Grenze International Journal of Engineering and Technology, Jan Issue

A Novel Adaptive Unclonable Utility Model for Secure Communication in Internet of Things Environment

Lavina Balraj[1], Dr. A. Prasanth[2] and K. K. Devi Sowndarya[3]
[1]Research Scholar, Department of Electronics and Communication, Engineering, Sri Venkateswara College of Engineering, Sriperumbudur,TamilNadu, India
Email: lavinabalraj2020@gmail.com
[2]Assistant Professor, Department of Electronics and Communication Engineering, Sri Venkateswara College of Engineering, Sriperumbudur, TamilNadu, India
Email: draprasanthdgl@gmail.com
[3]Assistant Professor, Department of Electronics and Communication Engineering, DMI College of Engineering, Tamil Nadu, India

***Abstract*—The security of Internet of Things (IoT) has fascinated more researches on their research endeavor because of the widespread of the implementation of IoT in real-time applications. However, the uniqueness management is considered to be the basic core to formulate a security mechanism. From a fundamental point of loss and identifying the fake, the traditional centralized identity management system continues. This study proposes a new secure communication paradigm based on Blockchain to address IoT's privacy and security concerns. The proposal work includes a secure IoT model taking advantage of Blockchain as the primary framework with Adaptive Unclonable Utility (AUU) recognizing the sensors in a unique way. The major objective of the suggested system is to enhance the Identity Authentication mechanism. The performance result evident that the suggested approach was very powerful and more secure over various attacks.**

***Index Terms*— IoT; Blockchain; Identity management; Adaptive Unclonable Utility.**

I. INTRODUCTION

The IoT, which connects a large number of actuators and sensors, has significantly changed the world. According to a recent Juniper Research, there will be 83 billion IoT interconnections worldwide by 2024, up from 35 billion in 2020 [1-3]. It also hikes a major province about security even though it can be considered as technical improvement. Access control is explored from a realistic angle to design safe IoT. The conventional centralized Internet access control system, however, which depends on Certificate Authority (CA) or extra authenticated servers, runs the danger of having a single point of failure, consumes a lot of resources, and is not scalable. As an alternative, it's essential to explicitly identify the terminating node. Long established product's unique number based on identity is difficult from identity forgery. The smaller number of resources, extensive nodes, and lively topology is complex to achieve from Identity authentication in IoT. On the other hand, authors in [4] separated the identification of items into inherent and imposed characteristics. As with a human thumbprint, the fundamental identification of things would be determined by AUU, a variable and unpredictable

Grenze ID: 01.GIJET.9.1.726

but a repeatable response component [5].
To confirm identification, the AUU-based induced authentication apps, however, employ a Star architecture and single point authentication servers. This structure is not scalable and suffers from a centralized failure. As a result, the notion of a self-sufficient identity is maintained [6]. A decentralized self-reliant identity can be created using blockchain, which is seen as a reassuring technology. The Blockchain gateway, despite being a crucial part of IoT Uniqueness management, is hardly ever addressed in collected works.
The authors of [7] designed a device registration using AUU, method certification, and protocol for secure communication as the protocol for communication between two IoT nodes. Furthermore, authors in [8] enhanced it and proposed a unique strategy for communication involving two nodes. Nonetheless, the crucial framework examined now is the exchange of data between the Blockchain gateway and IoT gadgets. These dual nodules don't take part simultaneously. The secure communication protocol and verification protocol are made clear to fix in the gateway-node communication mode in expectation of reducing the nodes' evaluating load without sacrificing security.
The following are the crucial contributions of the suggested research:

- The blockchain is regarded as the fundamental architecture for identity management in the proposed IoT system.
- A blockchain gateway is established and developed using Raspberry Pi 4 platform.

The proposed work is implemented with the improved AUU-based identity registration and authentication strategy to strengthen the security level and mitigate the Replay and Denial of Service (DoS) attacks.

II. Proposed Blockchain-based IoT Model

The four layers of the IoT system framework focused on blockchain are the implementation layer, gateway clustering layer, terminal junction layer, and blockchain layer according to Figure 1.

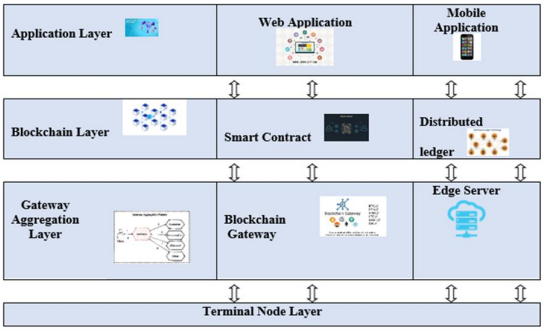

Figure 1: Proposed Blockchain- Based IoT Framework

The sensors and actuator nodes are placed in the terminal junction layer. Various blockchain IoT gateways are included in the layer that clusters gateways. From the viewpoint of the blockchain, the gateway is a full node that keeps a complete backup of all block data. Referring to the blockchain layer, the accord algorithm-based tamper-proof distributive evaluating and cache architecture, which clarifies the negative effects of trust between nodes and the data sent across IoT devices. The web and mobile applications are part of the implementation layer. The blockchain gateway and AUU in junction nodes are two essential components that are highlighted in the proposed architecture.

A. Blockchain Gateway

The blockchain gateway is in charge of caching data in the blockchain and clustering terminal node data in its broadcasting area. Figure 2 illustrates the function blocks that include node enrollment, self-acknowledgement, data decoding, data ownership validation, and data upload block. Since the variety of IoT station nodes, the blockchain gateway might remain adaptive to a wide range of communication protocols, including cabled Ethernet, mobile WiFi, LoRa, and Narrow Band IoT. Utilizing WiFi and LoRa technology, the Raspberry Pi is used to create the blockchain gateway. It is connected with the IoT terminal nodes through the LoRa connection. Additionally, its draughts the node's personality, decodes the data, groups varied data into a substantial message set, emblems the message set by means of the individuality of the node's owner, and sends the message set towards the blockchain.

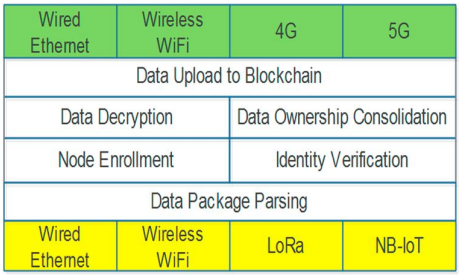

Figure 2: Blocks in proposed method

B. Junction Nodes with AUU

The indisputable identity of the IoT terminal nodes can be created by AUU, but AUU is not with all of the nodes. Currently, only a part of microcontrollers have AUU blocks. The following procedure are adopted to the implementation of AUU based identity:

- Maxim's Max32520, an AUU function is chosen as a secure microcontroller at the stage of designing a device.
- DS28E38, an AUU chip, can be selected as an identity co-processor to increase the device's dependability while the circuit is being designed.
- There are a lot of gadgets that might not have an AUU feature. The Micro Control Unit (MCU) General Purpose Input/output (GPIO) and Analog Digital Converter (ADC) can be utilized to imitate AUU for those devices [9].

III. Proposed Identity Management Protocol Centered on Auu

The device registration conventions and the device confirmation conventions are included in the aforementioned protocols. Beneficial to suit the server-node communication outline, the certification and key swapping protocol in [8] is tolerant and enhanced by including initial encipher to get profit in high safety. In the system architecture, the server referred to in forthcoming conventions representation be able to view as the blockchain gateway. The six tuple parameters (q,b,c,B,n,k,l) [10] over measurable domain Dq are employed in Elliptic Curve Cryptography (ECC), where base point is B. In the preferred conventions, we designate H as a hash function, followed by the symbols || for merging two messages and the whole -or operation is represented by the icon $\oplus$. The conventions use elliptic curve point arithmetic for the summation or repetition.

A. Registration

The model must have several nodes for communication. Each of these nodes must register to the corresponding server underneath the power of its holder previously allotting in the communication network. The registration procedure ought to handle in confident and reliable circumstances. The server arbitrarily selects the private and public key. Here $ds \in Dq$ as taken as its private key and $Ps=dsB$ as its public key. Throughout the registration process, the server gathers several Challenge-Response Pairs (CRPs) from the device, saves them in the databank, and then transmits the public key Ps to the device. This involves a series of the following actions, in that order:

- When a node directs a registration request, registration begins.
- The node stores the key while also receiving Ps from the server. A random challenge (rc) is produced by the server and sent towards the node.
- Following receipt of the challenge, the node obtains the AUU response, R= AUU (rc). The node then transmits to the server (ESN, rc, R), where ESN is the node's eccentric serial number.
- The server adds the database with the parameters (ESN, rc, R)
- Repeat steps 2-4 k times, where k depends on the system's control over the repository area and the security's degree of difficulty. If k is mapped to a larger value, the CRPs repository will need a lot of storage space and the system will have more candidate CRPs, making it harder for attackers to identify the real CRP.

B. Creation of Keys and Certification

(a) Node 1 transmits the communication request to the server with the individual serial number ESN1 and the current timestamp CTS, both encrypted with Es, to initiate the certification process.

$$R = F(ESN_1||CTS, Es) \quad (1)$$

Where E(n,l) represents the ECC encipher among the plaintext n with the key l. Meanwhile, Node1 stores ESN1 and TS for future use.

(b) When the request arrived at the server, it establishes a session, initially it decodes the message with SK:

$$ESN_1 \,||\, CTS = C\,(R, d_s) \quad (2)$$

Where C (a, b) symbolizes the ECC decipher above the cipher text c through the private key k. Additionally, the server extracts the message's ESN1 and CTS. The CRPs database is then searched for elements whose key equals ESN1 there. It then searches CTS in reference with the SN1 only if the result is not equal to null. n an earlier session. As a result, the request needs to be refused because it is a replay attack. In the absence of it, it randomly selects two CRPs from its node, (x1, y1) and (x2, y2). Later, it evaluates

$$x_2' = x_2 \oplus H(R||CTS \,||\, ESN_1) \quad (3)$$

Additionally, a hash value is required to insert to confirm the consistency of the message. The rate for Node1 is evaluated as given below:

$$H1 = h(x1 \,||\, x2 \,||\, CTS) \quad (4)$$

The message x1, x, H1 will be transferred to Node1. The parameters ESN1, R1, R2, TS will be sent to the Server for further use.

(c) Node1 wType equation here.ill try to parse the message once the message is obtained. The message will be consisting of x1, x', H1 parameters with the required size.

Now, Node1 evaluates R1 for x1 with AUU immerged in the node. x2 can be evaluated as follow:

$$x = x_2' \oplus h(R \,||\, CTS \,||\, ESN_1 \quad (5)$$

x1 and x2 can be used to confirm the H1. If h(x1||x2|| CTS)=H1 is false, the message may be copied by the attacker for this reason. In the event that the outcome is accurate, Node1 extracts R2 and arbitrarily selects the p1Dq to evaluate P1=p1G. Later, H2=h(R1||R2||CTS||P1) is calculated. In addition to saving R1, R2 in the session, the message (H2, P1) is also sent to the server.

(d) The server directly confirms H2 for Node1's identity when the message contains (H2, P1) of the predicted length. If not, the node appears to be an unapproved provider. Consequently, the transmission will be intermittent. Else, the server saves P1 and applies it to compute the transmission encode the cipher T:

$$T = d_s \times P_1 = (x_k, y_k) \quad (6)$$

Here, the node and xk, yk are used to encrypt communication while T is the distributed key.

(e) At the node phase, the distributed key also be computed as:

$$T = d_1 \times P_1 = (x_k, y_k) \quad (7)$$

As a result, the key xk, yk is used to encipher the texts communicated amongst the server and node

IV. Results and Discussion

A blockchain network has been built using the Hyper ledger Fabric. The first network of four nodes and the blockchain's genesis block were built using 2 CPU cores, 8 GB of RAM, a 40 GB high-performance cloud storage, and a 5 Mbps network speed are all features of a cloud server. With the aid of the internal Fabric Client module constructed on a 32GB TF-card with 8GB of RAM for the Raspberry Pi 4b, the suggested architecture is integrated into the blockchain through Wi-Fi. The DS28E38 AUU authenticator and STM32L5RBT6 processor are developed for the AUU-enabled terminal node

A. Performance Analysis

The efficiency of the proposed framework has been accessed via two essential metrics such as detection accuracy and average end-to-end delay. The detection accuracy states that the percentage of the suggested methods detect the various attacks accurately [10-12]. Figure 3 depicts the detection accuracy computation. It is noticed from the figure that the proposed framework outperforms fine as compared with the traditional IoT communication models. This is because the AUU algorithm has been established in the suggested model. Typically, the AUU algorithm allows the authorized users to access the cloud environment. It also detects the various DoS attacks with the aid of the proposed model. In contrast, the traditional IoT communication models lagged to provide the secure communication over data transmission. It also failed to detect the DoS attacks which cause lesser detection accuracy than the proposed model.

Figure 4 demonstrates the comparison of average end-to-end delay. It is observed from the figure that the proposed framework achieves reduced delay as compared with the traditional IoT communication models. This is due to the AUU algorithm's incorporation into the suggested model. The AUU algorithm provides quick

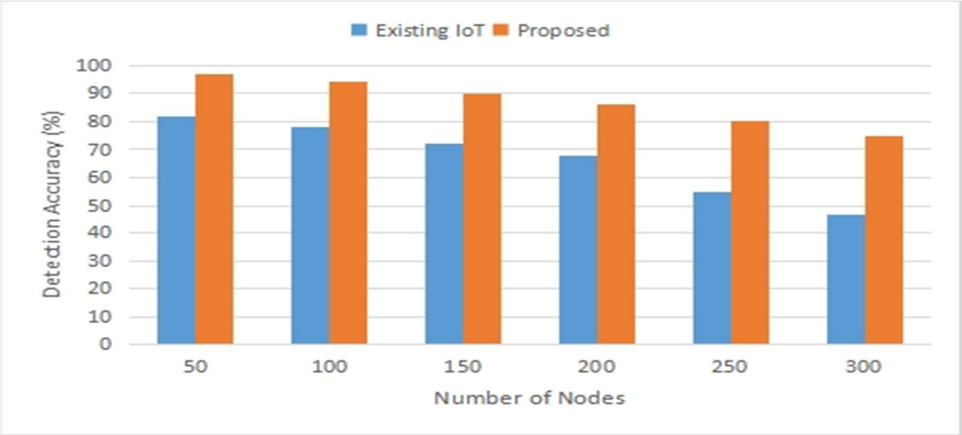

Figure 3: Comparison of detection accuracy for different methods

access to various IoT users. It overlays a way to attain lesser delay in the network. Alternatively, the traditional IoT communication models failed to offer the secure communication and privacy to transmitted data. This cause higher delay than the proposed model.

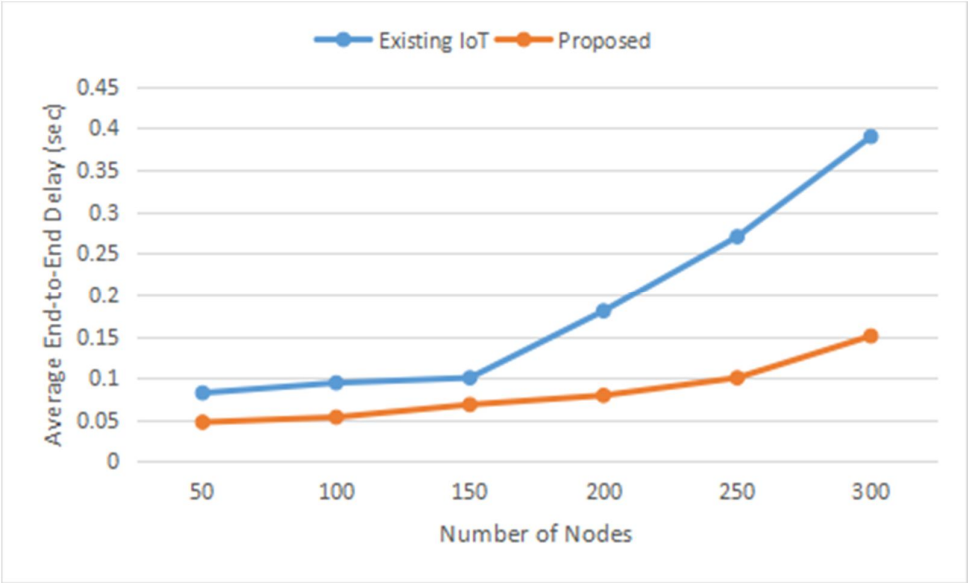

Figure 4: Average end-to-end delay computation

V. Conclusions

The proposed work suggested an IoT system architecture established on blockchain as the evaluating arrangement, with the help of AUU as the identity module for nodes. The proposed blockchain gateway would assist to enhance the registration and certification protocol. This will be done by involving the initial encoding strategy. At last, it also found that the offered scheme is more essential in the certification phase and highly secure by removing the various DoS attacks. The outcomes demonstrate that the recommended structure outperforms the existing IoT design.

References

[1] S Lavanya, A Prasanth, S Jayachitra, A Shenbagarajan, A Tuned classification approach for efficient heterogeneous fault diagnosis in IoT-enabled WSN applications,Measurement 183, 109771:1-20.

[2] A.Prasanth, S.Jayachitra, A novel multi-objective optimization strategy for enhancing quality of service in IoT-enabled WSN applications, Peer-to-Peer Networking and Applications 13 (6), 1905-1920.
[3] Pavelić, Marko, et al. Internet of things cyber security: Smart door lock system. in 2018 international conference on smart systems and technologies (SST). 2018. IEEE.
[4] Maes, Roel, AUU-Based Entity Identification and Authentication, in Physically Unclonable Functions: Constructions, Properties and Applications, R. Maes, Editor. 2013, Springer Berlin Heidelberg: Berlin, Heidelberg. p. 117-141.
[5] Pappu, Ravikanth, et al., Physical one-way functions. Science, 2002. 297(5589): p. 2026-2030.
[6] Tobin, Andrew and Drummond Reed, The inevitable rise of self-sovereign identity. The Sovrin Foundation, 2016. 29(2016).
[7] Chatterjee, Urbi, Rajat Subhra Chakraborty, and Debdeep Mukhopadhyay, A AUU-Based Secure Communication Protocol for IoT. ACM Trans. Embed. Comput. Syst., 2017. 16(3): p. Article 67.
[8] Braeken, An, AUU Based Authentication Protocol for IoT. Symmetry, 2018. 10 (8).
[9] Vaidya, G., T. V. Prabhakar, and L. Manjunath. GPIO AUU For IoT Devices. in GLOBECOM 2020 - 2020 IEEE Global Communications Conference. 2020.
[10] S.Jayachitra, A.Prasanth, An efficient clinical support system for heart disease prediction using TANFIS classifier, Computational Intelligence, 2021, 1-22.
[11] A Prasanth, Certain investigations on energy-efficient fault detection and recovery management in underwater wireless sensor networks, Journal of Circuits, Systems and Computers 30 (08), 2150137:1-13.
[12] SNR Kalli, T Suresh, A Prasanth, T Muthumanickam, K Mohanram, An effective motion object detection using adaptive background modeling mechanism in video surveillance system, Journal of Intelligent & Fuzzy Systems 41 (1), 1777-1789.