International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6368
***Article Received**: 10 January 2023 **Revised**: 14 February 2023 **Accepted**: 20 February 2023*

Secure Authentication Scheme for the Internet of Things

Animesh Srivastava[1], Dr. Anoop Kumar[2]
[1]Research Scholar , Department of Computer Science[1]
Banasthali Vidyapith
Vanasthali , India
e-mail: er.animesh10@gmail.com
[2]Assistant Professor , Department of Computer Science[2]
Banasthali Vidyapith
Vanasthali , India
e-mail: anupbhola@gmail.com

Abstract— The Internet of Things (IoT) is based on an extensive and wide range of interconnected heterogeneous units' general applications, including healthcare systems, environmental monitoring, household automation, and business automation. This work presents an approach variant of the elliptic curve; The cryptography approach is implemented to provide more security with fewer key sizes and with protocol enhancements to perform an efficient authentication process. In the process of authenticating the device, we use the Electronic Product Code (EPC) as a key to authentication, where the overhead of giving input is removed. Mention the methods followed to meet all your performance metrics (minimum execution time; low energy consumption, and qualitative comparison). This proposed scheme (i.e., the energy consumption of 0.27 mJ, the reduction in end delay of 0.058 sec., the reduction in the computation cost, and being more resistant to attack) is compared with other recent authentication protocols. The proposed system creates a secure network to lessen the damage if there is an attack in the IoT environment. The performance evaluation results indicate that the proposed scheme has a lower energy consumption and a more resistant authentication scheme, and we observe a trade-off between security and the lightweight factor.

Keywords- Authentication, Efficient, Devices, Internet of Things, Secure.

I. INTRODUCTION

The Internet of Things (IoT) is a modern computing model that refers to interconnected devices. The IoT consists of nodes with minimal resources, which, regardless of time or place, are widely dispersed in the IoT environment. IoT is now used for various purposes, including hospitals, Smart homes, Smart manufacturing, and Smart cities [7][8]. Authentication in the network is the most important thing to work on when it comes to the security challenges. If the network of sensors in a given environment doesn't have authentication properties, it's very likely that intruders can easily pretend to be real users and get important information from the network. Any new user or device from outside the network that wants to talk to other devices on the network needs to be checked to make sure it is a real device.

The IoT faces different challenges with user nodes or sensor nodes communicating with each other and dynamic in nature. The user authentication system has to ensure the protection of functional specifications to ensure the safety of the IoT system, which is an efficient authentication protocol to improve the performance of sensor devices in the system. So, for IoT systems to reach their full potential, they need a way to communicate that is both light, safe and less overhead [15][16]. We suggest a secure authentication scheme for making sure that Internet of Things devices can connect safely with registrant of the external attack.

IoT devices can be easily attacked for security reasons because of how they are set up. Even though there are a lot of security solutions for traditional systems, they can't be used directly with the Internet of Things (IoT) because of limitations like memory, resources, energy, and the fact that the IoT is used in an unattended environment. This means that new security schemes are needed for IoT in wireless sensor networks, where the nodes can't do very complicated tasks or store a lot of data.

The outcome of the proposed work will be a secure model and low energy consumption for the node. This will also lead to low packet losses, which is another significant parameter for the network evaluations. Using the enhanced authentication protocol, the proposed system creates a secure network to lessen the damage of an attack in the IoT environment

B. Contributions

This paper main contributions are that we report to show that our protocol is secure against many types of known attacks, and we compute various performances and compare them against other existing schemes.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6368
***Article Received**: 10 January 2023 **Revised**: 14 February 2023 **Accepted**: 20 February 2023*

B. AUTHENTICATION IN THE PERCEPTION LAYER: SECURITY ISSUES, MODELS

Protecting the IoT viewing device is a tedious task due to its heterogeneity and nature, such as unreliable wireless technology and limiting the emissions of devices left in a derelict environment [28]. To ensure the safety of these devices, we need to be careful of different security features. These assets can be separated into two categories: The main refuge features are authentication, data accessibility (or confidentiality), and integrity. The second type has characteristics such as timestamp adjustment, data updating, or the network's self-organization. The value of this attribute depends on the application area of the Internet of Things. For example, confidentiality is imperative in environmental observation. Accuracy, accessibility, and completeness are essential attributes in the medical field. Because of the deployment of IoT devices, they are vulnerable to security. Although many security solutions exist in traditional networks, they are not directly relevant to the Internet of Things due to constriction such as memory, resources, energy, or resources, which places them in an unguarded world. Because nodes cannot perform very complex tasks or store large amounts of data, they need a new solution that can be used on the IoT in a wireless network environment.

Internet of Things (IoT) security issues:
1. Ecosystem Complexity
2. Device capacities are limited.
3. Threats and attacks
4. Safety versus efficiency
5. Lack of rigour in data processing.

II. Related Works

In order to ensure safe interaction between users and IoT devices, numerous authentication protocols have been proposed in recent years.

Author work looks into why threads and vulnerabilities happen, especially in IoT, IIoT, SCADA, and Android application systems. Integrity, confidentiality, availability, privacy, and non-repudiation are the five basic principles that make up the system's basic security framework. Along with Honeynet, IDS, and IPS, hardware-based security like CPU and Memory is also a very effective way to protect infrastructure. The developers have built in parts of different systems so that they can offer different services [34].

Author discusses the Internet of things (IoT) is getting better because of how quickly technology is changing. IoT devices come with sensors that allow them to do the jobs they were made for. Using these kinds of devices is linked to making sure that communication between devices and users is safe. Authentication and agreeing on session keys are the most important parts of communication [35].

Author discuss the RFID systems get better, there is a need for more secure RFID authentication. Chiou and Chang recently came up with a plan for an RFID protocol that is based on EPC Class 1 Gen-2. In this paper, we use both formal and informal methods to show that the proposed protocol is safe. In the formal method, we use the Scyther tool's Compromise version [36].

The author proposed a new authentication and key agreement protocol based on the user's identity. They asserted that their protocol is impervious to different forms of attack. research showed that it was vulnerable to privileged insider attacks, device theft, verifier theft, and temporary data exposure. [26].

Author discusses the authentication and session key establishment is an essential security requirement. Many schemes for authenticated key exchange between IoT devices and cloud servers have been proposed. The extended Canetti–Krawczyk (eCK) adversary model is regarded to be a more strict and relevant adversary model [27].

Author discuss Security and Stability Control System (SSCS) is a very important part of making sure that the power system works well. Still, SSCS doesn't have a good security system, so attackers can easily get in. To solve this problem, we suggest that Identity Authentication Schemes for Intelligent Electronic Devices be based on the blockchain (IEDs) [28].

Author discusses the Internet of Things (IoT) is an up-and-coming technology because it has new ideas and solutions for a wide range of problems. Wireless Sensor Network (WSN) is used by many devices in the real world to collect valuable raw data from sensors. In related work, there are many 2-factor verification protocols that use a smart card, a public key, and a password. Most of them have trouble balancing the need for skill and safety [29].

Author elaborates to facilitate seamless integration with the Internet of Things, edge computing, grid computing, cloud computing, and smart networks, redundant data transmission should be kept as straightforward as possible. Eliminating redundant information with the desired degree of precision presents some difficulties and limitations. Scaling WSN applications, mobility, SN localization, environment, and user satisfaction are all aided by IoT applications. [33].

Author discuss lightweight IoT gateway suitable for the IoT industry for embedded Web servers. The low-power MAC STM32F407 controller is the included controller, and the UCOSIII is the software operating system. Network migration can be accomplished by migrating the LWIP protocol stack. The Web server included in the gateway is shipped with a gateway. The elliptic curve encryption algorithm is built to realize the anti-encryption send. The connection between the gateway and the back-end server receives a special relationship. Protocol. By the gate display test, the packet loss rate at the gate is 0.08%, and the network delay is less than 10ms. Therefore, the gateway

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6368
***Article Received**: 10 January 2023 **Revised**: 14 February 2023 **Accepted**: 20 February 2023*

has reliable data transmission, reliable efficiency, simple installation and setup, and high application cost [1].

Author Investigated the repetitive filtering of the Time-Varying Discrete Sequence System (DSS) under the Weighted Attempt Once Discard (WTOD) account, which is used to manage access permissions. In shared networks to reduce the communication burden. A transmission model that relies on a white line in the Bernoulli division was developed to predict the occurrence of an attack signal. Aiming at customized models and attack models, a kind of recursive algorithm in Riccati variance comparison is proposed to improve the filtering efficiency in a square sense. In addition, with mathematical input, the combination of the proposed recursive algorithm is discussed in depth. Finally, a simulation example is provided to verify the use of the recursive filter performed [3].

Author discuss Smart pole mesh networks with multiple IEEE 802.11p/WAVE radios should use an RSSI-based routing protocol. Because of the time it takes to measure metrics, traditional mesh routing protocols don't work very well in IEEE 802.11p-based multi-radio, multi-channel environments. Due to the delay in switching channels, the periodic probe messages that check the quality of each channel add a lot of extra work. To solve this problem, we propose a routing metric that predicts how long it will take to send a message and a lightweight channel allocation algorithm that uses only the RSSI value. We use simulation experiments with NS-3 to test how well the proposed solution works. Simulations show that it can improve network performance in terms of latency and throughput compared to the old WCETT routing scheme [4].

Author Analyze the low-key switching protocol (UFSOOK) effectiveness commonly used for lightweight communications. Data transmission is structured as a measurement process, and analysis of the underlying measurement channels and data sources may reveal the protocol's characteristics. The theoretical error rate is a function of the features of the receiver camera, the frequency between the transmitter and receiver, the measurement noise, and the protocol parameters. Therefore, measurements are also recommended and are used to verify theoretical results [5].

Author discusses security issues associated with the authentication of data on intelligent IoT networks, blockchain technology has been developed to achieve significant and secure management functions and blockchain parameter innovation. The proposed system is designed for lightweight IoT devices and provides additional security measures through the details of installation difficulties. This article examines hash extraction and implementing the proposed solution implemented in the java programming language. In addition, this article also discusses the application of algorithms to different fractions of the proposed solution and compares their processing times. Combining more complex parameters and faster decryption algorithms provides the most suitable solution for IoT devices with low computing power and low memory [2] [6].

Author discuss Most IoT devices communicate wirelessly, which raises security concerns for wireless sensor networks. Authenticating wireless sensor network nodes is a concern. In IoT, if a device initiates communication, an attacker might listen in or impersonate the device. This gives the attacker access to communication information and the ability to reconfigure devices [37][38].

B. Research Gaps

With the study literature review, gaps in the research have been found. We focused primarily on the security challenges of the IoT. We need to tackle the problem of authentication in the perception layer of the IoT. We have found that the existing authentication methods are still subject to attacks and produce some overhead for the device. There are several security challenges. The main problem is authentication on the network. If the network in the authentication possession is missing in any given environment, intruders can easily access legitimate users and critical information from the network and distribute the network. Therefore, each new external user or a new device that is ready to communicate with other devices available in the network that exists in the network will be checked to see if it is a legitimate device. All of the authentication schemes that have been made so far are successful to some degree, but there are still some problems with them. Based on their performance analysis, it can be assumed that these methods sometimes cause sensor devices to run out of power and also add extra work for the network to do. Complex authentication protocols can lead to problems like these, so it's best to use a simple authentication protocol to improve the performance of sensor devices in the system. Below are points we will take as challenges:

- Energy exhaustion.
- computational overhead.
- challenges for optimizing IoT networks.
- Limited Resistance to the authentication scheme.

The outcome of the proposed work will be a secure model with low energy consumption for the node. This will also lead to low packet losses, which is another significant parameter for the network evaluations. Using the enhanced authentication protocol, the proposed system creates a secure network to lessen the damage of an attack in the IoT environment.

III. Methodology

The scheme's ultimate objective is authentication of devices using less time- and energy-intensive security methods. To improve security with smaller key sizes and faster authentication with protocol enhancements, the cryptography approach is proposed for use with variants of the elliptic curve.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6368
***Article Received**: 10 January 2023 **Revised**: 14 February 2023 **Accepted**: 20 February 2023*

A Proposed ECC- based authentication scheme for the internet of things

The Internet of Things (IoT) lets real and virtual objects that are controlled by different kinds of hardware, software, and communication technologies talk to each other. IoT is being used on a large scale all over the world, which makes it possible for smart cities, smart factories, smart health, and many other applications and projects to happen. IoT will make our cities and daily applications smart. IoT, however, also pose a number of risks and privacy issues. Due to the limitations of their hardware, IoT objects make it hard to implement and deploy strong and effective security and privacy solutions for the IoT environment. We use Electronic Product Code in the authentication that could be a good solution for the Internet of Things (IoT) and smart cities. We add to the Electronic Product Code principle and suggest a new way to make sure IoT security based on elliptic curve cryptography and isogeny.

A promising solution for the IoT in many environments. An enhanced authentication scheme for the Internet of Things based on elliptic curve cryptography as a result of which there is less computation overhead. [8]

The parameter we have changed in the computed the functional points in the ECC algorithm to perform the operation of successively accumulating the points along an elliptic curve, which reduces the size of the ECC computation. We can fix the level or value of computation during the encryption and decryption process and reduce the complexities.

We have a cryptographic elliptic curve and the point G (point G form cyclic groups (or cyclic subgroups), which means that a number r exists (r > 1)) that makes it. From the ECDH scheme, we can use the following two functions to figure out a shared secret key for encryption and decryption:

This approach uses six tuples {P, a, b, G, n, h}
P= Filed that the curve is define over
G= Generator point
a, b= Values define the curve
h=Co-factor
n= Prime order of G

Algorithm 1: Key Generation & Sharing:

• calculateEncryptionKey(publicKey) —> (ciphertextPublicKey, sharedECCKey)

1. Generate ciphertextPrivateKey = new private key chosen at random.
2. Use ciphertextPrivateKey + G to figure out ciphertextPublicKey.
3. Use the formula sharedECCKey = publicKey * ciphertextPrivateKey to figure out the ECDH shared secret.
4. Give the sharedECCKey and the ciphertextPublicKey back. If you want to use symmetric encryption, use the sharedECCKey. Use the ciphertextPublicKey that was made by chance to figure out the decryption key later.

• sharedECCKey = calculateDecryptionKey(privateKey, ciphertextPublicKey)

1. Use the formula sharedECCKey = ciphertextPublicKey * privateKey to figure out the ECDH shared secret.
2. Give the sharedECCKey back and use it to decrypt.

• (a * G) * b = (b * G) * a

Now, let's say that an is the privateKey, a*G is the publicKey, b is the ciphertextPrivateKey, and b*G is the ciphertextPubKey. This is how the above equation looks:

• ciphertext * publicKey
ciphertextPubKey = privateKey * privateKey = sharedECCKey

The above two functions do calculations that are exactly the same as the ECDH key agreement scheme. In hybrid encryption schemes, the encapsulated ciphertextPublicKey is also called a "ephemeral key" because it is only used temporarily to find the symmetric encryption key using the ECDH key agreement scheme.

B. Device Registration

In this phase, the gateway and the IoT device are configured with the established security settings. The new gadget needs to be registered at the gateway before it can access the network or undergo authentication.

Symbol Meaning

v = Secret Value of the system
‖ = Concatenation
Nd = Random nonce of the device
⊕ = Exclusive OR
Ng = Random nonce of the gateway
Dk = Shared key generated using Diffie-Hellman
E(M, K) = Encryption function of M with key

Algorithm 2: Device Registration Phase

1: D → G: Sends Electronic Product Code -EPC encrypted with Elliptic Curve Diffie-Hellman symmetric key Dk
2: G: Decrypts message to find Electronic Product Code -EPC or Computes the shared secret value SK = H (Id ‖ V), P = SK ⊕ EPC
3: G → D: Sends P

C. Device Authentication

A device needs to log in and prove its identity at the network's gateway before it can talk to other devices and do its work safely. After the device has been successfully registered at the gateway, it will go through the authentication process when it tries to connect to other devices.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6368
Article Received: 10 January 2023 Revised: 14 February 2023 Accepted: 20 February 2023

Algorithm 3: Device Authentication Phase

1: D: Generates random number Nd, Computes SK′ = P ⊕ Electronic Product Code -EPC

2: D → G: Message M1 = Id, ESK′ (Nd)

3: G: Decrypts ESK′(Nd) with SK, then calculates SK = h(Idv), N ′ d to get a random number. Ng

4: G → D: Message M2 = ESK (N ′ d ‖Ng)

5: D: Gets N'd and N'g by decrypting M2 with SK', checks that Nd = N'g, and figures out session key K = Nd - N'g.

6: D → G: Message M3 = ESK′ (N ′ g)

7: G: recovers N ′ g by decrypting M3 with SK and making sure Ng = N ′ g; calculates session key K = N ′ d Ng.

In the above used An Electronic Product Code is a unique number that can be used to identify any product. makes it possible to track and identify items.

E. Attack Mitigation

Identity verification is one of the requirements for the security of the Internet of Things. Users must be authenticated to use IoT applications and services. In general, IoT applications and services are based on data exchange between diverse platforms. The data attained from IoT devices is pre-processed, processed, or then pre-processed by the decision-making system. These processes may be different depending on the IoT architecture. However, the data flow in these systems may be similar. When applications and users need to receive data from IoT devices without any general losses, the entity (user or application) must be authenticated through the IoT network. It should ensure that the applicant has all the data. License. Otherwise, requests for access to such data will be denied. Like in other networks, access control is also significant in IoT networks. Due to (but not incomplete) network heterogeneity, network number, device resource limitations, network (insecure), and attack vulnerability, contact control also has problems. some. In addition, it is also significant to grant and disable access to submission data and IoT services for some users. Earlier, we talked about the system that controls ML access to the Internet of Things. Therefore, it is important to clarify the type of access control.

***Algorithm 4: Attack Mitigation Algorithm*:**

The flow of traffic
Start: Capturing Traffic
Determine: Features (F)
Extract: Selected Features (SF)
Feed: SF → Classifier (For Training)
Run: Classifier "Within a limited amount of time" / Time Frame
If the number of suspicious cases is less than the pre-set threshold value,
End If Cancelled: The Host
If "suspicious activity" means "attack,"
Raise: Alert
Remove: Things that look fishy
Else:
All the steps again, but with a new time frame
Output: Malicious Finding a signature

Threat model

Attack in the middle: Since all communications are locked, people will not attack in the middle. The timestamp is used to soften the repeat attack.

Failure points: failure points are transferred to the verifier rather than a single failure point to the previous model. If the verifier is damaged, all of the manufacturer's equipment is damaged. In addition, because the malicious verifier can add malicious material to the network, it can add access to the malicious material to the blockchain. Because other verifiers trust the malicious verifier, it is the entire network. It is disrupted.

Insider attacks: If there is an internal hacker attack, it may damage the manufacturer's key.

F. ECC ALGORITHM

ECC: In the field of public-key cryptography, elliptic-curve cryptography is one method that utilises the algebraic structure of elliptic curves over finite fields. A public essential encryption technique based on the algebraic arrangement of elliptic curves over finite fields can create faster, more minor, or more competent cryptographic keys [12].

(I) Key Mechanism: The sender (signer) is the only one who knows the private key, it is used to make a signature. All communication partners get the public key, or their trusted party gives it to them.

(II) Key Generation: In the ECC, the sender chooses a privatekey and counts the public key. "d" is the specific key for the sender, and "A" controls the elliptical curve.

(III) Key Distribution Method: The sender knows the personal key and gives the recipient the public key through a secure channel (such as Diffie-Hellman key exchange or other means of replacing base).

(IV) Signing mechanism: The first step of this mechanism is to use a reliable hash algorithm to prepare the hash or decryption of the message to be signed. The second step is to use a number calculator to figure out a number value. This number is neutral, so it can be used to figure out how to make an elliptic curve.

(V) Verification mechanism: the third mechanism is called the verification mechanism. The signing mechanism is when

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6368
***Article Received**: 10 January 2023 **Revised**: 14 February 2023 **Accepted**: 20 February 2023*

someone gets a message that has been signed. In this case, the public key of the verifier, which is the sender, can be used to check that the news is true.

ECC is a public-key encryption method based on the algebraic structure of elliptic curves over finite fields that can be used to make cryptographic keys that are faster, smaller, and more secure.

G. Key Generation & Shared secret key

Elliptic Curve Cryptography (ECC) is a popular public-key cryptography algorithm that is widely used for secure communication and authentication. Here are a few ways to make ECC lightweight:

Curve Selection: Choosing a smaller curve size can reduce the computational overhead associated with ECC.

Hardware Optimizations: Optimizing the implementation of ECC in hardware can significantly improve its performance. For example, hardware acceleration can be used to speed up key generation and encryption/decryption operations.

Hybrid Cryptosystems: Combining ECC with other cryptography algorithms, such as symmetric key cryptography, can help to make ECC more efficient. For example, ECC can be used to securely exchange a symmetric key, which can then be used for the bulk encryption of data.

It's important to note that reducing the computational overhead of ECC may also reduce its security. It's essential to carefully consider the trade-offs between security and efficiency when making updates to ECC. In our scheme we have taken the curve selection approach to enhance the performance of the ECC. The steps for encrypting and decrypting communications are shown in Figure 1 as well as how the node uses ECC to encrypt messages using the keys and parameters.

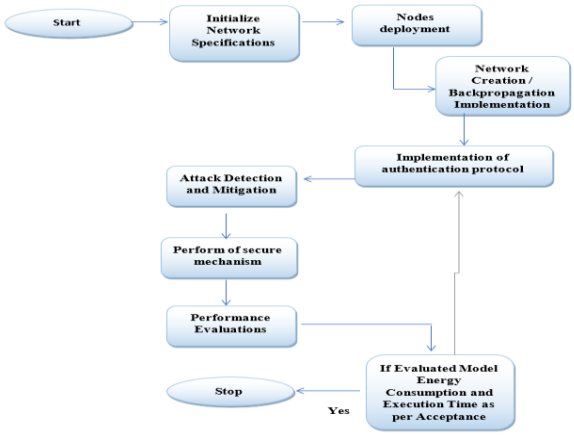

Figure 1: Proposed Flow Diagram

IV. Result & Discussion

The simulator is essential for prototyping, architecture exploration, and threat model testing. IoT projects typically have a very high sensor or actuator node densities. The results of the constructed network's simulation are presented here. Multiple performance parameter graphs are displayed. Existing algorithms are compared with the proposed system as well. In Figure 2, we see the results of a simulation run on a network with 30 nodes. The malicious actions of the monitor are broadcast across the entire administrative network. For the simulation, we turned to MATLAB. The use of symmetric core protocols, ECC encryption for authentication of devices, and machine learning-based security technologies are discussed in this section. Despite the WSN's many positive uses, it is especially susceptible to hacker attacks like Man in the Middle (MITM). In a man-in-the-middle attack, a hacker temporarily poses as a trusted user to steal sensitive information. The attacker or attacker takes on the role of a proxy user and manipulates the data to suit their purposes. MITM was often shortened to MIM and other forms in ancient writing. During a man-in-the-middle attack, the attacker illegally eavesdrops on a conversation between two legitimate users. In order to gain access to sensitive information or data, an attacker may pose as a legitimate user in order to conduct an attack. During an MITM attack, new conversations or file transfers frequently occur. In the absence of solid security, two legitimate users will be unable to verify the authenticity of the information.

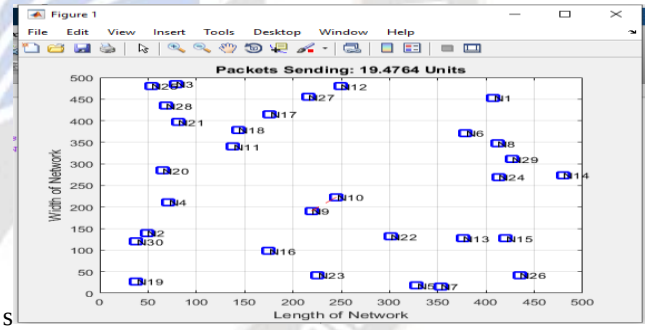

Figure 2: Network Initialization

To carry out the route request, data from the public node is sent to the source routing node in the region. The source node then adds information about the chosen route to the source routing header. In the process of sending data in a data packet, the transmission point between the intermediate points follows the relay path and moves forward based on the source path information in the packet head. There is no connection to the source routing node, which can help the system use less energy.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6368
***Article Received**: 10 January 2023 **Revised**: 14 February 2023 **Accepted**: 20 February 2023*

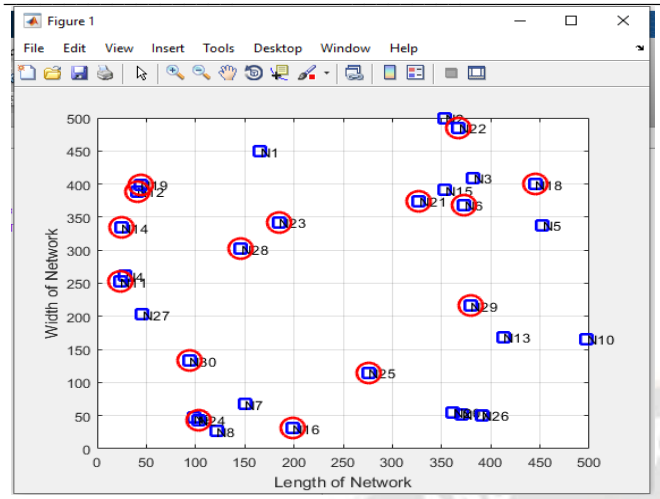

Figure 3: Device Registration

Figure 3 shows the zone configuration depends entirely on the energy efficiency between the source routing node and the public node. To extend the network's life, the energy efficiency determines which of the resource node areas is more suitable for the public domain. Zone creation is accomplished by controlling message exchange between the source routing node and the shared node.

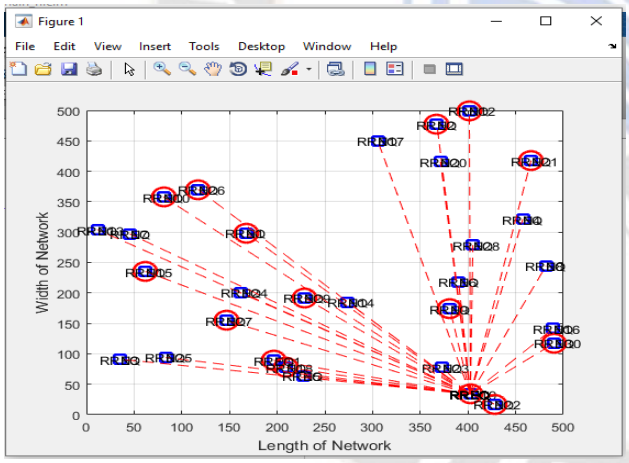

Figure 4: Route Request Packet (RREQ) is broadcasted from a Source Node to Other Nodes in the Network.

Figure 4 shows that the possibility of sending different messages through RREQ is when a request path packet (RREQ) is sent from a source node to another point in the network. The default record field in the source transport package contains all the paths from the source to the destination as it travels. The data packet comes with a source data transmission function that allows an intermediate hop between the source node and the target node to include the network address in the data packet (RREP). In contrast, the data packet follows the path from the target to the source. In this way, a route is created, and the source node can use the path to send data packets to the destination of the source path,

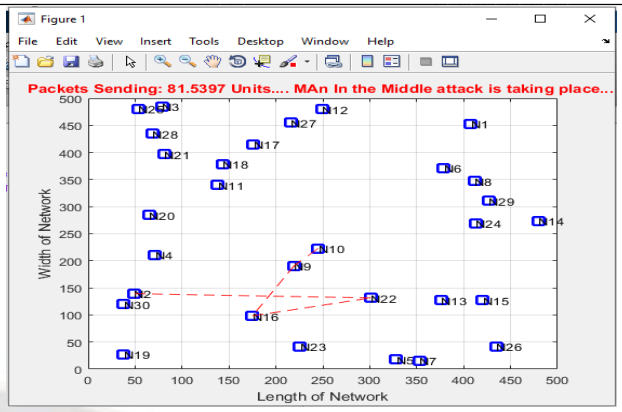

Figure 5: MIM attack taking place

Figure 5 shows that a middleman attack occurs when an intruder enters the network and is positioned in the middle of the data stream. There are two sensors and a router node. We report to show that our schema is secure against known attacks.

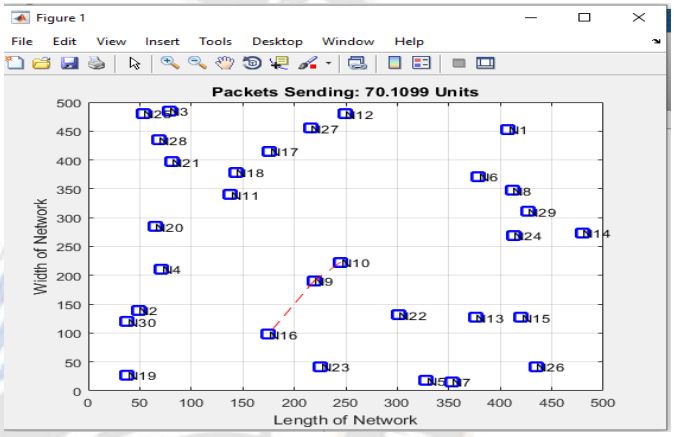

Figure 6: Searching Path and Reroute

And finally, the malicious node forwards the configured data packet to the target node, blocking its path in the wrong direction and creating a wrong neighbour between the target points in the process. The next step is to capture the data packet to find the modified application data and insert it into the target node. When the dirty spot cannot withstand interesting traffic, it will store the package and repeat the capture process. MITM attacks will focus primarily on data entry between clients and servers for other malicious activities. However, MITM attacks can use more attacks. Thus, we define that MITM attackers can establish an independent relationship with the victim and convince them that their conversation is still being conducted through personal contact. Attackers can block, transmit data packets, and even inject new data packets. MITM attacks are primarily focused on importing data between clients and servers for other malicious activities. However, we believe that MITM attacks could be more numerous. Thus, the MITM attacker can establish an independent relationship with the victim and convince them that their conversation is still being carried out through personal communication. Attackers can block, transmit, and even inject new packets.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6368
***Article Received**: 10 January 2023 **Revised**: 14 February 2023 **Accepted**: 20 February 2023*

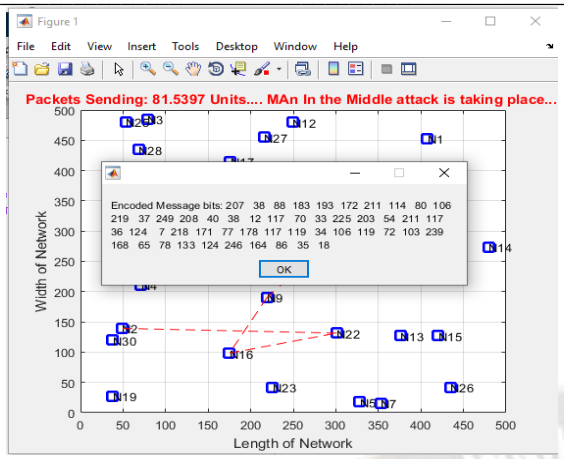

Figure 7: Elliptic Curve Cryptography (ECC) Message Bits

Figure 7 shows that Elliptic Curve Cryptography (ECC) is a type of public-key cryptography. The user or device participating in the communication usually has a key, a public key, a private key, and a series of functions associated with these keys to perform encryption operations. Only private users know the private key, and the public key is shared with all users participating in the connection. In an asymmetric account, the data is erased and locked by a common shared key, so there is a basic exchange problem. However, the secure sharing of key communication keys is a big problem because it is impossible to share keys. shows the network latency, which measures the time it takes for some data to reach the network's destination. It is usually measured by the delay back and forth - the time it takes for the message to reach its destination and return.

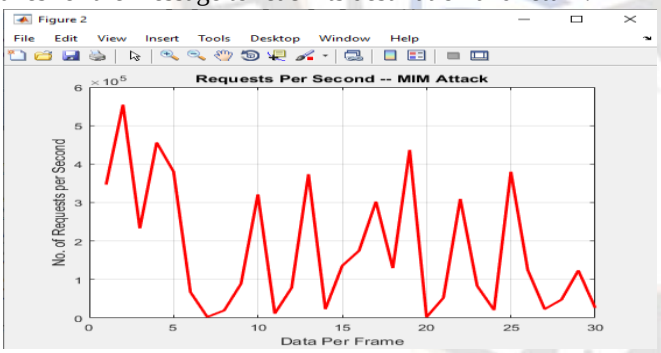

Figure 8: Number of Requests Per Second MITM Attack

Figure 8 shows the number of attacks per second with each data frame, where the y-axis shows the amount of data per second and the x-axis shows the data frame

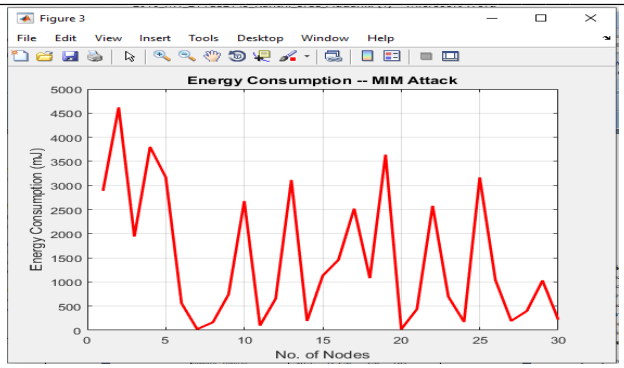

Figure 9: Energy Consumption While MITM Attack

Figure 9 shows energy consumption while MIM attacks in Wireless networks, most of the energy is consumed in the process of data transmission. In the Figure, the y-axis shows the amount of energy consumption during packet transmission, and the x-axis shows the number of node Network latency is the time it takes for a network to send a message. It tells you how long it takes for data to move across the network.

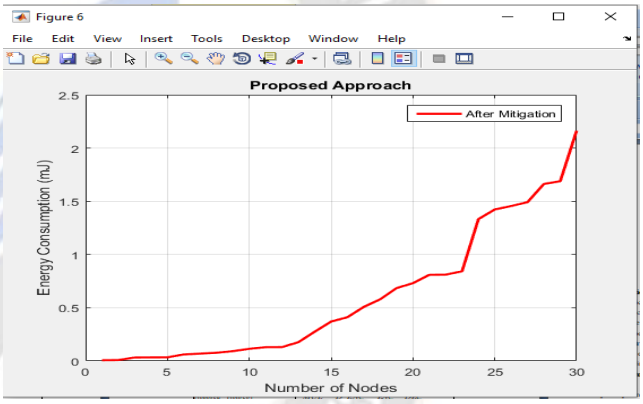

Figure 10 Proposed Energy Consumption

The system's energy consumption is depicted in Figure 10. Energy consumption rises in proportion to the square of the coverage area, primarily because of the member's increased distance from the single CH. The equipment's energy consumption and the wireless sensor network's transmission power are the two main factors in the energy balance. The y-axis shows the energy consumption, and the x-axis indicates the number of nodes.

Performance Comparison:

Compared with taking the value as per the comparison component.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6368
Article Received: 10 January 2023 Revised: 14 February 2023 Accepted: 20 February 2023

Energy Consumption:

Table 1: Energy Consumption

Algorithm	Energy Consumption
Proposed	2.1
LoRa Transmission	2.95
ECC [9]	24.9
ECC-L [9]	32.2

Table 1 shows the energy consumption for the different algorithms. The energy consumption is reduced from 24.9 to 2.1 mJ.

Table 2: End Delay

Algorithm	End delay
Proposed	0.058s
ECC [9]	29.5s
ECC-L [9]	18.9s
S. Chatterjee [30]	6.018s
SDWSN-NETCONF [14]	25s
SDWSN-OF [14]	16s
SDWSN-BGP [14]	21s

Table 2 shows the end delay for the proposed algorithm which has reduced to nearby 6 sec to 0.058 sec.

Cost of Computation

When designing the protocol, the limited resources of IoT devices were taken into account. As a result, all of the operations used in our protocol are simple and lightweight to meet this need.TH:

TH: The amount of time it takes to run a one-way hash function
TMUL: The amount of time it takes to do an ECC point multiplication
Tsign is the amount of time it took to make the signature.
TENC: The amount of time it takes to run the symmetric key encryption.
TPU ENC: The amount of time it takes to run the public key encryption.
TDEC: The amount of time needed to decrypt a symmetric key.

Table 3: Computation Cost

Protocol	Computation Cost
Proposed	*TMUL + TDEC + TENC*
Addanki [8]	*TPU_ENC* + 2*TENC* + *TDEC*
Zhao's Protocol [10]	2*TH* + 3*TMUL* + *Tsign*
Chatterjee's Protocol [11]	3*TH* + 2*TMUL* + 3*TDEC*

Key contributions as follows:

1. Design a Strong authentication scheme that mitigates the effect of the attack on the IoT network. We provide a More secure and less overhead authentication scheme in this research strategy.
2. Results from simulation indicate that the proposed scheme has outperformed other current schemes in terms of energy consumption, End delay, and computation cost.

Our results and simulation show that our schema is secure against many types of known attacks. Our results improve the level of security and reduce the overhead. This implementation is done on the IoT Perception layer. We computed various performances and compared them against other existing schemes. Analysing the existing schemes that may present an improved form of the existing methods.

B. Analysis

The proposed scheme can conduct analyses like the following, depending on the security needs:

• Camouflage: Because to use the user authentication using a EPC which is unique and given by the manufacturer so difficult to alter and Clone.

• Exposure: With ECC, we can encrypt data with fewer keys while increasing security, and we can use security to ensure that only authenticated users can access data.

V. Conclusion And Future Directions

In this paper, we propose an authentication scheme based on symmetric base agreement that uses ECC during the registration process and symmetric base configuration in the validation process. We have used the Electronic Product Code as the authentication key, which is unique and difficult to clone. Based on the performance analysis, this method is also light and easy to use because the key for lightweight cryptography ECC is small compared to the keys for other methods. The outcome shows that the proposed scheme is efficient (i.e., has the lowest computation cost**,** energy consumption, and end delay**)** compared with other recent authentication protocols, making the proposed scheme reasonable and realistic for massive implementation scenarios based on IoT environments. Based on the performance analysis, the proposed method is only light compared to the existing methods, but we can make exchanges in terms of safety and lightness. The outcome shows that the proposed scheme (i.e., the energy consumption of 0.27 mJ, the reduction in end delay of 0.058 sec., the reduction in the computation cost, and being more resistant to attack) compared with other recent authentication protocols.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6368
***Article Received**: 10 January 2023 **Revised**: 14 February 2023 **Accepted**: 20 February 2023*

Future Directions

In the future, possible improvements to build a collaborative architecture that allows devices to access numerous cloud-based network services using the same lightweight authentication model. For Internet of Things systems, we can create a Multi Gateway Authentication Scheme as well. It's great for use cases where lots of IoT/IIoT devices need to be networked together. The lack of adequate stability and light objectives can explain the recurring errors that can occur in old verification principles and build a more effective and robust approach to future work.

REFERENCES

[1] HaiYang Zhang;Yanli Ma;Benzhen Guo;Zhe Xu Light-weight IoT Gateway with Embedded Web Server 2020 12th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC) Year: 2020 DOI: 10.1109/IEEE Hangzhou, China

[2] Hui Xia; Zhetao Li; Yuhui Zheng; Anfeng Liu; Young-June Choi; Hiroo Sekiya A Novel Light-Weight Subjective Trust Inference Framework in MANETs IEEE Transactions on Sustainable Computing Year: 2020 DOI: 10.1109/TSUSC.2018.281721

[3] Xin Li; Guoliang Wei; Derui Ding; Shuai Liu Recursive Filtering for Time-Varying Discrete Sequential Systems Subject to Deception Attacks: Weighted Try-Once-Discard Protocol IEEE Transactions on Systems, Man, and Cybernetics: Systems Year: 2020

[4] Jong-Young Choi;Jiwoong Park;Sung-Hwa Lim;Young-Bae Ko A RSSI-Based Mesh Routing Protocol based IEEE 802.11p/WAVE for Smart Pole Networks 2021 23rd International Conference on Advanced Communication Technology (ICACT) Year: 2021

[5] Gyula Simon; Márk Rátosi Characterization and Measurement of Performance Properties of the UFSOOK Camera Communication Protocol IEEE Transactions on Instrumentation and Measurement Year: 2020

[6] Ahmed Alrehaili; Aabid Mir POSTER: Blockchain-based Key Management Protocol for Resource-Constrained IoT Devices 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH) Year: 2020

[7] Shafkat Islam;Shahriar Badsha; Shamik Sengupta, A Light-weight Blockchain Architecture for V2V Knowledge Sharing at Vehicular Edges 2020 IEEE International Smart Cities Conference (ISC2) Year: 2020

[8] Kanthi Sree Addanki, Secure and Lightweight Authentication Protocols for Devices in Internet of Things, Computer Science and Engineering, National Institute of Technology Rourkela 2016.

[9] Notom Ajaykumar, Mrinal Sarvagya, Parag Parandkar, A novel security algorithm ECC-L for wireless sensor network, Internet technology letter Volume3, Issue3, May/June 2020.

[10] S. Chatterjee, A. K. Das, and J. K. Sing, "A novel and efficient user access control scheme for wireless body area sensor networks," Journal of King Saud University-Computer and Information Sciences, vol. 26, no. 2, pp. 181–201, 2014.

[11] Abosata N, Al-Rubaye S, Inalhan G. Lightweight Payload Encryption-Based Authentication Scheme for Advanced Metering Infrastructure Sensor Networks. Sensors (Basel). 2022;22(2):534. Published 2022 Jan 11. doi:10.3390/s22020534

[12] S Ebrahimi, S Bayat-Sarmadi , Lightweight Fuzzy Extractor Based on LPN for Device and Biometric Authentication in IoT, - IEEE Internet of Things Journal, 2021

[13] Bouguera, T.; Diouris, J.-F.; Chaillout, J.-J.; Jaouadi, R.; Andrieux, G. Energy Consumption Model for Sensor Nodes Based on LoRa and LoRaWAN. *Sensors* 2018, *18*, 2104.

[14] Modieginyane, Kgotlaetsile & Malekian, Reza & Letswamotse, Babedi. (2019). Flexible network management and application service adaptability in software defined wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing. 10. 1-10. 10.1007/s12652-018-0766-7.

[15] A. Srivastava and A. Kumar, "A back propagation NN to optimize the IoT network," *2022*, pp. 1-4, doi: 10.1109/ICCCI54379.2022.9740861.

[16] Dengmei Xiang, Xuelian Li, Juntao Gao, Xiachuan Zhang, A secure and efficient certificateless signature scheme for Internet of Things, Ad Hoc Networks, Volume 124, 2022

[17] Prakasam P, Madheswaran M, Sujith KP, Sayeed MS. Low Latency, Area and Optimal Power Hybrid Lightweight Cryptography Authentication Scheme for Internet of Things Applications. Wireless Personal Communications. 2022 May 4:1-5. https://doi.org/10.1007/s11277-022-09748-1

[18] King-Hang Wang, Chien-Ming Chen, Weicheng Fang, Tsu-Yang Wu, A secure authentication scheme for Internet of Things, Pervasive and Mobile Computing, Volume 42,2017,Pages 15-26, https://doi.org/10.1016/j.pmcj.2017.09.004.

[19] Park, K.; Park, Y. On the Security of a Lightweight and Secure Access Authentication Scheme for Both UE and mMTC Devices in 5G Networks. Appl. Sci. 2022, 12, 4265. https://doi.org/10.3390/app12094265

[20] Bin Hu, Wen Tang, Qi Xie,A two-factor security authentication scheme for wireless sensor networks in IoT environments, Neurocomputing,Volume 500,2022,Pages 741-749, https://doi.org/10.1016/j.neucom.2022.05.099.

[21] Bhanu Chander & Gopalakrishnan Kumaravelan (2022) An Improved 2-Factor Authentication Scheme for WSN Based on ECC, IETE Technical Review, DOI: 10.1080/02564602.2022.2055671 Zhongliang Xie, Lingyun Jiang. (2020). An improved authentication scheme for Internet of things. IOP Conference Series: Materials Science and Engineering. 715. 012031 https://doi.org/10.1088/1757-899X/715/1/012031

[22] Zhanat Kenzhebayeva, Zhanar Akhmetova, Rysgul Bainazarova, Zhanar Kazhenova, Aigul Sariyeva. (2021). Simplified and Secure Authentication Scheme for the Internet of Things. Journal of Theoretical and Applied Information Technology.99 (23):5774-5782.

[23] Muhammad H. Alharbi, Omar H. Alhazmi. (2021). User Authentication Scheme for Internet of Things Using Near-Field Communication. International Journal of Reliability, Quality

and Safety Engineering. 27(5). 2040012. https://doi.org/10.1142/S0218539320400124

[24] Hash-Based Signature for Flexibility Authentication of IoT Devices. HAN Songshen, XU Kaiyong, ZHU Zhiqiang, GUO Songhui, LIU Haidong, LI Zuohui. Wuhan University Journal of Natural Sciences 2022, Vol.27 No.1, 001-010. DOI https://doi.org/10.1051/wujns/2022271001

[25] Lee, Young-Sil & Alasaarela, Esko & Lee, Hoonjae. (2014). An Efficient Encryption Scheme using Elliptic Curve Cryptography (ECC) with Symmetric Algorithm for Healthcare System. International Journal of Security and Its Applications. 8. 63-70. 10.14257/ijsia.2014.8.3.07.

[26] Chien-Ming Chen, Xuanang Li, Shuangshuang Liu, Mu-En Wu, Saru Kumari, "Enhanced Authentication Protocol for the Internet of Things Environment", Security and Communication Networks, vol. 2022, Article ID 8543894, 13 pages, 2022. https://doi.org/10.1155/2022/8543894

[27] Ummer Iqbal, Aditya Tandon, Sonali Gupta, Arvind R. Yadav, Rahul Neware, Fraol Waldamichael Gelana, "A Novel Secure Authentication Protocol for IoT and Cloud Servers", Wireless Communications and Mobile Computing, vol. 2022, Article ID 7707543, 17 pages, 2022. https://doi.org/10.1155/2022/7707543

[28] Li Z, Li J, Zhao S, Chen X, Feng K, Wang W (2022) A blockchain-based lightweight identity authentication scheme for the IEDs of security and stability control system. PLoS ONE 17(3): e0265937. https://doi.org/10.1371/journal.pone.0265937

[29] Bhanu Chander & Gopalakrishnan Kumaravelan (2022) An Improved 2-Factor Authentication Scheme for WSN Based on ECC, IETE Technical Review, DOI: 10.1080/02564602.2022.2055671

[30] S. Chatterjee, A. K. Das, and J. K. Sing, "A novel and efficient user access control scheme for wireless body area sensor networks," Journal of King Saud University-Computer and Information Sciences, vol. 26, no. 2, pp. 181–201, 2014.

[31] Qing Fan, Jianhua Chen, Lazarus Jegatha Deborah, Min Luo, A secure and efficient authentication and data sharing scheme for Internet of Things based on blockchain, Journal of Systems Architecture, Volume 117, 2021,102112, ISSN 1383-7621,https://doi.org/10.1016/j.sysarc.2021.102112.

[32] Saraireh, J., & Joudeh, H. (2022). An Efficient Authentication Scheme for Internet of Things. International Journal of Communication Networks and Information Security (IJCNIS), 13(3). https://doi.org/10.17762/ijcnis.v13i3.3422

[33] Jain K, Kumar A, Singh A. Data transmission reduction techniques for improving network lifetime in wireless sensor networks: An up-to-date survey from 2017 to 2022. Trans Emerging Tel Tech. 2022; e4674. doi: 10.1002/ett.4674

[34] Yadav, C.S., Gupta, S. A Review on Malware Analysis for IoT and Android System. SN COMPUT. SCI. 4, 118 (2023). https://doi.org/10.1007/s42979-022-01543-w

[35] Szymoniak, S.; Kesar, S. Key Agreement and Authentication Protocols in the Internet of Things: A Survey. Appl. Sci. 2023, 13, 404. https://doi.org/10.3390/ app13010404

[36] Foroozan Ghosairi Darbandeh, Masoumeh Safkhani, SAPWSN: A Secure Authentication Protocol for Wireless Sensor Networks, Computer Networks,Volume 220,2023,109469,ISSN 1389-1286,https://doi.org/10.1016/j.comnet.2022.109469.

[37] Srivastava, A., Kumar, A. (2022). A Review of Network Optimization on the Internet of Things. In: Saini, H.S., Sayal, R., Govardhan, A., Buyya, R. (eds) Innovations in Computer Science and Engineering. Lecture Notes in Networks and Systems, vol 385. Springer, Singapore. https://doi.org/10.1007/978-981-16-8987-1_6

[38] A. Srivastava and A. Kumar, "A Review on Authentication Protocol and ECC in IOT," *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 2021, pp. 312-319, doi: 10.1109/ICACITE51222.2021.9404766.