematics, Govt. Nagarjuna PG College of Science, Raipur, Chhattisgarh, India.

[2]Assistant Professor, Department of Mathematics, Govt. Nagarjuna PG College of Science, Raipur, Chhattisgarh, India.

Abstract

Wireless sensor network (WSN), a type of communication system, is normally deployed into the unattended environment where the intended user can get access to the network. The sensor nodes collect data from this environment. If the data are valuable and confidential, then security measures are needed to protect them from the unauthorized access. This situation requires an access control protocol (ACP) in the design of sensor network because of sensor nodes which are vulnerable to various malicious attacks during the authentication and key establishment and the new node addition phase.Nowadays, wireless sensor networks are being widely applied in many fields of human life such as civil and military applications. Although WSNs can bring a lot of benefits and conveniences. However, when applying the WSNs in the real world we have to face many challenges such as security, storage due to its centralized server/client model. Therefore, it is necessary to apply the distributed model in the WSNs system. One of the newest distributed systems today is Blockchain (BC). Blockchain is a decentralized technology that can help the computation and management processes as well as security in WSNs.In this paper, we propose a secured ACP for such WSN. This protocol is based on Elliptic Curve Discrete Log Problem (ECDLP) and double trapdoor chameleon hash function which secures the WSN from malicious attacks such as node masquerading attack, replay attack, man-in-the-middle attack, and forgery attacks. Proposed ACP has a special feature known as session key security. Also, the proposed ACP is more efficient as it requires only one modular multiplication during the initialization phase.This article provides an overview of Blockchain integration in WSN with highlighting the benefits and challenges of applying this technology to WSN. We can conclude that using Blockchain technology to solve the problem of security and distributed storage for WSN can be an effective approach. It could pave the way for new research directions and distributed applications.

Keywords: Blockchain, Chameleon hash function, Access Control Protocol Based on Elliptic Curve Discrete Logarithm Problem , Wireless sensor networks, Security issues.

1 Introduction

Blockchain is a technology that allows the transmission of data securely based on an extremely complex encryption system, similar to a company's accounting ledger, where data is closely monitored and record all transactions on the peer-to-peer network. Each block contains information about its creation time and is linked to the previous block by hash code and transaction data. Once the data is recorded by the network, there is no way to change it. Blockchain is designed to resist fraud and alteration of data[12].

A wireless sensor network (WSN) is a system of a network consisting of spatially distributed autonomous devices which uses sensors to cooperatively monitor physical or environmental conditions such as temperature, sound, vibration, pressure, motion, or pollutants at different locations. The purpose of a WSN is to collect and process data from a target domain and transmit the information back to specific sites. WSN technology is an emerging technology that can be utilized in a wide range of potential applications in the real world. Such a network usually consists of a number of wireless sensor nodes that arrange themselves into a multihop network. Each node consists of one or more sensors. In many WSN, it is sufficient to secure the data transfer between the sensor nodes and the base station, especially, when the base station is needed to ensure that the received message sent by the specific sensor node is unaltered during transfer. However, in any WSN, providing security during authentication, key establishment and new node deployment is important and for that purpose, an ACP is needed. In the health-care monitoring systems, military domains, and in many other applications, WSN requires a hard and fast authentication scheme to secure the data from the attackers because the authenticity and integrity of such data received at the base station highly in[uence the Snal results in many WSN applications, as shown by Abduvalievet al.[1].In a paper, Zhou et al.[2] developed an ACP based on the elliptic curve cryptosystem (ECC) for securing the new node deployment process.For details on the elliptic curve (EC) one can refer to Miller and Koblitz [3]and so forth.Next, Huang [4] proposed an efficient ACP based on the EC and hash chains. In this scheme, new nodes can be easily added. The authors claimed that it is resistant to various attacks. Later, Kim and Lee [8] pointed out that the ACP given by Huang [4] is insecure and it lacks hash chain renewability which is an important aspect needed in any resource constrained sensor network. Consequently, Kim and Lee [5]further proposed an enhanced ACP by adding a hash chain renewal phase supporting the mutual authentication. Also, they claimed that their enhanced access control protocol is resistant to various known attacks.

Further, Shen et al.[6] and Zeng et al.[7] demonstrated that the scheme given by Kim and Lee was still vulnerable to masquerade attack executed by new as well as legal nodes because it lacks hash chain renewability soon after the authentication and key established phase. Finally, Lee et al.[8]and Zhou[2]are also vulnerable to various adversary attacks and had hung storage overhead at the sensor node.

The concept of chameleon hash function was first given by Krawczyk and Rabin[9]. Chameleon hash function is used to calculate the message digest. A chameleon hash function is a basically trapdoor collision-resistant hash function. It is found to be a very useful tool in cryptography. In order to take such advantage of this function, Chen et al.[10] involved it in the access control protocol. However, the Chen et al. [10] protocol required the precomputed secret value of x^{-1} during the transection even without verifying the authentic value and thus invites attacks.

Motivated by the use of the double trapdoor chameleon hash function by Chen et al.[11], in this paper, we propose a secure and efficient ACP based on ECDLP. In our opinion, the proposed protocol which does not require the precomputed value of x^{-1} dynamically provides the security against different attacks, even when new nodes are added to the WSN. Looking to the other advantages, our proposed scheme is better as compared to the scheme given by Chen et al.[10].

Integrating blockchain technology into WSNs will bring a lot of benefits. A large number of connections between sensor devices will be handled thanks to the distributed nature of blockchain. This will significantly decrease the costs associated with installing and maintaining large centralized data centers. At the same time, computing and storage needs are distributed to all devices in the network. In addition, when blockchain technology is integrated into WSNs, it will eliminate the centralized architecture of WSNs [13].Furthermore, the Centralized Server and Client Model will be eliminated when peer-to-peer messaging, file distribution, and automatic coordination between devices in the network[14].

The rest of the paper is organized as follows. In Section 2, we give preliminaries required for the proposed access control protocol. In Section 3,the system model and benefits are explained. In Section 4 the proposed scheme is explained. The research challenges are explained in Section 5. The security and efficiency analysis of our proposed scheme is given in Section 6.Applications are given in section 7. Finally, the conclusion is made in Section 8.

2 Preleminaries

As we have said earlier, in this section, we first explain the requirements for the ACP of a wireless sensor network using the ECDLP and trapdoor chameleon hash function. Before doing so, we need to explain the notion of a trapdoor chameleon hash function as given by Chen et al.[15] scheme. Let us first recall the EC as given below.

2.1 Elliptic Curve

We consider the parameters of any EC such that the EC domain parameters can be verified to meet the requirements as given by Law et al.[16]. In order to avoid the Pollard-rho [17] and Pohlig-Hellman algorithms for the discrete logarithm problem defined on EC, it is necessary that the number of F_p -rational points on E, denoted by $*E(F_p)$, be divisible by a sufficiently large prime n. Also, in order to avoid the reduction algorithms of Menezes et al.[18] and Frey and Ruck [19], our EC should be nonsuper singular (i.e.,p should not divide $(p+1-*E(F_p))$). Further, in order to avoid the attack of Semaev [20] on F_p-anomalous curves, our EC should not be F_p-inconsistent (i.e.,$*E(Fp) \neq p$).

2.2 Elliptic Curve Discrete Logarithm Problem

Let E be an elliptic curve defined over a finite field F_p and let P $\epsilon E(F_p)$ be a point of order n. Given Q, where $Q \epsilon E(F_q)$, the ECDLP is used to find the integer l, $0 \leq l \leq n - 1$, such that $Q = l.P$.

2.3 Trapdoor Chameleon Hash Function

Following the ACP of Chen et al.[15], we define double trapdoor chameleon hash function as below.

Let G be a subgroup generated by P and define a cryptographic secure keyed-hash function $f : Z_q \times G \rightarrow Z_q$. Choose random elements (two trapdoor keys)k, $x \epsilon Z_q$ and compute $K = kP$, $Y = xP$. The public hash key is $HK = (K, Y)$, and the private trapdoor key is $TK = (k, x)$. For the given hash family, we define the hash key HK and the proposed chameleon hash function $f : Z_q \times Z_q \rightarrow G$ as follows:

$H_{HK}(m, r) = f(m, K).(K + Y) + rP$................ (1)

A double trapdoor chameleon hash function carries the following properties.

•**Efficiency** : Given a hash key pair HK a pair $(m, r) \epsilon Z_q \times Z_q$, $H_{HK}(m, r) = f(m, K).(K + Y) + rP$ is computable in the polynomial time.

•**Collision − Resistance** : Without the trapdoor key TK it is computationally infeasible to find two pairs $(m_1, r_1), (m_2, r_2) \epsilon Z_q \times Z_q$ which satisfy $m_1 \neq m_2$ and $H_{HK}(m_1, r_1) = H_{HK}(m_2, r_2)$.
•**Trapdoor − Collision** : Assume that we have given the hash and the trapdoor key pair (HK, TK) a pair $(m, r) \epsilon Z_q \times Z_q$, and an additional message $m_2 \epsilon Z_q$ and we want to find $r_2 \epsilon Z_q$ such that $f(m_1, K).(K + Y) + r_2Y = f(m_2, K).(K + Y) + r_2Y$ ....(2)
The value of r_2 can be computed in polynomial time as follows: $r_2 = r_1 + (k + x)(f(m_1, K) - f(m_2, K))$ modq. Also, as r_1 is uniformly distributed in $\mathfrak{R}$ then the distribution of r_2 is computationally indistinguishable from the uniformly distributed r_1 in $\mathfrak{R}$.

2.4 Notations Used in the Proposed Scheme

The notations involved are listed as follows:
N_i : i-th node.
N_j : j-th node.
BS: base station.
l: integer number.
E: elliptic curve.
P: generator of subgroup G.
f: cryptography secure hash function.
r: random number.
H_{HK}: chameleon hash function.
A_u:authentication value.

2.5 Blockchain

Blockchains are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company or government). At their basic level, they enable a community of users to record transactions in a shared ledger within that community, such that under normal operation of the blockchain network no transaction can be changed once published. In 2008, the blockchain idea was combined with several other technologies and computing concepts to create modern cryptocurrencies: electronic cash protected through cryptographic mechanisms instead of a central repository or authority.
This technology became widely known in 2009 with the launch of the Bitcoin network, the first of many modern cryptocurrencies. In Bitcoin, and similar systems, the transfer of digital information that represents electronic cashtakes place in a distributed system. Bitcoin users can digitally sign and transfer their rights to that information to another user and the Bitcoin blockchain records this transfer publicly, allowing all participants of the network to independently verify the validity of the transactions. The Bitcoin blockchain is independently maintained and managed by a distributed group of participants. This, along with cryptographic mechanisms, makes the blockchain resilient to attempts to alter the ledger later (modifying blocks or forging transactions). Blockchain technology has enabled the development of many cryptocurrency systems such as Bitcoin and Ethereum1 . Because of this, blockchain technology is often viewed as bound to Bitcoin or possibly cryptocurrency solutions in general. However, the technology is available for a broader variety of applications and is being investigated for a variety of sectors.

The numerous components of blockchain technology along with its reliance on cryptographic primitives and distributed systems can make it challenging to understand. However, each component can be described simply and used as a building block to understand the larger complex system. Blockchains can be informally defined as:

Blockchains are distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules.

3 The System Model and Benefits

In traditional WSNs, data will be accessed using a centralized network by different devices through a central server.However, the number of devices participating in the network and the demand for large-scale network applications are increasing. Therefore, using a centralized server is no longer an effective approach for large-scale WSN systems. The WSNs system requires the integration of the most advanced technologies. The use of distributed networks will be one of the effective solutions to solve this problem where "Peer-to-Peer Networking (PPN), Distributed File Sharing (DFS), and Autonomous Device Coordination (ADC)" functions could be capable. The use of Blockchain (BC) technology allows the WSNs system to monitor a large number of devices in the network, especially in the case of WSNs with application expansion needs. The WSNs system can coordinate the handling of connections between devices, and the security and reliability of the system will be greatly enhanced by integrating BC technology. In addition, the WSNs system can handle peerto-peer connections quickly with the help of a distributed ledger.

We can see the difference between the two data flow processes in BC-integrated WSNs and traditional WSNs. The data in WSNs with Blockchain does not use centralized data centers. In WSNs integrated BC technology is the same as traditional WSNs but when the data goes to the Internet the data will go through the distributed Blockchain because the centralized server has been eliminated. Thanks to the distributed ledger in the blockchain, data authentication, and data tampering have become better. The data flow will also become more reliable and secure with the application of BC technology.

The use of Blockchain technology in WSN can bring a lot of benefits such as greatly reducing costs because it does not need to maintain a centralized data storage center, will distribute computing needs, data is stored on all devices in the network.

The outstanding characteristics of Blockchain technology such as decentralization, reliability, and security make it an ideal solution to solve the challenges facing WSNs. Due to the transparency of data in the blockchain, users can track the data when they want. In addition, transactions in the network need to use confirmation and participant consent to prevent tampering.

4 Proposed Access Control Protocol Based on ECDLP

Now we propose our ACP based on ECDLP and double trapdoor chameleon hash function. This method consists of two phases: initialization phase and the node authentication with key establishment phase. The implementation of the proposed ACP is as follows.

4.1 Initialization Phase of the Proposed ACP

The initialization phase is described in the following steps.

Step − 1 : The base station (BS) chooses a random element $x\epsilon Z_q$ and computes $Y = xP$. The public hash key is $HK = Y = xP$ and the private trapdoor key is $TK = x$.

Step − 2 : Choose a random number $k^* \epsilon Z_q$, and compute the chameleon hash value $H_{(HK)BS} = k^*P$.

Step − 3 : Given message m from pair (k_i , k_iP), where $k_i\epsilon Z_q$ as the secrete key and $i = 1, 2, 3, ..., n_1$, then compute a security key $r_i = k^* - f(m, k_iP).(k_i + x)$ modq, uploaded (N_i , k_iP, r_i , H_{HK}) to node N_i .

Note $r_i = k^* - f(m, k_iP).(k_i + x)$ modq. It requires only 1 modular multiplication of Z_q in this phase.

In this section, we give different steps of authentication of the proposed ACP. In all the sensor nodes when deployed, if node N_i wants to communicate with another node N_j , they must implement the following steps to authenticate each other. Subsequently, they must establish a shared session key for securing their communication.

Step − 1 : Two nodes are N_i and N_j , where $i = 1, 2, 3, ..., n_1$ and $j = 1, 2, 3, ..., n_2$, for n_1, $n_2\epsilon n$ and node N_i chooses random number $c_1\epsilon Z_q$ to compute the public key c_1P and $(K + Y)r_i$ and then sends (N_i , c_1P, $(K + Y)r_i$, k_iP) to node N_j .

Step − 2 : Node N_j computes the chameleon hash value H_{HK} of node N_i based on the received message (N_i , c_1P,$(K+Y)r_i$, k_iP). If $H_{(HK)BS}$ and $H'_{(HK)BS}$ are equal, then node N_j chooses random number $c_2\epsilon Z_q$ to compute c_2P and session key $(c_1c_2)^xP = (c_2c_1)^xP$ between nodes N_i and N_j . Then node N_j uses different security key r_j to compute authentication value $A_{(u)j} = H_{HK}((c_1c_2)^xP \parallel (K+Y)r_j)$. It then delivers the message (N_j , c_2P,$(K+Y)r_j$, k_jP, $A_{(u)j}$) to node N_i .

Step − 3 : Node N_i receives the message from N_j and computes chameleon hash value of node N_j and according to the message (N_j , c_2P,$(K+Y)r_j$, k_jP, $A_{(u)j}$) from N_j , it then computes $H'_{(HK)BS} = f(m, K)(K+Y)r_iP$ with the chameleon hash of base station $H_{(HK)BS}$. If $H_{(HK)BS}$ and $H'_{(HK)BS}$ are equal, node N_i then computes the share session key and $(c_1c_2)^xP = (c_2c_1)^xP$ the authentication value $A'_{(u)j}$, where $A'_{(u)j} = H_{HK}((c_1c_2)^xP \parallel (K + Y)r_j)$. Again, node N_i checks the authentication value $A_{(u)j}$; if $A_{(u)j} = A'_{(u)j}$ then node N_j is valid and goes back to a authentication value for given r_i and $(c_1c_2)^xP$ where $A_{(u)j} = H_{HK}((c_1c_2)^xP \parallel (K + Y)r_i)$.

Step − 4 : Node N_j receives $A_{(u)i}$; it also computes the value $A'_{(u)j} = H_{HK}((c_1c_2)^xP \parallel (K +Y)r_i)$. if $A_{(u)j} = A'_{(u)j}$ then node N_i is authenticated; otherwise, the value $A_{(u)i}$ is discarded. Same method applies for node N_j , if $A_{(u)j} = A'_{(u)j}$ then node N_j is authenticated; otherwise, the value $A_{(u)j}$ is discarded. New Node Addition Phase. During the network communication phase, if some sensor nodes are lost, new sensor nodes are needed to deploy. When a new node with N_{i+1} is added, the base station also generates a secret key k_{i+1} and then the base station computes the chameleon hash value $H_{(HK)BS} = f(m, k_{i+1} P)(k_{i+1} P+Y) r_{i+1} P$ at node N_{i+1} and update as broadcasting chameleon hash value $H_{(HK)BS}$ in the base station. The authentication and key establishment for any old node with the new node N_{i+1} is the same as authentication steps.

In order to show the correctness of our proposed ACP, we assert that, during the authentication with key establishment phase, node N_j authenticates node N_i based on the chameleon hash value of node N_i ; that is, it computes the value of $H_{(HK)BS} = f(m, K)(K + Y)r_iP$ based on the received message (N_i , c_1P,$(K + Y)r_i$, k_iP) from node N_i and publishes the message of the base station which is written as $H_{(HK)BS} = f(m, k_iP)(k_iP + Y)k^*P - f(m, k_iP)(k_iP + xP) = k^*P$ the chameleon hash value.

5 Research Challenges

We can see a lot of benefits that Blockchain can bring. However, Blockchain is not a perfect technology, it also has its flaws and challenges, when applying them users also need to trade-off some characteristics. These challenges can be summarized as follow:

Scalability : Blockchain's distributed character may be lost as the scale of the WSNs expands. Many characteristics of Blockchain will decrease as the number of nodes in WSNs increases. This is considered as one of the significant limitations because the expansion needs of WSNs are huge.
Power − consumption − and − processing − time : Blockchain requirements on power consumption, computing power as well as processing time are very strict. Meanwhile, the devices in WSNs are mostly low-power devices. In addition, in WSNs there are many different devices that are not synchronized in terms of power consumption, computing power, and processing speed. Therefore, the application of Blockchain in WSNs faces many difficulties.
Storage : Using a distributed ledger to store transactions and device IDs in the network and eliminating the central server model is one of the key advantages of Blockchain. However, these ledgers are stored in each network node, the size of which will increase over time. Moreover, the number of network nodes is increasing due to the need to expand the network. Meanwhile, devices in WSNs have low computing power and storage capacity. Therefore, the application of Blockchain technology will require significant changes to the infrastructure of WSNs.

Lack − of − skills : The number of people who know about Blockchain technology is still limited because it is a quite new technology. Meanwhile, many applications require users to have a clear understanding of how Blockchain works. WSNs are applied everywhere around us, so in order to apply Blockchain in WSNs, it is necessary to have public awareness about Blockchain.

Legal − and − Compliance − issues : Blockchain technology can connect different devices from all over the world without following any standards or laws, which are challenges for manufacturers and service providers and make many businesses afraid to use Blockchain technology.

6 Security Analysis

For the purpose of analysing the security aspect of our proposed ACP, we claim that attacker cannot find the authentication value for communication node between N_i and N_j. These nodes require authentic value of the message to be communicated from N_i to N_j . First we ascertain that node N_i has been authenticated by node N_j using the chameleon hash value
$H_{(HK)BS} = f(m, k_{i+1} P)(k_{i+1} P + Y) r_{i+1} P$ ....(3)
and then computes the authentication value $A_{(u)j}$ corresponding $A_{(u)i}$ .The authentication value $A_{(u)i}$ is obtained by the shared session key and the security key r_i .However, only the communication nodes accept the session key c_1c_2P and the only node N_i and the base station can have the security key r_i .
Second, node N_j is preloaded with the chameleon hash value by the base station $H_{(HK)BS}$ along with node N_i and obtained $H'_{(HK)BS}$. However, the computed value of $H'_{(HK)BS}$ needs some value of identity ID, secure hash key k_iP and security key r_i of node N_i. This way, the process can authenticate ID and the hash key because computing $H'_{(HK)BS}$ is an elliptic curve discrete logarithm problem and attacker cannot find any information about ID and hash key. On the other hand, even if attacker successfully sends out

the security key r_i then also he cannot know the secret values x and k^* because of its trapdoor chameleon hash value. Only the authorized user can find out the secret key.

In addition, we claim that the proposed ACP is able to resist the attacks such as forgery attacks, legal node masquerading attacks, new node attack, replay attacks, man-in-the-middle attacks, and session key security attack as given below.

(i) **Forgery – Attack**: Say, an attacker tries to obtain the commutation values by eavesdropping on the communication channel as

$r'_i = r_i - (k_i + x)(f(m', k_iP) - f(m, k_iP))$ modq

$r'_i = k^* - f(m, k_iP)(k_i + x) - f(m', k_iP)(k_i + x) + f(m, k_iP)(k_i + x)$ modq

$r'_i = k^* - f(m, k_iP)(k_i + x)$.........................(4)

But it is not possible for him because the value of r'_i cannot be computed without secret key $(k_i + x)$.

(ii)Legal − Node − Masquerading − Attacks : Under this attack, the attacker has to deploy a pseudonode by removing the legal one. For this purpose, attacker has to obtain the commutation values by eavesdropping on the communication between nodes N_i and N_j. However, even if the attacker obtains the values of c_1P and c_2P from the authentication and key establishment phase, then also, deriving the legalized session key c_1c_2P is extremely difficult to obtain because of the security tool employed as ECDLP. In other words, the legal node N_j is well equipped with the security key $r_j(K + Y)$ provided by the base station $H_{(HK)BS}$ which attacker cannot retrieve.

(iii)New − Node − Masquerading − Attacks : Under this attack, when some sensor node is lost, it needs to be replaced by new sensor node N_{i+1}. To take advantage of this situation, the attacker may try to know the secrete keys x and k^* from the new node. But, this is not possible because the secret keys are provided by the base station to the new node with chameleon hash values $H_{(HK)BS}$ and r_{i+1} which attacker cannot compute.

(iv)Replay − Attack : In this attack, the adversary first eavesdrops on the communication between two communicating entities and then tries to impersonate the legal authentic message by simply replacing the other messages to the dedicated entity. For example, when an attacker transfers the message (N_i, c_1P, $r_i(K + Y)$, k_iP) to another node N_j , the attacker provides r_i for establishing authentication value $A_{(u)i}$. $A_{(u)i}$ is required for shared session key with the node to be connected. It is not possible for the attacker to obtain r_i without x and k^* which is the trapdoor secret value and available at the base station only. On the other hand, if the attacker sends the authenticated value $A_{(u)i}$ to node N_j , he can use the shared session key to authenticate, whether the connecting node is legitimate or not; if the node is legitimate then process is to proceed for the next step, otherwise discard, because the authenticated node uses up-to-date session keys c_1 and c_2 in order to apply the different strategies. Hence our proposed ACP successfully resists the replay attack.

(v)The − Man − in − the − Middle − Attack : This is one of the classical attacks that can be executed in any WSN environment. However, in any WSN equipped with our proposed ACP, the communication nodes can authenticate and establish the session keys between the users and the server. If attacker wants to mount the man-in-the-middle attack, he only knows the public keys c_1P and c_2P and wants to solve the ECDLP. Even if the attacker obtains the user's information (N_i , k_iP, $r_i(K + Y)$), then also the attacker cannot pass the authentication and key establishment phase, because he cannot compute the session key $A_{(u)i}$. Hence, our ACP can resist man-in-middle attack.

(vi)Session − Key − Security : Our proposed ACP is well equipped with the session key security feature. Since only the communicating parties know the session key c_1c_2P and hence are aware of the security of the session key, consequently, they can only verify the user of the message. The session key c_1c_2P is not known to anyone because random values c_1P and c_2P are protected by the ECDLP. Therefore, the proposed ACP provides session key security as an additional feature.

7 Applications

In this section, we will explain about the two different proposals based on the type of blockchain in detail.

7.1 Permissioned Blockchain

Consider a permissioned blockchain with n permanent validators. Here, the trap- door key k will be split into n shares using non-linear secret sharing. In this case, we do not need an ephemeral key since any block will be published by the fixed validators who already have the share of the main trapdoor key.

7.2 Public Blockchain

In a public blockchain like Bitcoin, anyone could join a network and publish a block, it is theoretically impossible to split the main trapdoor key and give shares to all the miners. By specifically considering Bitcoin where a pool of seven miners publish most of the blocks, the trapdoor key can be divided into seven shares and distributed among them. But, for a particular block, the publisher could be someone who is not among the top seven miners. Thus, we need an ephemeral trapdoor key to make sure that the initial proposer is also involved in the redaction process.

7.3 Other Applications of Chameleon Hash Functions

(i) Sanitizable Signatures: There exist some environments where the different users can access same data depending on their role. For example, consider a medical report in which few portions of the data remain confidential and only higher authorities can be able to access it. The authentication and integrity is usually achieved by using digital signatures. Sometimes there can be situations where an authorized third party should modify the content in the document. But, if the original signer of the document is not available or his/her key is expired etc., then authorized third party should be able to sign the document with a valid signature on behalf of original signer without contacting him/her. This can be achieved by using Sanitizable Signatures. The signer and the trusted party agree upon the mutable portions of the document before the modification such that the trusted party can modify only those portions. Consider a case where a trusted party wants to modify a document. The original signer of the document t will partition it into some n blocks. The signer selects some blocks out of n blocks and signs it by computing the chameleon hash using the public key pk of third party. Now, as the private key sk is with the third party only he can be able to compute hash collision and thus modify the selected portions of the block without changing the signature i.e., the signature is valid.

(ii)Wireless Sensor Networks (WSN): Sensors are used in Wireless Sensor Network (WSN) to collect the information about temperature, sound, etc., at different locations, process and send it back to the destination. Usually, a Multi-hop network contains n number of nodes in which each and every node contains one or more sensors. Sensor nodes can transfer the information to other sensor nodes via a base station. The information should not be altered during the transmission. If two nodes say n_1 and n_2 wants to communicate with each other, they must authenticate themselves before data transfer. Authentication can be achieved by using Chameleon hash function in which both the nodes n_1 and n_2 share a key k through secure channel such that only the key holders can compute the hash collisions.

(iii)Chameleon Signatures: In chameleon signature scheme, the signer of a particular message m uses chameleon hash function to compute the hash h. This hash can be signed by using any signing algorithm. For example, if user A wants to send a message to user B such that no other users should be able to know information about the message, then user A uses the chameleon hash function of user B, computes hash h and signs it using any digital signature algorithm. When user B receives the signature he can be able to verify that the signature is valid by computing hash collision. In this way, authentication is guaranteed and the signature is non-transferable.

8 Conclusions

Collecting data from the surrounding environment becomes easier thanks to the strong development of sensor technology. Thus, greatly improving people's lives due to the benefits that wireless sensor networks bring. However, the current WSN architecture is based on the server/client model, so there are still many limitations, especially scalability, security, and distributed data storage. With outstanding advantages in the emergence of Blockchain technology, this is considered an effective solution to overcome the above limitations. In this article, we have provided an overview of the benefits and challenges of applying Blockchain technology to WSN. Finally, we can show, the participation of Blockchain technology will solve the limitations of WSN. At the same time, it also creates quite many new challenges. Therefore, we still need more research to investigate the implementation of Blockchain technology in the WSN network.From the aforesaid sections, we conclude to say that our proposed ACP using the double trapdoor function and whose security is based on ECDLP is best suited to any WSN environment. 4e reason for being more secured is that it can resist many known attacks such as masquerading, replay, man-inthe-middle, and forgery attacks and has a special feature known as session key security.

References

1. A. Abduvaliev, S. Lee, and Y.-K. Lee, "Simple hash based message authentication scheme for wireless sensor networks," in Proceedings of the 9th IEEE International Symposium on Communications and Information Technology (ISCIT '09), pp. 982–986, Incheon, South Korea, September 2009.
2. Y. Zhou, Y. Zhang, and Y. Fang, "Access control in wireless sensor networks," Ad Hoc Networks, vol. 5, no. 1, pp. 3–13, 2007.

3. N. Koblitz, “Elliptic curve cryptosystems,” Mathematics of Computation, vol. 48, no. 177, pp. 203–209, 1987.
4. H.-F. Huang, “A novel access control protocol for secure sensor networks,” Computer Standards and Interfaces, vol. 31, no. 2, pp. 272–276, 2009.
5. H.-S. Kim and S.-W. Lee, “Enhanced novel access control protocol over wireless sensor networks,” IEEE Transactions on Consumer Electronics, vol. 55, no. 2, pp. 492–498, 2009.
6. J. Shen, M. Sangman, and C. Ilyong, “Comment: enhanced novel ACP over wireless sensor networks,” IEEE Transactions on Consumer Electronics, vol. 56, no. 3, pp. 2019–2021, 2010.
7. P. Zeng, K.-K. R. Choo, and D.-Z. Sun, “On the security of an enhanced novel access control protocol for wireless sensor networks,” IEEE Transactions on Consumer Electronics, vol. 56, no. 2, pp. 566–569, 2010.
8. H. Lee, K. Shin, and D. H. Lee, “PACPs: practical access control protocols for wireless sensor networks,” IEEE Transactions on Consumer Electronics, vol. 58, no. 2, pp. 491–499, 2012.
9. H. Krawczyk and T. Rabin, “Chameleon hashing and signatures,” in Proceedings of the Network and Distributed Systems Symposium (NDSS ’00), pp. 143–154, San Diego, Calif, USA, February 2000.
10. C.-Y. Chen, A. D. Yein, T.-C. Hsu, J. Y. Chiang, and W.-S. Hsieh, “Secure access control method for wireless sensor networks,” International Journal of Distributed Sensor Networks, vol. 2015, Article ID 261906, 6 pages, 2015.
11. X. Chen, F. Zhang, W. Susilo, and Y. Mu, “EYcient generic on-line/oZline signatures without key exposure,” in Applied Cryptography and Network Security, vol. 4521 of Lecture Notes in Computer Science, pp. 18–30, Springer, Berlin, Germany, 2007.
12. A. Stanciu, “Blockchain based distributed control system for edge computing,” in 2017 21st International Conference on Control Systems and Computer Science (CSCS), pp. 667–671, IEEE, 2017.
13. A. Banafa, “Iot and blockchain convergence: benefits and challenges,” IEEE Internet of Things, 2017.
14. E. Karafiloski and A. Mishev, “Blockchain solutions for big data challenges: A literature review,” in IEEE EUROCON 2017-17th International Conference on Smart Technologies, pp. 763–768, IEEE, 2017.
15. X. Chen, F. Zhang, H. Tian et al., “EYcient generic on-line/offline (threshold) signatures without key exposure,” Information Sciences, vol. 178, no. 21, pp. 4192–4203, 2008.
16. M. Q. J. S. L. Law, A. Menezes, and S. Vanstane, “An efficient protocol for authenticated key agreement,” Codes and Cryptography, vol. 28, no. 2.
17. J. M. Pollard, “Monte carlo methods for index computation mod p,” Mathematics of Computation, vol. 32, no. 143, pp. 918–924, 1978.
18. A. J. Menezes, T. Okamoto, and S. A. Vanstone, “Reducing elliptic curve logarithms to logarithms in a Snite Seld,” IEEE Transactions on Information Peory, vol. 39, no. 5, pp. 1639– 1646, 1993.
19. G. Frey and H.-G. Ruck, “A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves,” Mathematics of Computation, vol. 62, no. 206, pp. 865–874, 1994.
20. I. A. Semaev, “Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p,” Mathematics of Computation, vol. 67, no. 221, pp. 353–356, 1998.