Privacy Protected IoT-Blockchain using ZKP for Healthcare application

R. Yugha * **S. Chithra** ** **N. Bhalaji** *** **S. Karthika** ****

* *Department of Information Technology, Sri Sivasubramaniya Nadar College of Engineering Affiliated with Anna University, Chennai, Tamil Nadu (Corresponding author E-mail: ryugi0728@gmail.com)*
** *Department of Information Technology, Sri Sivasubramaniya Nadar College of Engineering Affiliated with Anna University, Chennai, Tamil Nadu (Email: chithras@ssn.edu.in)*
*** *Department of Information Technology, Sri Sivasubramaniya Nadar College of Engineering Affiliated with Anna University, Chennai, Tamil Nadu (Email: bhalajin@ssn.edu.in)*
**** *Department of Information Technology, Sri Sivasubramaniya Nadar College of Engineering Affiliated with Anna University, Chennai, Tamil Nadu (Email: skarthika@ssn.edu.in)*

Abstract: In recent years, the concept of the Internet of Things (IoT) is making a 'Thing' in real-world life to be smart by designing the devices to be pervasive, mobile and wearable. The IoT applications may be supported by big data or cloud computing for data analysis. The data analytics has to be performed remotely on the data received from the IoT device. The user has to send highly sensitive personal data to centralized devices for analysis which may lead to serious risks for privacy and security. This can be addressed by IoT systems maintained as peer-to-peer (P2P) systems incorporated with Blockchain technology. Mutual authentication has to be performed to improve the security and trust of IoT applications on a peer to peer basis. This paper addresses two challenges: (i) Mutual authentication is a decentralized P2P IoT environment addressing the tradeoff between privacy and security using Zero-Knowledge Protocol (ZKP) Protocol. ii) The data storage to be secure and for handing it in transparent P2P mode, the Blockchain technology is used for IoT healthcare system. This ZKP protocol has been proved to satisfy the properties of Zero-Knowledge proof systems. The algorithm has been proved to be optimized with respect to space which is one of the limitations of sensor nodes in IoT devices.

Keywords: Internet of Things, Zero-Knowledge Protocol, Authentication, Blockchain, Cryptography

1. INTRODUCTION

The Internet of Things (IoT) is the network of physical "Things" embedded with electronics, software, sensors, and network connectivity, which enable these objects to collect and exchange data. The things, animals, people or any entity are provided with a distinct and unique identifier. This unique identifier is used for transferring the data collected over a network for analyzing the data for automation without requiring any human-to-computer interaction or human-to-human interaction. IoT has evolved as a result of the convergence of many modern domains such as wireless technologies, micro-electro mechanical systems (MEMS) and the Internet.

The Internet of Things is made up of several nodes that are also known as participating entities referred to as a 'thing'. It can be a person with a heart monitor implant or anybody parameter measuring sensor, a farm animal with an electronic chip or even a tracker that can track the whereabouts of an animal if it is within the field, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an IP address and uniquely identified along with the ability to send or receive data over a network. So far, the Internet of Things has been most closely associated with Machine-to-Machine (M2M) communication in manufacturing and power, oil and gas utilities. The products that are built withM2M capabilities are often referred to as being 'smart'.

One of the important factors in the development of IoT is the increase in IPv6 address space. Every 'thing' on the planet can be assigned an IP address. An increase in the number of smart nodes, as well as the amount of upstream data the nodes generate, is expected to raise new concerns about data privacy, data sovereignty and security. For instance, an attacker can gain access to sensitive data or perform a reset mechanism on a device or a sensor that controls the health system of a person by masquerading as a legitimate user. This requires a stringent authentication mechanism without affecting privacy.

The authentication of the IoT device has to be verified for sensitive sensor data communication for the conventional ZKP system. On Internet, users are authenticated with their passwords. The browsers authenticate the users using protocols such as the Secure Socket layer (SSL). However, password-based IoT-scale authentication is challenging compared to password-based Internet-scale authentication. The various security challenges in IoT have been studied since its inception in securing devices that perform life-critical functions and comply with stringent regulatory requirements. This paper examines the constraints and security challenges posed by IoT-connected devices and the Zero knowledge-based authentication approach for addressing them.

Knowledge-based authentication (KBA) authenticates a user based on the knowledge of their personal information, substantiated by a real-time interactive questions and answer process. This technique employs the use of secret or personal questions. The questions can be either static or dynamic. In the static version, the end-user can choose the question and its answer. The user is authenticated with the same set of question and answers. In the dynamic KBA, the user is completely unaware of the questions that would be posted to him. All the question and answer pairs are chosen by how the user has previously interacted or used the system or from the public records. Username/passwords (Conklin et. al, 2004) and Challenge-response protocols are commonly used in KBA approach. The most commonly and widely used keyword / passphrase-based mechanisms are simple but succumb to masquerading attacks by the verifying entity. In authentication terminologies, the prover is the person who requests for service and the verifier is the service provider who has to verify the details of the prover. The problem with this technique is that if a password is supplied by the prover for verification to the verifier who authorizes it, the verifier can use it to masquerade or fake the prover in other upcoming session exchanges.

In challenge-response protocols, the prover does not directly hand over the secret to the verifier but is required to undergo a series of challenges and respond to it. The responses given by the prover to the verifier must be in such a way, that they show that the prover possesses the secret. This scheme can address and resist certain third-party attacks. However, the disadvantage of this system is that during the course of these challenges and responses, a part of information about the secret is exposed. The verifier could use this loophole and exploit this mechanism by choosing challenges called "chosen text attacks" to find out the secrets.

To enhance the security aspects of Blockchain technology (Ethereum) is implementing by Zero-Knowledge Proof System of AZTEC Protocol (Anonymous Zero-Knowledge Transactions with Efficient Communication) to improve its transactional privacy so that it could be used for various applications. Blockchain is a technology that provides a secure and distributed mechanism to record transactions and acts as a reliable alternative for achieving the desired security of information exchange and privacy. Blockchain provides the advantages of trust, security and transparency. The transparency of blockchain is restricted to enhance privacy. The ZKP is incorporated with Blockchain technology to address the tradeoff between the privacy and security. The IoT data will be stored in the Blockchain. Here, ZKP plays a major role while the entities are sharing the data in the IoT healthcare applications. The ZKP provides the P2P authentication for all the entities involves in the application.

The property of Zero-Knowledge Protocols (ZKP) where the "*truth of an assertion is proven without revealing any information about the secret itself*". This algorithm based on discrete logarithms is used to implement ZKP and is designed to be an optimized one to address the resource constraint issues of sensor nodes in IoT Healthcare applications. For instance, this application tries to provide credential verification using AZTEC protocol. AZTEC Protocol enables us to prove certain information to anyone without revealing the exact information and also without leaking any data. All the information is converted into notes and hashed using the public key which is then sent along with the signature to verify if it is right without exactly revealing it.

This paper has been organized as follows: Section 1 introduces the Internet of Things and discusses the challenges of IoT. The authentication mechanisms have been discussed in Section 2. Section 3 explains the architectural details of IoT. The proposed authentication scheme has been illustrated in Section 4. Sections 5 and 6 discuss security and how it is being addressed.

2. LITERATURE REVIEW

IoT being one of the visionary technologies aims at bringing some feasible; real-time applications e.g., smart home, building automation, smart city, and e-health. All these applications require preventing leakage of sensitive information and other harmful attacks by authentication of nodes and secure transmission of data. The standard IP-based security solutions become unsuitable as they are power-consuming and computation intensive. Hence, there is a necessity for lightweight security mechanisms which are tailored for constrained environments to fulfill the research gap in IoT Yugha and Chithra (2020).

With its unusual combination of characteristics, such as decentralization, immutability, and accountability, Blockchain technology has great potential to foster different sectors. We believe that the use of this technology in science and academia has a lot of potential. The Blockchain is considered a distributed database that is organized as a list of ordered blocks, where the committed blocks are immutable. Smart contracts enabled by Blockchain technology allow more complex processes and interactions, establishing a new paradigm of potentially infinite applications. Hence, it is necessary to ensure all these transactions are anonymous and privacy is maintained.

The security protection for IoT in its area can be provided by establishing a secured connection through a VPN tunnel, secured connections using HTTPS protocol or using wireless network security approaches such as Wi-Fi Protected Access (WPA) protocols. Most IoT applications have their solution for communication and lightweight authentication Aufner (2020). Lack of standards in IoT communications is one of the main reasons for the existence

of several communication and authentication solutions. DTLS is an adaption of the widespread TLS protocol, used to secure HTTPS, for unreliable datagram transport Kothmayr et al. (2013). The author introduced the fully two-way authentication security scheme for the Internet of Things (IoT) based on existing Internet standards, specifically the Datagram Transport Layer Security (DTLS) protocol. In Yugha and Chithra (2019), the author proposes the attribute trust evaluation for providing security in the IoT networks. In this article, trust management plays an important role in healthcare applications.

It has been proposed Hummen et al. (2013, 2014) that the delegation-based authentication and authorization architecture has reduced the requirements of resources of DTLS- protected communication for constrained devices. Additionally, the delegation architecture naturally provides authorization functionality when leveraging the central role of the Delegation server in the initial connection establishment and does not require the assumption that the gateways are to be fully trusted. In Kittur and Pais (2020), Multiple digital signatures are verified in this system. The ZKP protocol must meet the properties of Completeness, Soundness and Zero-knowledge. There are certain conventional and traditional ZKP-based systems constructed on mathematically and computationally intensive problems such as factorization Feige et al. (1988); Fiat and Shamir (1986) and discrete logarithm Balasubramanian and Koblitz (1998), ZKP based on multiplicative groups such as Zn. Elliptic curves over finite fields, which in many ways are found to be secure, effective, efficient and analogous to other groups are found to hold a great edge in cryptography Hummen et al. (2013); Bellare et al. (2009).

In Karthigaiveni and Indrani (2019), an efficient authentication mechanism for IoT applications is to prove secure communication between the users. This Scheme proposed two-factor authentication schemes by using Elliptic Curve Cryptography which provides high security with minimum computational cost. Concerning related progress of Zero-knowledge protocol primitives and comparing the effectiveness and secure features of the elliptic curve version against that of the multiplicative groups for protocols that are based on discrete log and factorization problems in Chaum et al. (1986); Almuhammadi et al. (2004). The Elliptic Curve Discrete Log Problem (ECDLP) is proved and concluded to be more secure than protocols that are based on the elliptic curve factorization problem. The additional advantage of using ECC is its small key size. In the proposed work, the authentication is based on ZKP using ECC.

3. IOT ARCHITECTURE AND REQUIREMENTS

The main components of IoT systems are Things/devices, users, applications, cloud and gateway. The IoT architecture is explained in Figure 1. The devices that can percept the surroundings and measure the parameters related to sensing the environment. For instance, the data related to sensing home, building, land or body are transmitted to devices such as mobile phones or laptops in a remote location over the Internet. Communication plays a major role in IoT which requires secure data transmission assurance. Hence, the authentication process has to be carried out mutually at both endpoints of communication. The transmitting device has to ensure that the device to which it is transmitting its data is the right device. In this paper, the term Prover and Verifier is used to mention the nodes to be involved in the authentication process.

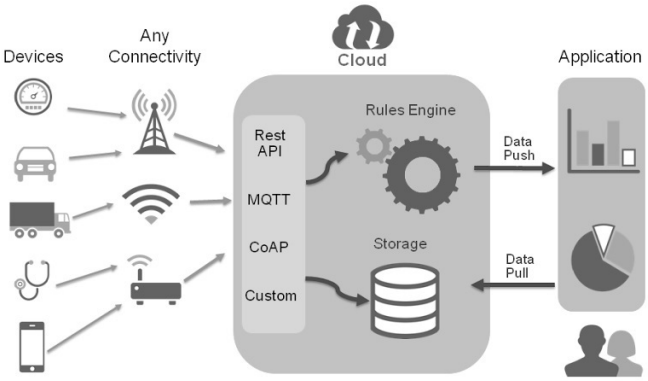

Fig. 1. IoT architecture

The participatory entities in IoT are designed to operate autonomously in the above-stated environments with energy constraints. However, in major applications Internet of Things are deployed to be utilized by multiple users in different hierarchies which demands multiple access rights and authentication schemes to be prevalent among them. For example, a critical healthcare application relies on accurate and timely human physiological measurement. If the end device attached to collect the data is encountering attacks like Man-in-the-middle, Replay and Denial of Service then it should be realized by both the device and the centralized collecting authority to protect and mitigate against them. Thus, the security threats raise huge concerns in the Internet of Things and emphasis the need for strong security schemes to combat the threats.

4. PROPOSED SYSTEM

4.1 Blockchain for Healthcare application

It has been almost a decade since Blockchain technology, a distributed peer-to-peer linked structure was described by Satoshi Nakamoto. A block records several transactions, similar to pages in a book and the number of transactions on a block can vary from blockchain to blockchain. These transactions are hashed i.e strings of numbers and letters. This is done to include information from the current as well as previous transactions. The order of hashes cannot be changed thereby forming a Chain. As a result, the Blockchain structure can keep a reliable and auditable record of all transactions.

The Blockchain must be always considered as a distributed append-only time-stamped data structure in theory. The need for a trustworthy authority is removed because Blockchain helps us to build a peer-to-peer distributed network in which no entrusting participants will communicate with each other in a verifiable manner. This is achieved by a set of interconnected mechanisms. The proposed ZKP with Blockchain is implemented using the AZTEC (Anonymous Zero-Knowledge Transactions with Efficient Communication) protocol that describes an intertwined

system of zero-knowledge proofs. These proofs define the pathway that is mindful of privacy and supports confidential transactions. The AZTEC protocol is designed for use within all Blockchain protocols that support Turing-complete general-purpose computation. The protocol also enables confidential cross-asset trades for digital assets defined on the same Blockchain platform via confidential, zero-knowledge decentralized exchanges. The next section describes the implementation of ZKP which is combined with Blockchain technology for the IoT healthcare systems. Currently, the patient records are electronically stored by an organization that creates an account for all the health data of a patient. But in blockchain technology, patient records can be stored globally on the blockchain network.

The blockchain-based framework is the implementation in healthcare that aims to create a blockchain that validates patients' credentials. Each citizen has a blockchain-based identity that is associated with their Electronic Health Record (EHR). Any change in the EHR data reflects in the blockchain system. This system is immutable and not prone to any malicious activities. Because, any update in the EHR will be assigned a timestamp and stored in a separate block. This system is highly secure and auditable that can make any modifications in the healthcare records.

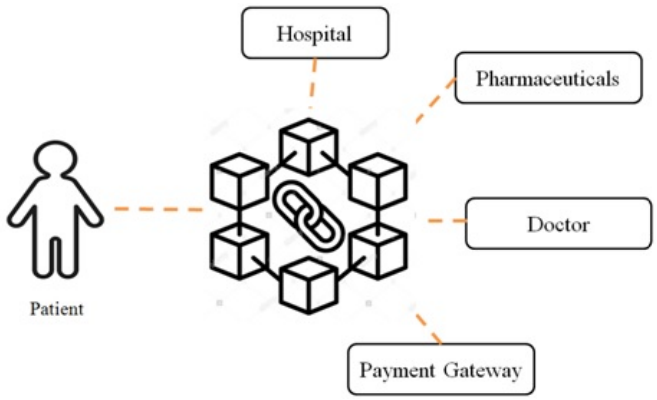

Fig. 2. Flow diagram of the proposed system

In figure 2, the patient EHR shares the many entities from blockchain like Doctor, payment gateway, Hospital and pharmaceuticals. In the block, entities are used to shared the information by AZTEC protocol based authentication which is private or public after verifying the credentials such as smartcard. Every transaction is also appended to a block and is assumed that it is a true transaction, being the owner the one responsible for adding/removing devices. In Ethureum network, blocks will be created depends upon the number of transactions. The block is created for average of 2800 transactions ZKP based system for blockchain is exist to blockchain adoption in healthcare and also improve security, fraud prevention and reduces duplication.

For consider the scenario of IoT healthcare application as in the figure 2, the Pharmacists need the information about the patients in the Bockchain network. So, AZTEC protocol based authentication provides between the P2P system for admin and the pharmacists. After verifying the credentials between them and then sharing the information about the patients. The next subsection is describes about the ZKP authentication using the Blockchain.

4.2 Zero-Knowledge Proof (ZKP) Authentication

Authentication is a key issue for IoT systems that involve critical information sharing Chaum et al. (1986). It is necessary to establish the credentials of the node and prove that it is whom it claims to be" without affecting its privacy (Balopoulos T (2008), Wu C et al (2019)). The authentication of a node can be verified by the verifier only when the credentials of the node are known. This may reveal secret information. However, there is a challenge that the authentication has to be verified without the credentials. Hence, Zero-knowledge authentication does not verify the credentials but verifies the possession of the credentials. The proposed authentication scheme is a public key-based authentication in which the ownership of the respective private key and the public key value are verified without loss of secret key information.

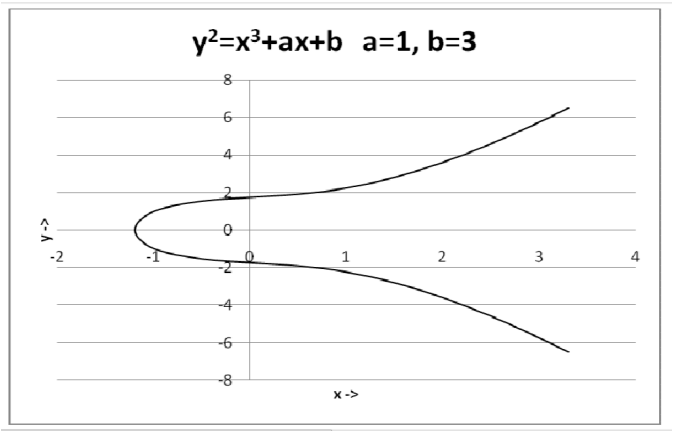

Fig. 3. Sample Elliptic curve

Zero-Knowledge protocol proves that the requestor possesses the private key for the public key being communicated without any part of the private key being exposed or revealed. The concept of ZKP was first introduced by Goldwasser and has been employed in many authentications and identification protocols. The ZKP system guarantees authentication without giving any knowledge of the private key. Because, the strength of ZKP with Elliptic Curve Cryptography (ECC) having the advantage of small key size of ECC.

The node requesting for service (from now on referred to as the prover) would have an Elliptic Curve denoted by 'E' which is defined over a Finite Field Fq, where q is known as the prime or prime power. Figure 3 shows an Elliptical curve for equation 1 as follows.

$$y^2 = x^3 + ax + b \tag{1}$$

for a = 1 and b = 3.

The elliptic curves obtained would be different and vary for different values of 'a' and 'b'. All points satisfying the above equation plus a point at infinity would lie on the elliptic curve. The private key, which is known only to the prover, is a random number r, such that, r ε Z, where Z is the set of integers. The public key is obtained as a

product of the private key and the generator G, where G ε E, in the elliptic curve. The generated (x, y) pairs for the equation are (1,0), (2,2), (2,3), (3,1), (3,4), (4,3),(4,2). Any of these points can be chosen as Generator point G. For each execution cycle, the value of g is randomly chosen. The public key P is obtained such that the product of r and G which is nothing but rG= P.

The prover communicates to the service provider node (from now on referred to as the verifier), the public key P, E and G. The steps in the authentication process are now explained.

(1) A random number n, is chosen by the prover ($2 \leq n \leq \#$ G-1), who then calculates witness value W= nG and sends W to verifier.
(2) A challenge c is chosen by the verifier which is 1 or 0 and the same is sent to the prover.
(3) The response x = n + cr is calculated by the prover, which is then sent to verifier.
(4) The verifier accepts only if the following equation satisfies, xG = W + cP.

Case 1 : Challenge = 0 If the verifier chooses the challenge value to be 0, the prover computes the response as x = n (substituting c = 0 in x = n+cr). The verifier can verify the response, by substituting the x value in the equation (xG - cP). As c is 0, the equation computes as xG = nG = W.

Case 2 : Challenge = 1 If the challenge value is 1, the prover computes the response by substituting c=1 in the equation x = n + cr, and the response would be x = n + r. The verifier can verify the response, by substituting the x value in the equation

$$xG = W + cP \tag{2}$$

$$xG = (n + r)G = nG + rG = W + cP \tag{3}$$

The whole process (steps i to iv) is repeated for k number of times where k decides the soundness of the algorithm. The challenge value used is 0 or 1. After k iterations without rejection, the probability of any cheating is 2^{-k}. This implies if k is large enough, that can make the probability of cheating sufficiently small. As long as k is large, the algorithm is to prove as sound. The Further section is illustrates about the implementation of the ZKP with blockchain technology.

5. IMPLEMENTATION

5.1 Blockchain Implementation for IoT Healthcare applications

This system is implemented using Javascript, JSON (JavaScript Object Notation), NPM (Node Package Manager) and Solidity. JavaScript, often abbreviated as JS, is a high-level programming language. It is a just-in-time compiled multi-paradigm. It has curly-bracket syntax, dynamic typing, prototype-based object orientation and first-class functions. JSON also is an open standard file format, and data interchange format, that uses human-readable text to store and transmit data objects consisting of attribute-value pairs and array data types (or any other serializable value). It is a very common data format, with a diverse range of applications, such as serving as a replacement for XML in AJAX systems. NPM is the JavaScript programming language's package manager. For the JavaScript runtime environment Node.js, NPM is the default package manager. It consists of a command-line client, also known as npm, and the npm registry, an online directory of public and paid-for private packages. Solidity is a high-level object-oriented language for creating smart contracts. Smart contracts are a program that controls how accounts behave in the Ethereum state.

On testing the performance of the algorithm, it is implemented in an IoT application with an Arduino board connected to reading pulse rates from sensors. The experimental setup of the IoT application is shown in Figure 4. The pulse sensor is interfaced with this Micro-Controller Unit (MCU) and it is programmed through Arduino IDE.

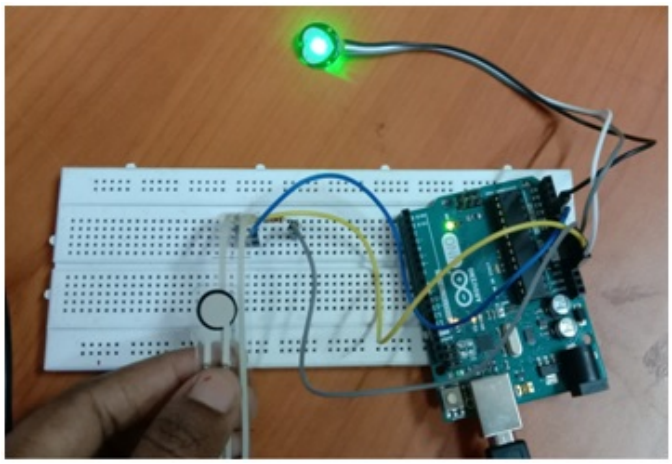

Fig. 4. Experimental setup of IoT application to healthcare

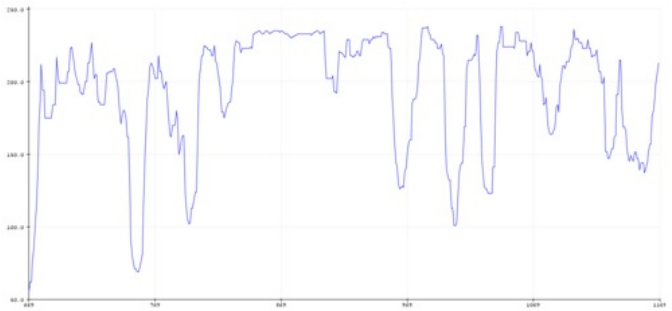

Fig. 5. Screenshots showing results of implementation for ZKP in IoT

The sensor used here is a pulse sensor interfaced with the node MCU Wi-Fi module. The sensor reads the pulse rate in bpm (beats per minute) and then when the user wants to view the data, the authentication is carried out. The user can read the level of pulse rate only when authenticated. The results of authentication verification are shown in Figure 5.

5.2 Implementation of ZKP for IoT Healthcare applications

The Zero-Knowledge Protocol has been implemented using socket programming in "C language". The sequence of operations between these two nodes is shown in Figure 6.

The screenshots for key generation and the Prover-Verifier communication are given in Figure 7 and Figure 8.

The proposed authentication scheme has been tested by constructing a node to node network with fifty nodes and a value of k = 10, which gives 2-k as 0.0009, which is a sufficiently low probability of fraud in verifying the possession of the private key. The value of k can be increased to provide greater authenticity. The process of authentication is implemented taking into consideration the memory requirements of the sensors used in IoT applications. The sensor nodes have to authenticate the sink node before transmitting the data. In this case, the sensor node would serve as a verifier and the sink node as a prover. However, mutual authentication can also be performed.

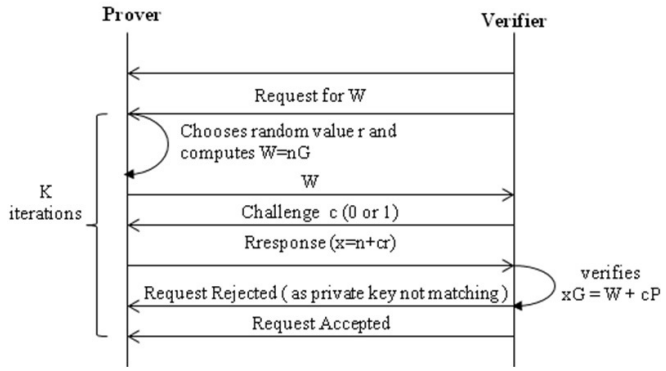

Fig. 6. ZKP Implementation

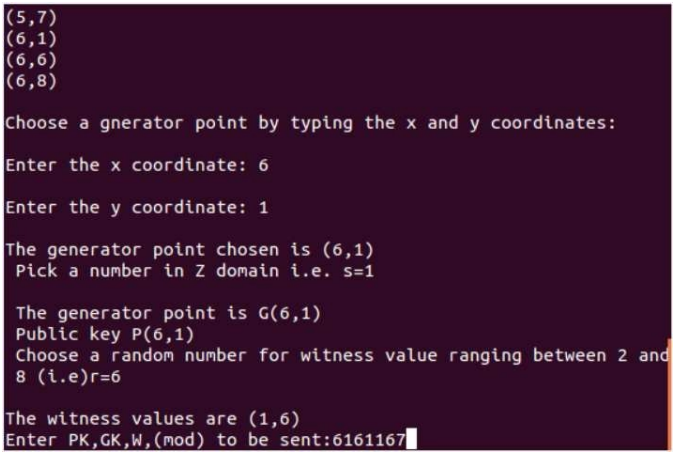

Fig. 7. Screenshot showing Key Generation

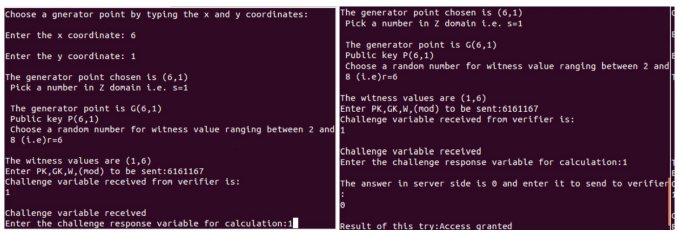

Fig. 8. Screenshot showing Prover-Verifier communication

6. RESULTS AND ANALYSIS OF THE PROPOSED SYSTEM

This section discusses chosen ZKP protocol and verifies the truth of the assertion that the private key possession is proven without exposing or giving away any information about the secret. The protection provided against various security attacks on node authentication is also discussed.

6.1 Blockchain implementation results

Deploying of contracts into the Ethereum Blockchain: Using yarn migrate, all the initial contracts are migrated and added to the blockchain so that these can be used to verify user credentials as shown in figure 9.

Fig. 9. Initial Migration

Mapping the transaction with the Blockchain: We can see that the transaction ID of block number 20 and transaction hash of IDegree are the same indicating that this contract has been successfully added to the blockchain as shown in figure 10 and figure 11.

Adding new blocks for verification: After the initial contracts have been successfully deployed, our flow.js file is executed and as a result of which, new blocks are added to the chain. A total of 29 blocks are added and 21 after the initial migration and 8 after running flow.js which are for the verification of the user credentials as in figure 12.

Credential Verification of the user: All the credentials are provided and the corresponding note value is given which is then hashed using the public key in figure 13. If any verification is to be done, the user sends the signature and proof data to the concerned authority which verifies it. If the credentials match the eligibility, SUCCESS is the output shown else an ERROR output is thrown saying verification failed.

6.2 ZKP Proof

The completeness, soundness and zero-knowledge properties have to be satisfied by the ZKP protocols. The ZKP protocol in this scheme is based on classical works of Fiat & Shamir Kittur and Pais (2020) and Chaum et al. (1986); Feige et al. (1988) as demonstrated in its elliptic curve

Fig. 10. Transactions of initial contracts

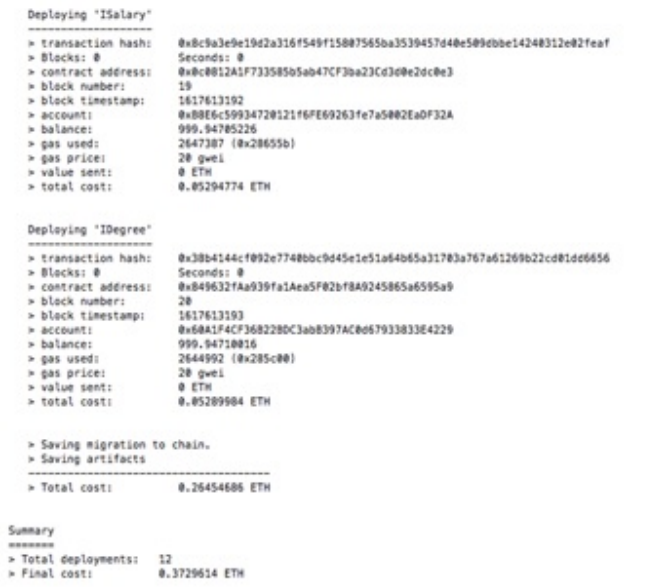

Fig. 11. Matching transaction hash

Fig. 12. New blocks added to the blockchain

version Balasubramanian and Koblitz (1998). The proofs are analogous to that of the classical schemes and are as follows.

Fig. 13. User Verification

Completeness: If suppose the prover possesses a secret s;in all cases (c = 0 or 1) the prover provides the verifier with a value of x where x= n (if c = 0) or n + r (if c = 1), which will be accepted by an honest verifier with probability = 1.

Soundness: If there exists a node A which is not the prover but waits to pose as a prover by impersonation, then A guesses the challenge to be 1 or 0 and can do the any of the following in order to make the verifier accept is as the prover:

Case 1: A guesses c = 0 and sends W = nG. Verifier sends challenge as 0. A sends x = n to verifier, who will compute (xG = W + cP = W + 0 = W) and accept A. Verifier sends challenge as 1. A has to send n + r to the verifier. A does not know r and cannot sent n + r.

Case 2: A guesses c=1 and sends W = nG-P. Verifier sends challenge as 1. A sends x = n to verifier, who will compute (xG - cP = nG - P = W) and accept A. Verifier sends challenge as 0. A has to send n – r in order to satisfy the verifier. A does not know r.

The probability of a node being able to guess the challenge value as 0 or 1 is 2^{-k} where the challenge-response is carried out for k number of iterations. The value of k has to be large enough to make the guessing difficult. The error probability for different values of k is given in Figure 14.

Zero Knowledge Property: This can be argued as explained. The values G and P are public. The values which the verifier is aware of for all iterations are W and x. If challenge is 0, then x = n, and information about 'r' is not known to verifier. If challenge is 1, then x = n + r is computed and sent by prover and the value of 'r' is not revealed to verifier.

Given knowledge of (E, G, P), it is computationally infeasible for A to determine s as it is based on the Elliptic Curve Discrete Log Problem (ECDLP). The value of r is different and changes for every cycle. Therefore, no additional information is exposed to verifier pertaining to the secret s, and hence the zero knowledge property is satisfied by this scheme.

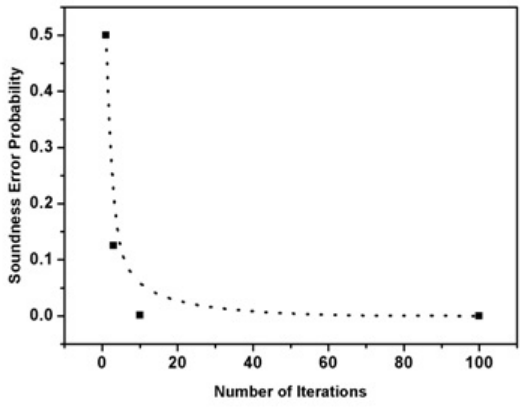

Fig. 14. Soundness Error Probability vs No. of Iterations

Privacy: One of the important issues related to IoT is to find a suitable node to maintain the credentials of all the nodes. The credentials cannot be maintained centrally because of the availability of less storage space of the sensor nodes. The use of ZKP protocol avoids the maintenance of credentials with a central node and the dependence on certification authorities. Hence privacy is maintained on larger scales over time.

Time Complexity: The steps for implementation are given in the form of a Table 1 for both Prover and Verifier.

The algorithm execution begins from step 1 to 4 and is executed once. The steps 5 and 6 are iterated n times until the verifier is convinced that the prover possess the key. The algorithm has a time complexity which is determined to be O(n). However, the value of n can be decided by the user based on the security requirements.

The time complexity of the Feige-Fiat-Shamir proof of identity Feige et al. (1988) and Graph Isomorphism is also O(n). However, in the first case, there is 50% chance of masquerading. The prover or the verifier themselves can pose as an imposter which might lead to either of them illegally claiming the information. The public key is generated by a third party. Also, another major drawback is that the verifier is able to recover a part of the data possessed by the prover and this violates the rules of ZKP, where there are chances of the key being shared and misused.

In the second case, the algorithm might be compromised by brute force technique. This is because the combinations of certain number of nodes can be attacked on brute force basis. If this has to be avoided, the number of nodes in the graph needs to be increased, which will lead to increase in file size, memory requirement, processing speed and computational overhead. The time complexity of ZKP algorithm based on the concept of ECC is O(n) and it does not compromise the Zero Knowledge property.

Space Complexity: The sensors used in IoT are memory constraints. This algorithm has been implemented using socket programming in 'C' language. The size of the source file is around 5 KB. The CPU usage of this algorithm is dependent on the number of iterations of the algorithm. However, the algorithm uses only a small amount of CPU because limited number of iterations is acceptable as it provides enough zero knowledge security. Also, the algorithm uses simple computational methods like arithmetic operations. The memory requirement of the algorithm is also found to be small which can be used in microcontrollers such as omega and also in the sensors/high-end sensors having the required memory space.

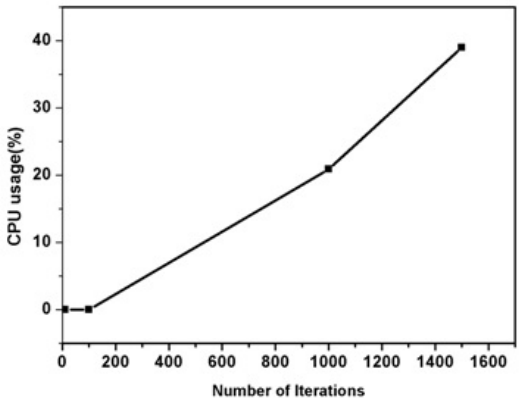

Fig. 15. The percentage of CPU utilization VS No. of Iterations

The computation time required is described in Figure 15 showing that it is proportional to the number of iterations. However, if the number of iterations is more, the percentage of CPU usage is high initially and it gets reduced on successful completion of those iterations.

Additionally, the interaction between the prover and the verifier comprise of simple challenge response interaction which requires small amount of CPU utilization so that the memory usage is less.

The comparative analysis of the Zero-Knowledge Protocol (ZKP) has been depicted in Table 2. An Efficient Identification Scheme is proposed by (Liu, P. Ning (2008)), which is used for proving the proof of identity. This scheme is closely related to the notation of digital signatures and uses the property of Feige-Fiat-Shamir proof of identity. The Optimized implementation is adopted in this scheme and executed with the polynomial function of time $O(|N|^2)$ and requires more memory space for computations.

In Chaum et al. (1986), the scheme is formulated to use proof of knowledge and satisfy the properties of soundness and completeness. However, this scheme does not focus on mutual authentication and optimization. The polynomial-time reduction for P and NP-complete problems has been applied.

A novel algorithm has been introduced by Almuhammadi et al. (2004), which is based on ZKP and accumulated hashing to provide secure authentication for IoT mobile devices. The scheme is based on a one-time token generation which is a pseudo-random number. The computational complexity is very low and requires less memory. However, mutual authentication has been compromised. An attribute-based credential scheme has been introduced for authentication IoT systems (Balopoulos T et al(2008)).

This scheme uses the property of elliptic curves, ZKP, blind signature, selective disclosure and randomization. This scheme is not supportive of mutual authentication.

The proposed scheme provides support for mutual authentication and optimization using the ZKP protocol. This scheme satisfies the properties of ZKP like soundness, completeness and zero-knowledge. The time complexity is observed to be O(n) where n is the number of iterations that can be set as a policy by the user. Also, this scheme occupies less storage space and hence it is well suitable for IoT systems that use resource constraint devices.

From the results of the AZTEC protocol, able to see how the contracts were first deployed and using zero range proofs and we were able to verify the credentials. As a result of this, our system can

- Prove that they are underage or are of legal age to vote.
- Prove that their location is verified. They can prove that they live in a particular demographic area without revealing their exact location.
- Prove that their annual salary is within a certain range without disclosing it. This can help them in getting bank loans without disclosing full information.
- Disclosing that you have certain credentials without actually showing them what they are. For example, having a driving license and knowing how to drive a car without showing the license number.
- Proving that you have a certain level of education (high school, bachelor) or proving that you have done masters without telling them which are your majors or in which university.

6.3 Security Analysis

As the mathematical proof of the proposed algorithm is clearly explained in Section 4, some problems may still exist, such as the inappropriate and incorrect usage of the private key by the user and various attacks on the requesting and serving nodes.

If a node tries to impersonate other nodes, the challenge values may differ so that the attack is detected and access is denied. It is shown in Figure 16.

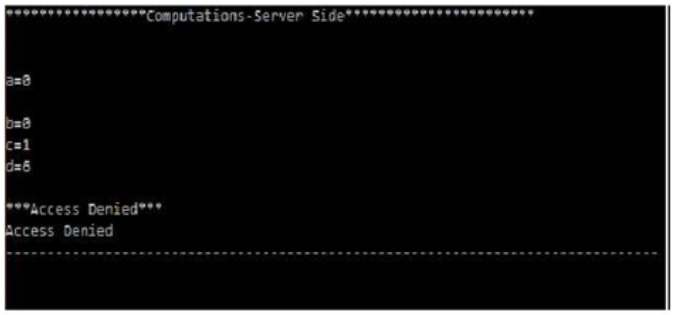

Fig. 16. Demonstration of Impersonation attack

The proposed methodology can withstand a few of those attacks (Zhao K, L. Ge (2013)). The attacks and the solution to address those attacks are given in Table 3. The proposed authentication scheme is strong against a few of the security attacks in IoT. It is also indirectly

Table 1. Implementation steps of the algorithm

Steps	Prover	Verifier
1	Request for access	Receive Request message
2	Waiting for keys Request	Request for keys
3	Generates private key and public key Pk(E,P,G)	Waiting for private key and public key
4	$P_k(E, P, G)$ is shared and also sends W to verifier	P_k and W is received
5	Waiting for Challenge variable (c)	Verifier chooses Challenge variable (c) and sends to prover
6	Computes x=r+cs and sends x	Accepted if xG = W + cP

can address other attacks like fake node attacks, Denial of Service (DOS) attacks, acknowledgment flooding attacks and timing attacks.

7. CONCLUSION

IoT technology has become popular in various crucial application scenarios like medicine, weather forecasting, industrial engineering and structural designing etc. The strength of the success of any IoT applications is based on the way that the data is transferred genuinely and the way that the transferring node is proved to be genuine. The authentication process is a crucial requirement for the success of IoT application. The use of Zero-Knowledge Proof systems would help in the non-transfer of secret information instead it helps in verifying the possession of the secret information. The strength of ZKP with Elliptic Curve Cryptography (ECC) is based on the Elliptic curve Discrete Logarithm Problem and also improves the privacy aspects of Blockchain Technology in IoT healthcare applications. The proposed system has been analyzed for various security attacks and behaves to be an authentication scheme in which the verification process does not need secret information about the prover by using the AZTEC protocol. This approach would increase the security level of IoT systems for healthcare applications. The future work extends to try to incorporate public range proofs in the future to add more verification mechanisms.

Table 2. Comparative Analysis

Title/ Ref	**Scheme**	**Property / Parameters**	**Mutual Authentication**	**Optimization**	**Time complexity**	**Space complexity**
Zero-knowledge proofs of identity Feige et al. (1988)	Proof of Identity is either accept or reject	Feige-Fiat-Shamir proof of identity	×	√	Polynomial Time- $O(\|N\|^2)$	Require more memory
A Primer on Zero Knowledge Protocols	Interactive Proof system	Soundness and completeness property using Graph Isomerism	×	×	Polynomial time Reduction for P and NP complete problems	Require more storage space
A Secure Authentication Infrastructure for IoT Enabled Smart Mobile Devices – An Initial Prototype	A light weight power efficient authentication and access control algorithm	One time token generation	×	×	Computation overhead is very low	Require less memory
I2PA: An Efficient ABC for IoT	An efficient attribute-based credential scheme	Attribute, Credentials, Zero Knowledge Proofs, Blind Signing, Blindness	×	×	Time Complexity is $t^{'} = t + O(q_i)T$	Memory usage-1024$(n+6)$ bits
Proposed Method	Authentication and Optimization of ZKP in IoT P2P systems	Soundness and completeness property	√	√	Time complexity is $O(n)$	Very less memory usage

Table 3. Security against attacks

Attack	**Description**	**Method used by this scheme to address the attack**
Cloning	Cloning is an attack by which the attacker can masquerade as a genuine node by using the existing Id	A node uses the random value from the Elliptic curve point to use as a parameter to prove its authentication. Also, the security lies in the selection of the challenge value. The exchange of challenge value is being carried over a number of iterations. The probability of a node trying to impersonate another node is very less, as it requires the node to take full control over the channel for continuing the process of cloning for all iterations.
Reflection attack	Reflection attack works on certain two-way symmetric challenge response protocols by getting the responses from the challenger itself (by reflecting the challenges back to the sending entity and using it to respond)	This scheme uses ECC which is asymmetric. The responses to the challenges are not the same for both entities even if the challenge is the same. In this scheme, the witness value is randomly generated for all iterations and capturing the responses is not useful.
Replay attack	A replay attack occurs when an attacker copies a stream of messages between two parties and replays the stream to one or more of the parties. Unless mitigated, the computers subject to the attack process the stream as legitimate messages	For a replay attack, malicious nodes collect some previous proofs of an initiator, and resend these proofs to the responder. To convince the responder, malicious nodes must guess the challenge message generated by the responder completely and correctly. The probability of a malicious node's guessing correctly challenge chosen by the responder is 2^{-k}. Thus, the success probability of a replay attack is 2^{-k} .
Man-in-the-middle attack	In Man-in-the-middle attack, the attacker tries to intercept the two- party communication by impersonating one to the other, and relaying the traffic between them.	The private key is never sent as part of the challenge. The private key is needed to respond to the challenges; and is available only with the prover.
Hello flood attack	Hello flood attack causes high traffic in channels by congesting the channel with an unusually high number of useless messages. Here a single malicious node sends a useless message which is then replayed by the attacker to create a high traffic	The proposed authentication mechanism requires the correct private key by the prover to ensure its identity. Hence, anonymous messages from anonymous users can be restricted
Sybil Attack	A Sybil attack is one in which an attacker subverts the reputation system of a network by creating a large number of pseudonymous entities and using them to gain a disproportionately large influence.	The probability of a node trying to impersonate another node is very less, as it requires the node to take full control over the channel for continuing the process of cloning for all iterations.

REFERENCES

Almuhammadi, S., Sui, N.T., and McLeod, D. (2004). Better privacy and security in e-commerce: using elliptic curve-based zero knowledge proofs. In *Proceedings. IEEE International Conference on e-Commerce Technology, 2004. CEC 2004.*, 299–302. IEEE.

Aufner, P. (2020). The iot security gap: a look down into the valley between threat models and their implementation. *International Journal of Information Security*, 19(1), 3–14.

Balasubramanian, R. and Koblitz, N. (1998). The improbability that an elliptic curve has subexponential discrete log problem under the menezes—okamoto—vanstone algorithm. *Journal of cryptology*, 11(2), 141–145.

Bellare, M., Namprempre, C., and Neven, G. (2009). Security proofs for identity-based identification and signature schemes. *Journal of Cryptology*, 22(1), 1–61.

Chaum, D., Evertse, J.H., van de Graaf, J., and Peralta, R. (1986). Demonstrating possession of a discrete logarithm without revealing it. In *Conference on the Theory and Application of Cryptographic Techniques*, 200–212. Springer.

Feige, U., Fiat, A., and Shamir, A. (1988). Zero-knowledge proofs of identity. *Journal of cryptology*, 1(2), 77–94.

Fiat, A. and Shamir, A. (1986). How to prove yourself: Practical solutions to identification and signature problems. In *Conference on the theory and application of cryptographic techniques*, 186–194. Springer.

Hummen, R., Shafagh, H., Raza, S., Voig, T., and Wehrle, K. (2014). Delegation-based authentication and authorization for the ip-based internet of things. In *2014 eleventh annual IEEE international conference on Sensing, Communication, and Networking (SECON)*, 284–292. Ieee.

Hummen, R., Ziegeldorf, J.H., Shafagh, H., Raza, S., and Wehrle, K. (2013). Towards viable certificate-based authentication for the internet of things. In *Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy*, 37–42.

Karthigaiveni, M. and Indrani, B. (2019). An efficient two-factor authentication scheme with key agreement for iot based e-health care application using smart card. *Journal of Ambient Intelligence and Humanized Computing*, 1–12.

Kittur, A.S. and Pais, A.R. (2020). A trust model based batch verification of digital signatures in iot. *Journal of Ambient Intelligence and Humanized Computing*, 11(1), 313–327.

Kothmayr, T., Schmitt, C., Hu, W., Brünig, M., and Carle, G. (2013). Dtls based security and two-way authentication for the internet of things. *Ad Hoc Networks*, 11(8), 2710–2723.

Yugha, R. and Chithra, S. (2019). Attribute based trust evaluation for secure rpl protocol in iot environment. In *2019 International Conference on Vision towards Emerging Trends in Communication and Networking (ViTECoN)*, 1–7. IEEE.

Yugha, R. and Chithra, S. (2020). A survey on technologies and security protocols: Reference for future generation iot. *Journal of Network and Computer Applications*, 169, 102763.