IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 11 March 2024, accepted 21 March 2024, date of publication 28 March 2024, date of current version 3 April 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3382508

RESEARCH ARTICLE

IoT-Enhanced Transport and Monitoring of Medicine Using Sensors, MQTT, and Secure Short Message Service

DAVID SAMUEL BHATTI[1], MUHAMMAD MUEED HUSSAIN[2], BEOMKYU SUH[3], ZULFIQAR ALI[4], ISMATOV AKOBIR[5], AND KI-IL KIM[6]

[1]Faculty of Information Technology, University of Central Punjab, Lahore 54000, Pakistan
[2]Department of Computer Science, Institute of Management Sciences, Lahore 54000, Pakistan
[3]Department of Computer Science and Engineering, Chungnam National University, Daejeon 34134, Republic of Korea
[4]Department of Computer Science, National University of Technology, Islamabad 44000, Pakistan
[5]Department of Computer Science and Engineering, Chungnam National University, Daejeon 34134, Republic of Korea
[6]Department of Computer Science and Engineering, Chungnam National University, Daejeon 34134, Republic of Korea

Corresponding author: Ki-Il Kim (kikim@cnu.ac.kr)

This work was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (RS-2023-00237300) and Institute for Information & communications Technology Planning & Evaluation(IITP) grant funded by the Korea Government, [Ministry of Science and ICT (MSIT)], (No. 2022-0-01200, Convergence security core talent training business (Chungnam National University)).

ABSTRACT Since its inception more than a decade ago, Internet of Things (IoT) technology has been guiding people in the development of a world full of smart solutions in which all devices and physical objects, represented as ''things,'' are interlinked with sensors using the Internet. In some areas, the delivery of medications to patients or receivers at their destinations remains highly outdated and informal. In smart medicine delivery, the medicine needs to maintain its original state while facing multiple environmental factors, such as temperature fluctuations, humidity, etc. This paper presents an effective implementation of IoT (Internet of Things) for monitoring the transportation of medicines and vaccines, along with temperature control facilitated through mobile applications and sensor networks. The system employs mobile applications as the user interface, utilizes Arduino, MQTT (Message Queuing Telemetry Transport) for communication, incorporates a temperature sensor, and employs a mini portable cooling box. Designed for the generalized delivery of medicines/vaccines from sender to receiver, the system also suggests CRC-32 as an optimal algorithm for error detection instead of complex hash functions such as MD5 and SHA, ensuring better performance, smooth operation, and data integrity. In addition, elliptic curve-based shared keys are used for protected data transmission. The accuracy of the proposed system is 89.88%, and the value of the F1-score is 0.686, which is greater than the threshold of 0.5, hence conclusively validating the authenticity and reliability of the proposed system.

INDEX TERMS Arduino, Internet of Things, web server, medicine, vaccine, temperature sensor.

I. INTRODUCTION

IoT and sensor communication play a vital role in daily life [1]. Internet of Things refers to everything connected to everything else through the internet, in which different nodes are connected to the network and each other in order to process information, make decisions, and respond to a virtual or physical environment [2]. IoT solutions are investing significantly in propelling the worldwide IoT in smart transportation and medical solutions [3]. In order to function properly in IoT-based smart transportation systems, numerous mechanisms and algorithms are being used [4]. These systems play a crucial role in the operation of railway systems [5], roads [6], flights [7], and ships [8], significantly enhancing the overall customer experience by improving the efficiency, tracking, and forwarding of goods

The associate editor coordinating the review of this manuscript and approving it for publication was Barbara Masini.

TABLE 1. A case study of cost analysis of medicine waste.

Sr.No.	Case Study	Date	Cost/Deaths
1	Vaccination error: the batch of vaccines concerned had been exposed to unacceptably high temperatures in South Sudan [13].	June 2017	Deaths of at least 15 children and the severe illness of 32 others
2	Wastage of medicine due to improper temperature control [14].	2014	15% of overall medicines
3	The biopharma industry alone loses billions annually to temperature failures [14].	2019	$35 billion annually

in transportation. The Internet of Things (IoT) is radically altering the transportation industry [9]. Smart transportation systems are enhancing the mobility of both people and goods, contributing to the overall improvement of the economy, general well-being, security, and environmental sustainability. IoT and sensor networks collaboratively exert significant influence on the healthcare system, offering solutions that facilitate patient care through continuous monitoring of physiological changes and physical activity. Because of these technologies, vital data such as heartbeat, blood pressure, and sugar levels are consistently recorded and transmitted directly to relevant healthcare professionals, even when the patient is not physically present in the doctor's office [10].

Moreover, the healthcare industry operates not only across different cities but also spans international borders, employing aeroplanes and ships to facilitate the swift transportation of medicines [11]. In the healthcare sector, mere transportation alone is insufficient to meet the intended purpose; the safety of medicines during travel is equally critical. In contrast to the large fridges and deep freezers traditionally utilized in pharmacies for medicine management, there are now compact and intelligent fridges/cooling containers that can be conveniently carried along with the medicines during a journey [12]. GPS trackers play a crucial role in monitoring the movement of delivery vehicles. The industry has adeptly leveraged these innovative technologies, integrating them seamlessly to achieve their objectives promptly and securely. However, a significant gap persists in fully monitoring the transportation of medicines and remotely managing the temperature of the system. This gap has led to a dramatic increase in the wastage of medicines, posing a severe risk to people's lives through the consumption of expired drugs. The utilization of expired medicines or vaccines creates a substantial risk of fatalities among consumers. Table 1 shows the impact of medicine expiry and its wastage on human lives and the economy. Visually assessing whether a medicine or vaccine has been exposed to detrimental temperature extremes is impractical. In many cases, there is no significant change, even after harmful exposure. Stakeholders involved in medicine and vaccine transportation remain unaware of the medicine's condition. Key factors such as temperature, humidity, the transporting vehicle, the container or box housing the medicine, and the associated hardware have a direct impact on the medicine's state.

This paper presents a robust and user-friendly system developed for monitoring the transportation of medicine, ranging from distributors, pharmacies, or individuals as senders to recipients, whether individuals or pharmacies. Additionally, the system includes a temperature control feature for refrigerating the medicines during transit. The proposed solution encompasses both hardware and software components, providing a straightforward user interface for ease of use. Furthermore, to ensure message integrity and facilitate error detection during communication, this paper will implement a seamless mechanism aimed at enhancing system efficiency and optimizing battery usage. A careful selection of the most suitable checksum mechanism for the proposed solution will be made among CRC-32, MD5, and SHA-1 [15].

This manuscript is organized in different sections, which are I-Introduction, II-Related Work, III-Proposed Model, VI-Limitations and Challenges, V-New Temperature Detection Methods, IV-Results and Discussion, VII-Conclusion and Future Work.

A. CONTRIBUTIONS

The chosen issue, addressing the secure transportation of medicines, is unique, and the proposed framework is genuinely innovative with the following key contributions:

1) The solution utilizes advanced technologies like sensors, microcontrollers, resource efficient MQTT protocol, and cellular networks to ensure the safe delivery of medicines.
2) Elliptic curve-based shared secret keys are generated for multi-party protected communication.
3) The system ensures equal access to monitoring data for all stakeholders involved in medicine transportation, preventing deception due to adverse environmental conditions like temperature variations.
4) The proposed system has the potential to save lives by preventing expired medicines and reducing pharmaceutical losses by incorporating sensing and backup hardware.

II. RELATED WORK

A preliminary system for a drone-based shipment was developed by Gatteschi et al. [16]. In this study, the architectural framework of the program is initially explored, focusing on hardware specifications. Subsequently, a software framework is outlined to manage and respond to shipment requests. The study particularly addresses challenges associated with fully autonomous parcel deliveries, proposing potential solutions to preemptively mitigate issues within this specific application scope. Given the urgency often associated with medication deliveries and the feasibility of drones for small and lightweight packages, the system is customized for drug consignments. However, it is crucial to acknowledge that the system model could potentially adapt to various other scenarios. While proficient for short-range deliveries,

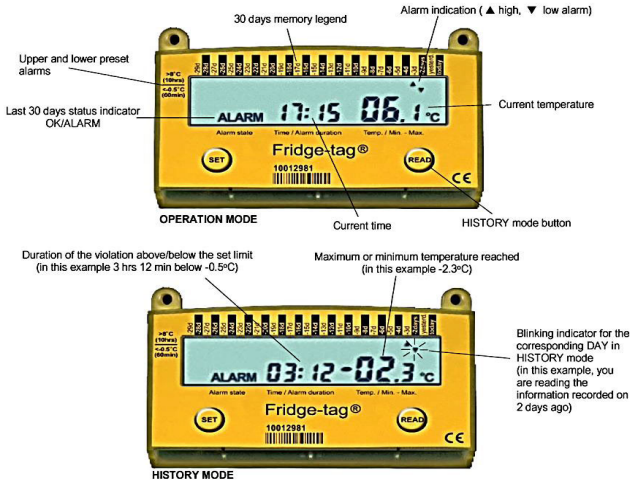

FIGURE 1. 30-day electronic refrigerator temperature logger.

it is important to note that the system is not designed to accommodate large parcels.

By Nanda et al. [17], Blockchain technology is seamlessly integrated with IoT to enhance health supply chain management. The proposed solution introduces decentralized tracking and tracing of medical products, effectively eliminating the risks associated with counterfeit medications. It ensures real-time product status updates throughout the distribution process from the manufacturer to the end-user. Smart contracts, designed using the solidity programming language and implemented on the public permission Ethereum blockchain, play a pivotal role in ensuring security, transparency, and trust in the system. This strategy offers a means to reduce errors and eliminate fraud, minimize delays, limit human interaction, enhance efficiency and accuracy, improve inventory management, and ultimately reduce costs.

WHO pre-qualified and re-validated in 2009 system is featured, equipped with the capability to store temperature readings for 30 days [18]. The system is designed to generate alarming alerts in the event of a deviation from the required temperature range. These recorded readings can be retrieved on the receiving end, providing a means to validate the reliability of the stored medicines. While proficient in recording temperatures and alarms within a 30-day time frame, it's important to note that this system does not have the functionality to control the fridge temperature. The 30-day electronic refrigerator temperature logger is shown in the Figure 1. Lloyd et al. [19] proposed a mechanism that aims to address the issue of vaccine wastage due to accidental freezing by implementing a systematic temperature monitoring approach. This solution necessitates ongoing and vigilant temperature surveillance, integrated into hand-carry boxes to ensure continuous monitoring and prevention of temperature-related issues. Similarly, the solution proposed by Sykes [20] underscores the importance of ensuring the high-quality packaging and delivery of medicines, incorporating measures such as the use of ice to maintain optimal temperatures during shipment. Additionally, the solution advocates for effective communication between stakeholders, emphasizing the need for mutual agreement on delivery timelines. It asserts that both the sender and receiver should coordinate and confirm the delivery time frame based on the distance between them, enabling proper arrangements for a successful and timely delivery process.

Konovalenko and Ludwig [21] given a drone-mediated medicine distribution system to remote locations has witnessed increased attention in recent years. However, there is a notable scarcity of information pertaining to the feasibility and impacts of drone delivery for medications, underscoring the significance of this study. Employing pharmacopoeial methodologies, the study delves into the effects of vibration and temperature on insulin, simulating crucial parameters during drone flight. The research demonstrates the preservation of insulin quality through human insulin testing, even after exposure to conditions mimicking a 30-minute drone delivery (temperatures ranging from -20 to $+40$ $\circ$C, vibration frequencies between 0 and 40 Hz). With the exception of a minor bubble formation post-takeoff, no adverse effects were observed on Act fast following drone transportation. To the best of the authors' knowledge, this marks the inaugural instance of utilizing a drone to assess insulin quality, providing compelling evidence for the feasibility of drone transportation in maintaining pharmaceutical stability and medication quality. Consequently, this study establishes a foundation for future research ventures exploring diverse drug classes, environmental influences, or alternative drone models. Loisel et al. [22] underscore the critical importance of temperature monitoring in medicine to ensure patient safety and maintain product quality using machine learning approaches. Despite significant advancements in temperature monitoring devices driven by the Internet of Things (IoT), challenges persist, particularly in the Cold Chain of medicine. Balachandar and Chinnaiyan [23] introduced a unique conceptual model that comprehensively addresses temperature monitoring challenges within the medical cold chain, considering perspectives from both the pharmaceutical and healthcare industries. This model is versatile, and applicable not only to pharmaceutical logistics but also to temperature-controlled laboratory medicine and vaccine cold chains. Its innovative approach paves the way for the development of an Internet of Things-based intelligent Cold Chain temperature monitoring system, aiming to enhance responsiveness by identifying areas for improvement and analyzing flaws in the existing Cold Chain processes.

Liu et al. [24] proposed a system that utilizes the Raft consensus algorithm to enhance throughput and the Blockchain Distributed Network (BDN) with bloXroute servers for improved network scalability. The hybrid approach incorporates multiple cryptographic techniques for privacy and security, offering adaptability to system requirements. The model allows for the addition or removal of components, and the use of alternative consensus algorithms for higher fault

tolerance, addressing network bottleneck challenges through bloXroute implementation.

Stringent international regulations govern shipping and storage temperatures in the cold chain, crucial for ensuring the quality and safety of goods, particularly temperature-sensitive items like medications and food. Incorrect handling of these items poses risks to public health and the economy. Vivaldi et al. [25] proposed a novel solution to address temperature-related challenges during medical supplies transportation, a modified RFID tag with a copper-doped ionic liquid was employed to detect temperature thresholds, unaffected by humidity changes. This tag permanently changed upon surpassing the ionic liquid's melting point, adjustable through dopant concentration. The introduction of copper ions facilitated melting and freezing point adjustments, providing a cost-effective solution for identifying cold chain breakdowns in transporting temperature-sensitive goods. The modified RFID tags enable non-contact acquisition of information from multiple packages simultaneously, offering a versatile and economical means of monitoring the cold chain.

A. CONCLUSION OF LITERATURE REVIEW

Examining the existing literature reveals a significant technology gap in the secure transportation of medicines, with minimal attention dedicated to this critical area. Our evaluation underscores the opportunity to guarantee the safe and secure transit of medicines by harnessing state-of-the-art sensing and information and communication technologies, including sensors, micro-controllers, MQTT, 5G, etc. that are neglected in prevailing solutions.

III. PROPOSED MODEL

The proposed model is given in Figure 2, which clearly depicts the flow of the system, overall, the designed architecture is capable of delivering medicine/vaccine safely and securely to the end users with use of the latest tools and technologies such as IoT devices, sensors, smart fridge, MQTT, client application, database and remote server. MQTT is a lightweight, open-standard protocol designed for efficient machine-to-machine communication in resource-constrained IoT environments over ordered, lossless, and bi-directional connections, typically utilizing TCP/IP or potentially QUIC (Quick UDP Internet Connections) [26]. MQTT QoS (Quality of Service) levels 0, 1, and 2 refer to the different levels of message delivery guarantees between the MQTT broker and the client. QoS 0 provides the lowest assurance of delivery, as the message is sent with the expectation that it may be lost or delivered multiple times. QoS 1 requires the sender to receive an acknowledgment (ACK) from the receiver, which may lead to potential duplicate deliveries. QoS 2 uses a four-step handshake process to ensure the message is delivered exactly once, eliminating the possibility of duplicates. QoS 0 is preferred due to the low-resource environment.

CRC codes are ubiquitously employed for detecting data transmission and errors. The common examples of CRCs include CRC-16-CDMA2000 deployed in 3G mobile networks, CRC-CCITT utilized for Bluetooth, CRC-24 applied in Long-Term Evolution (LTE), CRC-32 utilized in Ethernet and High-Level Data Link Control (HDLC) protocols, and CRC-40-GSM employed in the GSM control channel. If the probability of undetected error is given by the expression 1 with n as the degree of the CRC polynomial (CRC length) and k as the number of errors, then the probability of error detection of CRC-40>CRC-32>CRC-24>CRC-16, which implies an increase in computing complexity in the same order.

$$P_{\text{unDetectErr(CRC-n)}} \approx 1 - \left(1 - \frac{1}{2^n}\right)^k \tag{1}$$

CRC-32 is selected due to its significant error detection property and lower computational complexity than CRC-40. It is energy efficient compared with MD5 and the family of SHA message authentication protocols, and it is also highly efficient in terms of hardware and software implementation. As far as CRC encoding is concerned, it is done by multiplying a message polynomial $M(x)$ with the term x^n, followed by division by a generator polynomial $g(x)$ of degree n. The resulting remainder, represented as $r(x) = M(x) \cdot x^n \bmod g(x)$, constitutes the CRC check bits. The addition of these check bits to $M(x) \cdot x^n$ generates a codeword: $M(x) \cdot x^n + r(x)$. CRC decoding conventionally involves dividing the received message by the shared generator polynomial $g(x)$ and then comparing the coefficients of the obtained remainder with CRC check bits. A mismatch in bits indicates an error [27]. Algorithm 1 shows the simplicity and ease of the code to be implemented on the hardware. Similarly, it is

Algorithm 1 CRC32 Calculation Algorithm

```
Input: data: Input data for CRC32 calculation
procedure GenerateCRCTable
    for i ← 0to255 do
        crc ← i
        for j ← 0to7 do
            crc ← (crc ≫ 1) ⊕ (CRC32_POLYNOMIAL & (−(crc & 1)))
        crc32_table[i] ← crc
function CalculateCRC32(data, length)
    crc ← 0xFFFFFFFF                ▷ Initial CRC32 value
    for i ← 0tolength − 1 do
        crc ← (crc ≫ 8) ⊕ crc32_table[(crc ⊕ data[i]) & 0xFF]
    return crc ⊕ 0xFFFFFFFF         ▷ Final XOR operation
```

believed that symmetric key cryptography is more efficient in terms of large or frequent data encryption as compared to public key cryptography, which requires more resources and infrastructure and consumes more energy. In the realm of IoT, traditional asymmetric cryptography methods like

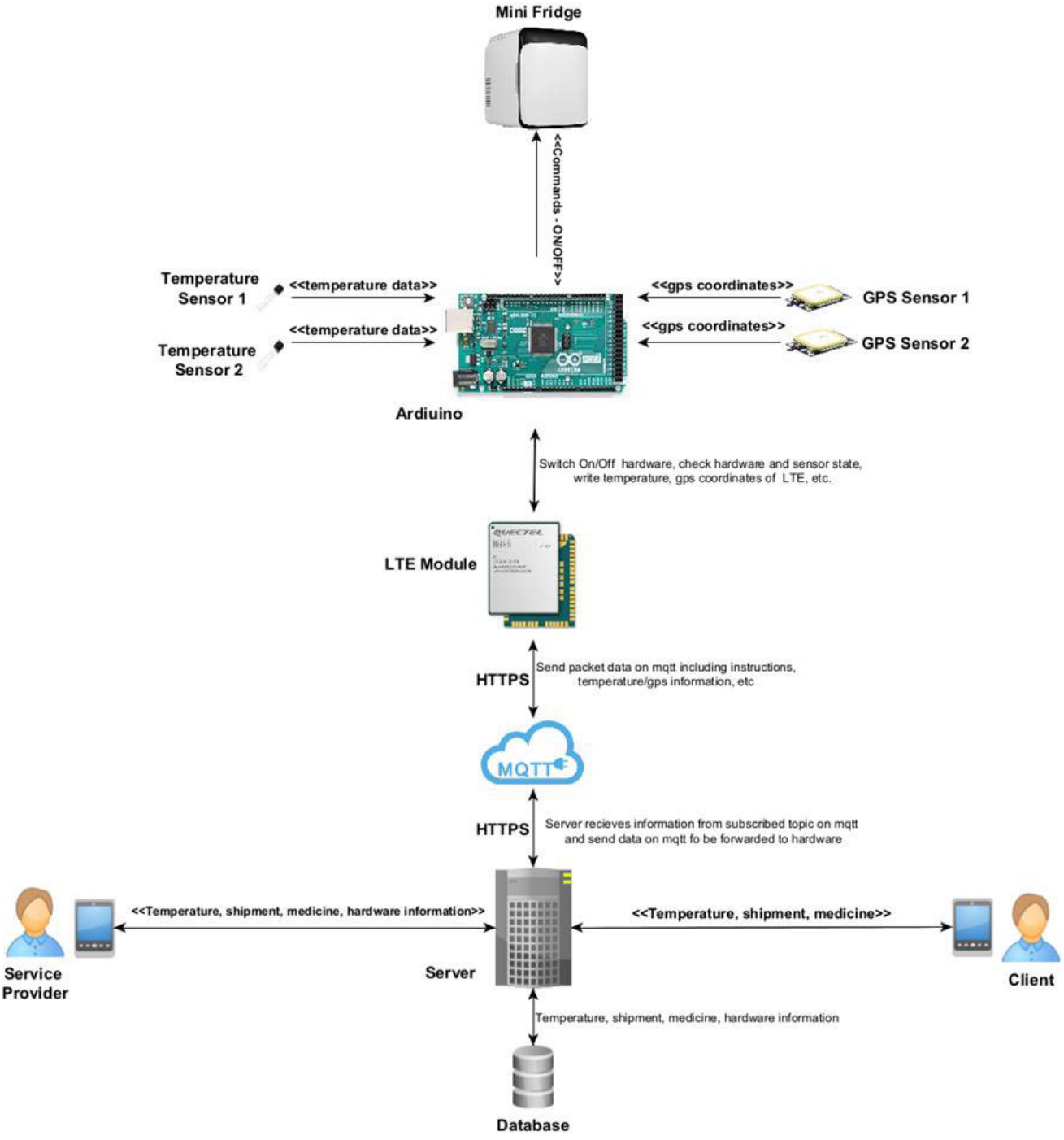

FIGURE 2. Proposed model.

RSA pose challenges due to resource-intensive computations. To address this, we propose lightweight alternatives, such as Elliptic Curve Diffie-Hellman (ECDH) with AES-256. ECDH outperforms DH and RSA in terms of key length and performance. In fact, the ECC 160-bit key security is equal to the 1024-bit key security of RSA and DH. The Diffie-Hellman (DH) key exchange is a mathematical protocol facilitating secret key exchange between two parties, A and B, based on an agreed-upon group G and a fixed group element g. A group is a mathematical set of elements with defined operations that combine two elements to produce a third element within the group. For secret key sharing in the DH protocol, each party generates a private random number. If A generates a and broadcasts g^a, and B generates b and

broadcasts g^b, the common secret is g^{ab}. The security of this protocol relies on the discrete log problem's difficulty in the given group, which is to find a given g^a and g. ECDH key exchange protocol, which is based on DH, is considered for establishing a shared secret key between the sender (A), the recipient (B), and the medicine container (C) through bi-linear pairing-based cryptography, as shown in Figure 4 [28], [29]. The primary difference between DH and ECDH is that the former operates on numbers while the latter uses curve points [30].

An elliptic curve defined over real numbers in its "standard form," is represented by the equation $y^2 = x^3 + ax + b$, where a and b are fixed values, and $4a^3 + 27b^2 \neq 0$. This elliptic curve forms an abelian group, where the addition operation is a group operator. Consequently, the curve follows the properties of closure, associativity, identity, inverse, and commutativity with respect to the addition of points on the elliptic curve. For adding two points $P(x_1, y_1)$ and $Q(x_2, y_2)$ on the curve to get the third point $R(x_3, y_3)$, the following rules are followed:

1- If points P and Q have distinct x and y coordinates, the addition of P and Q (i.e., R) involves reflecting the result about the x-axis, forming the point $-R$. This point is the intersection of the straight line connecting P and Q with the curve. The coordinates x_3 and y_3 are determined by calculating the slope of the line PQ as $m = \frac{y_2 - y_1}{x_2 - x_1}$ and then computing $x_3 = m^2 - x_1 - x_2$ and $y_3 = m(x_1 - x_3) - y_1$.

2- In the case of two overlapping points, a tangent is drawn at point P, intersecting the curve at $-R$. The addition of the two points results in $R = P + P$. The coordinates x_3 and y_3 are found by first calculating the slope of the tangent line as $m = \frac{3x_1^2 + a}{2y_1}$ and then determining $x_3 = m^2 - x_1 - x_2$ and $y_3 = m(x_1 - x_3) - y_1$.

3- When adding the points $P(x_1, y_1)$ and $-P(x_1, -y_1)$, the line connecting these two points does not intersect the curve at a third point. The intercepting point is at infinity, denoted as the point of infinity $\mathcal{O}$, serving as the additive identity of the group $(P + (-P) = \mathcal{O})$.

4- To find kP, where k is a scalar number, point P is added k times, expressed as $kP = P + P + \ldots + P$ k times.

We recommend the Barreto-Naehrig (BN) curve, which is commonly expressed in the Weierstrass form, defined by the equation $y^2 = x^3 + b$, where x, y are coordinates and b is a constant term. The BN curve parameters vary based on the chosen values, with BN256 being a standardized instance characterized by the equation $y^2 = x^3 + 3$. BN256 operates over a 256-bit prime field and finds extensive use in pairing-based cryptography [31], [32]. BN256 elliptic with addition of two points P and Q as R and its image as -R image is shown in Figure 3.

For the purpose of group key sharing, we propose a tripartite Diffie-Hellman protocol that utilizes the Weil pairing, as introduced by Joux in 2000. This protocol operates on an elliptic curve denoted as E, featuring two independent base points, P and Q implying that no integer d exists such that $P = d \cdot Q$ or $Q = d \cdot P$. In the key generation phase, each

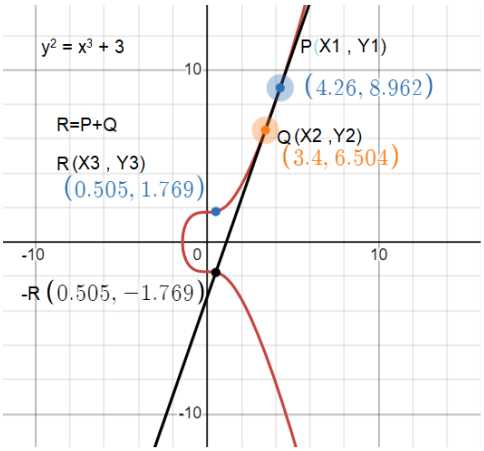

FIGURE 3. BN256 elliptic curve.

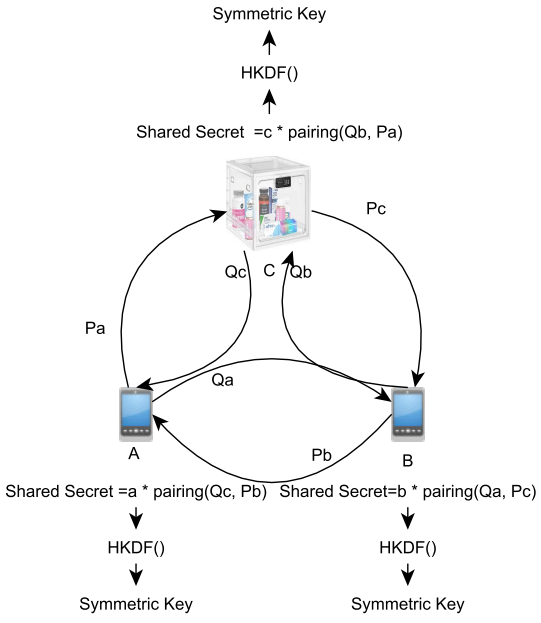

FIGURE 4. Group key generation.

participant, User A, B, and Container C, selects a secret key value: a, b, and c respectively. The public keys, represented as points on the elliptic curve, are denoted as (Pa, Qa), (Pb, Qb), and (Pc, Qc), where $P_i = d_i \cdot P$ and $Q_i = d_i \cdot Q$. Users share the public part of the shared key to be generated with one another. Shared secret key computation is shown in Algorithm 2 where each participant (at A, B, and Container C) computes their shared secret using the Weil pairing [33]. The shared secret is a point of an elliptic curve that is passed to the HMAC-based Extract-and-Expand Key Derivation Function (HKDF) to generate a 256-bit symmetric key [34], [35]. This symmetric is used for encrypted communication between A, B, and C using block cipher AES-256.

The shared secret computed using the Weil pairing should be hard to drive given the public keys (PA, QA), (PB, QB), and (PC, QC) are available to adversaries.

Algorithm 2 Tripartite Diffie-Hellman With Weil Pairing

Input: Elliptic curve E, independent base points P and Q
Initialize: Secret keys a, b, and c for User-A, User-B, and User-C
Compute and broadcast public keys:
User-A: $(P_a, Q_a) = (a \cdot P, a \cdot Q)$
User-B: $(P_b, Q_b) = (b \cdot P, b \cdot Q)$
User-C (Container): $(P_c, Q_c) = (c \cdot P, c \cdot Q)$
Compute shared secret and symmetric key using the HMAC-based Extract-and-Expand Key Derivation Function (HKDF) [34]
User-A:
$SharedSecret_{ABC} = F(a, P_b, Q_c) = F(a, Q_b, P_c) = e(P_b, Q_c)^a$
$SymmetricKey = HKDF(SharedSecret_{ABC})$
User-B:
$SharedSecret_{ABC} = F(b, P_a, Q_c) = F(b, Q_a, P_c) = e(P_a, Q_c)^b$
$SymmetricKey = KDF(SharedSecret_{ABC})$
Container-C:
$SharedSecret_{ABC} = F(c, P_A, Q_B) = F(c, Q_a, P_b) = e(P_a, Q_b)^c$
$SymmetricKey = HKDF(SharedSecret_{ABC})$

But such security solutions, while computationally secure, may be vulnerable to breaches with powerful adversaries, while information-theoretic cryptography solutions will offer resilience in the future [36].

To initiate the process, the system involves two key actors: the sender and the receiver. This process revolves around the reliable shipment of medicines or vaccines. The sender, typically a service provider, initiates the shipment by creating an order and placing the medicine into a smart fridge or a container designed to maintain a specific temperature range. The screen layouts used for start shipment and user selection are shown in Figures 5 and Figure 6 respectively. The smart fridge, secured with a password, requires a PIN code for access; this code is securely delivered to the customer via email upon order creation. The smart fridge, managed by an Arduino, is equipped with temperature and GPS sensors to ensure optimal conditions during transportation. Despite these precautions, the challenge to medicine's reliability arises during transit, where the fridge encounters fluctuating temperatures due to variations throughout the day, differing climates in various areas, and the immediate environmental conditions impacting the fridge's performance.

During the transportation of medicine, temperature sensors play a pivotal role in overseeing and broadcasting the temperature levels, promptly alerting the Arduino system to any fluctuations. If the temperature falls below the required range for the medicine, the Arduino instructs the fridge to initiate cooling, safeguarding the medicine from expiration due to adverse conditions. This dual-sensor approach enhances the safety measures, with a primary temperature sensor taking the lead and a secondary sensor serving as a reliable backup. In the event of a failure in the primary sensor, an immediate notification is sent to the service provider, who can remotely activate the backup temperature sensor through the client application. Additionally, two GPS sensors are integrated to provide real-time location updates to both the sender and receiver. Similar to the redundancy in temperature sensors, dual GPS sensors are employed to bolster system efficiency and reliability. This comprehensive sensing and notification system ensures the secure and well-monitored transport of medicines or vaccines.

Every piece of data throughout the entire process will be meticulously recorded. The Arduino, equipped with both temperature and GPS sensors, will transmit this data to a remote server via an LTE module using the secure HTTP protocol, functioning as a gateway. Subsequently, the module forwards the data to an MQTT broker, which, in turn, pushes the information to the remote server via the HTTP protocol; the basic operations of MQTT are given in Algorithm 3. Both the sender and the receiver will have access to relevant data through their respective mobile applications. For instance, the receiver's application will display comprehensive details, including GPS coordinates and temperature records. To maintain a historical record and preserve all shipment details, the data will be stored in a database.

Algorithm 3 MQTT Algorithm

Initialize: Broker:=ServerIP, Publisher:=Fridge, Subscriber:=Sender, Receiver, Topic:=Medicine Fridge State
Connect to Broker:
Publisher $\xrightarrow{\text{Connect}}$ Broker
Subscriber $\xrightarrow{\text{Connect}}$ Broker
Publish a Message:
Publisher $\xrightarrow{\text{Publish(topic, message)}}$ Broker
Broker stores and forward messages to subscribers
Subscribe to a Topic:
Subscriber $\xrightarrow{\text{Subscribe(topic)}}$ Broker
The broker adds a subscriber to the list for a specified topic
Receive Published Messages:
Broker forwards message to subscribers in the topic
Unsubscribe from a Topic:
Subscriber $\xrightarrow{\text{Unsubscribe(topic)}}$ Broker
The broker removes subscribers for a specified topic
Disconnect:
Publisher $\xrightarrow{\text{Disconnect}}$ Broker
Subscriber $\xrightarrow{\text{Disconnect}}$ Broker

Upon the completion of the shipment, the end user can issue a command to unlock the fridge through the application, utilizing the secure PIN code sent to it via email at the initiation of the shipment. The screen shown in Figure 7 is used for authentication purposes that demand this PIN. This meticulous data recording and secure access system ensures transparency, accountability, and reliability throughout the entire shipment process. Mobile security of different mobiles and business applications can also be ensured through different suggestions and recommendations, such as MVP, app right management, and inspection (anti-virus McAfee, CLAMAV, Bit Defender) [37]. Algorithm 4 lays out the

detailed functionality of the proposed model that clearly describes the functions of different elements of the solution.

Algorithm 4 Medicine Transportation Monitoring

Initialize medicine fridge with Arduino module and GSM chip.
Connect sensors to the Arduino for temperature and status monitoring.
Set up an MQTT server for messaging.
For the Diffie-Hellman key exchange
Make use of ECDH Tri-Partite Algorithm 2
Encrypted Data Transmission:
procedure Data_Transfer()
    while Medicine Transportation is ongoing **do**
        if One cooling fan fails **then**
            Activate the backup cooling fan.
        if Temperature is outside the specified range **then**
            Adjust cooling fan speed to regulate temperature.
        Read data from fridge sensors.
        CRC ← CalculateCRC32(data) Algorithm 1
        User-C $\xrightarrow{\text{CRC} \parallel \text{AES\_Encryption(Data, Symmetric Key)}}$ User B, A
        Transmit encrypted data and *CRC* to sender and receiver mobile screens using MQTT.
        Store data securely in the database.
procedure MedicineContainerUnlocking()
    Sender:
    Generate a unique code.
    Encrypt the code using a 256-bit ECDH symmetric key.
    Compute CRC for the encrypted code.
    Transmit encrypted code and CRC via MQTT Algorithm 3 to the receiver.
    Receiver:
    Receive encrypted code and CRC via MQTT Algorithm 3.
    Decrypt the code using the ECDH symmetric key.
    Verify the integrity of the code using the CRC.
    User Interaction:
    Enter the code to open the container.
    Container Access Control:
    if Entered code is correct **then**
        Open the medicine container.
    else
        Do not open the container.

A. IMPLEMENTATION

The system is implemented using different hardware and software components. A brief description of these components is given in Table 2.

IV. RESULTS AND DISCUSSIONS

A. TEMPERATURE RECORDING AND REPORTING TEST

In the testing phase of the monitoring system, every feature integrated into the application demonstrated optimal performance, consistently yielding the anticipated results. To assess the efficacy of the proposed solution in mitigating the environmental impact on medicine during transportation, a rigorous 20-day testing period was conducted on insulin. Throughout this duration, the transportation box was personally carried from home to the workplace, with daily temperature averages recorded. The testing parameters maintained a scale range between 2 degrees Celsius and 8 degrees Celsius to simulate real-world conditions. The choice of insulin, a commonly used and temperature-sensitive medication, served as a stringent test case, providing valuable insights into the system's reliability under challenging

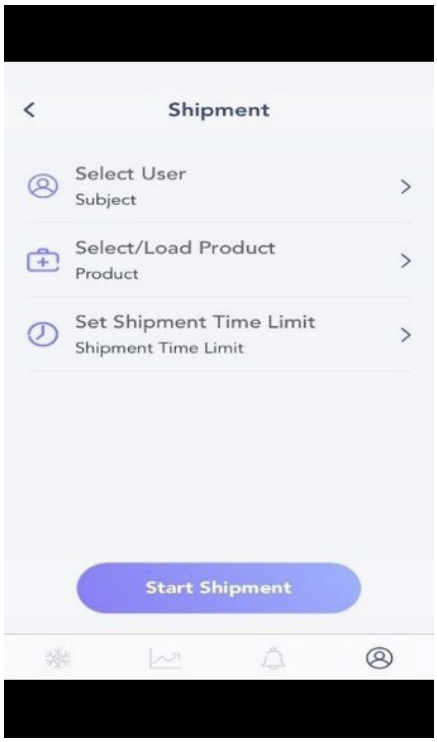

FIGURE 5. Start shipment.

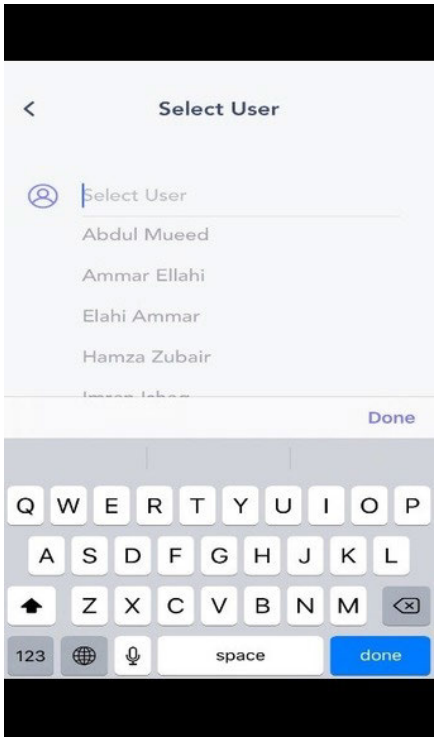

FIGURE 6. Select user.

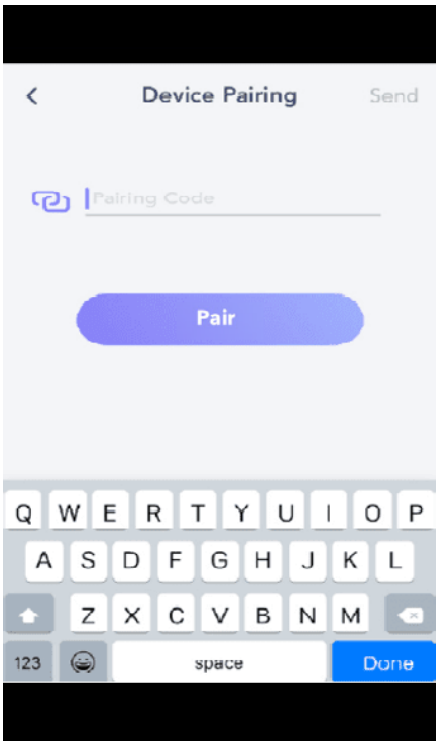

FIGURE 7. Shipment authentication.

TABLE 2. Hardware and software components.

Sr.No.	Name	Details
1	Arduino MEGA2560	a micro-controller board
2	Refrigerator / Thermal box	A box/fridge capable of storing and securing the state of medicine
3	Relay	To control the circuit
4	GPS	To find the location of something on Earth
5	Temperature Sensor	A box/fridge capable of storing and securing the state of medicine, Temperature Sensor is LM35
6	LTE Module	A cellular communications device
7	Cloud MQTT	A lightweight publisher/subscriber protocol, , MQTT Quality of Service Level 0
8	Webserver	To process and manage requests and responses from client system
10	MySQL	A relational database management system
11	Mobile application	To access application features on devices

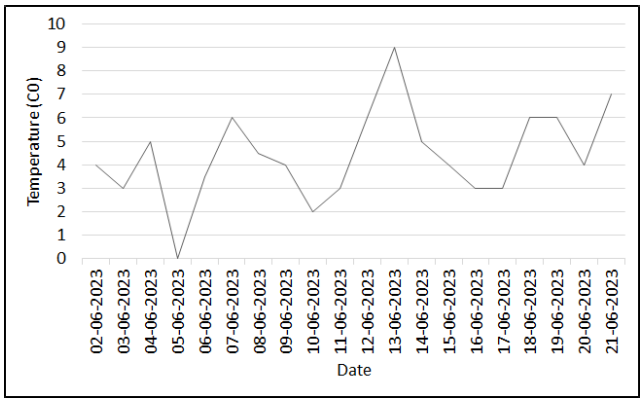

FIGURE 8. Temperature history of 20 days.

TABLE 3. Analysis of CRC, MD5, and SHA on 1 GB of data.

Sr.No.	Hashing Algorithm	Execution time (milliseconds)	Resources usage (%)	Battery drop %
1	CRC-32	972 - 1138	11	1
2	MD5	28660- 31431	34	3
3	SHA-1	33402-34318	36	4

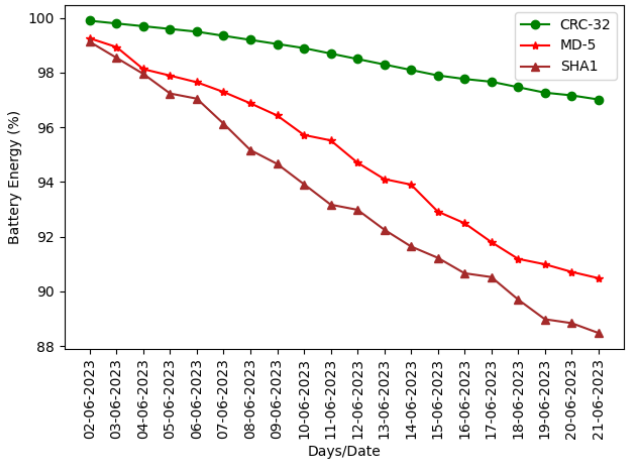

FIGURE 9. Energy drainage analysis [20-day trial].

circumstances. According to Figure 8 taken from the data generated by the system, the temperature remained within range for the majority of days. In 20 days, only once did it go below 2 degrees Celsius and once slightly above 8 degrees Celsius.

B. INTEGRITY TEST

After running MD5, CRC32, and SHA-1 using 1GB of data produced by the system on the fully charged Arduino, we got the results shown in Table 3.

The findings indisputably show that CRC32 is the most efficient solution for low-level devices and hardware components. Its use not only saves battery power but also improves the system's overall performance and durability. Furthermore, taking into account the amount of data produced by Arduino, it is around 100,000 bytes per day. In order to finalize the best algorithm for the given system, Figure 9 depicts the performance of CRC-32, MD5, and SHA-1 over 20 days. Hence, it is evident that CRC exhibited significantly faster execution times with minimal impact on resources such as the battery. In contrast, running the other two algorithms resulted in higher resource consumption and slightly increased hardware demands.

In the context of hashing for low-level devices, the evidence presented above strongly supports the conclusion that CRC32 is the most advantageous choice. Its efficiency

TABLE 4. Confusion matrix table.

Total records = 840	Predicted without alert	Predicted with alert
Actual without alert	True negative = 662	False positive = 15
Actual with alert	False negative = 70	True positive = 93
	732	108

in terms of speed, resource utilization, and minimal impact on hardware makes it a standout solution for applications where these factors are paramount. Choosing CRC32 not only ensures effective hashing but also enhances the overall performance and resource management of low-level devices.

C. DATA COMMUNICATION TEST

The test is conducted to verify the bidirectional communication between the server application and the device microcontroller via Cloud MQTT. Over 20 days, we initiated 20 shipments to assess the system's performance, subjecting it to diverse situations and circumstances. Throughout the 20-day trial, not a single packet was missed when the network was accessible, with successful encoding and decoding occurring on both ends. Whenever there is network unavailability, data packets are stored locally and subsequently pushed to the server once connectivity is restored. This process ensures data integrity and resilience. As depicted in Figure 10, the data is then transmitted to Cloud MQTT, becoming accessible to the devices.

D. NOTIFICATION ALERT TEST

Over the 20-day shipment period, the testing focus was primarily on the crucial aspects of the application, with a particular emphasis on notification alerts. The significance of these alerts lies in their pivotal role in ensuring the medicine's reliability. They serve as a real-time update mechanism, keeping users informed about the current state of the medicine during transit. Throughout the trial of these 20 shipments, a comprehensive assessment of 840 temperature records was conducted. While the system was expected to generate 108 temperature alerts, it exceeded expectations by producing a total of 163 alerts. This robust performance underscores the effectiveness and responsiveness of the notification system in providing timely and accurate information.

Now for data analysis, we will use the confusion matrix (Table 4). It is a useful tool for determining the variables that impact accuracy and precision.

Now we need to calculate accuracy [38], error rate, precision [38], true positive rate [39], false positive rate [39], true negative rate, prevalence, and F-score [40] from Table 4, and the results are given in Table 5.

The aforementioned calculations were conducted to comprehensively assess various aspects of the system through an analysis of the data using a confusion matrix, widely regarded as one of the best methods for evaluating system performance. Upon running the confusion matrix, it was determined that the accuracy of the notification alerts is 0.89, indicating that this classifier is accurate 89% of the time.

To measure the performance of the system, another important coefficient is used. The Matthews Correlation Coefficient (MCC) is a statistical measure designed to evaluate the effectiveness of a binary categorization system. It accounts for true positives, true negatives, false positives, and false negatives and gives an equitable metric even when the groups are of varying sizes [41]. The Equation 2 formula defines the MCC:

$$MCC = \frac{(TP * TN - FP * FN)}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}} \tag{2}$$

Where TP is the number of true positives, TN is the number of true negatives, FP is the number of false positives, and FN is the number of false negatives.

By putting in the values we got from Table 5 in MCC Equation 2, we get a value of 0.65, as shown in the mathematical expression 3.

$$MCC = \frac{(93 * 662 - 15 * 70)}{\sqrt{(93 + 15)(93 + 70)(662 + 15)(662 + 70)}} = 0.65 \tag{3}$$

The MCC score falls between -1 and $+1$, with $+1$ representing excellent prediction, 0 representing no better than random prediction, and -1 representing complete disagreement between forecast and observation. Overall, a higher MCC value indicates greater classifier performance. Based on this, our system produced 0.65, which is more than half way better than 0 and closer to $+1$.

The purpose of the notification alert test is to check the validity of the proposed framework when the container is moved from one location to another. We could not test for longer distances but for a short distance that is from lab to home and home to lab; on average, the distance is 35-40 kilometers. It is tested in hot summers where temperatures may vary from 40C^o - 47C^o and cellular service may also be disrupted in some areas or may become weak in overcrowded passages due to rush hours. Close investigations reveal that moisture and humidity, the aging of sensors, and inappropriate sensor placement may cause FNR and FPR. So, the following actions are recorded for reducing FNR and FPR:

1) ADVANCED FILTERING ALGORITHMS

Advanced filtering algorithms, such as Kalman filters or low-pass filters, can be explored to smooth temperature data and reduce the impact of short-term fluctuations [42], [43].

2) REDUNDANCY AND CROSS-VALIDATION

Redundancy and cross-validation for temperature sensors are also suggested, with redundant sensors deployed and consensus algorithms developed to cross-validate readings [44].

3) PERIODIC REVIEW, AND MAINTENANCE

Periodically reviewing and updating the error detection algorithm based on system performance and evolving

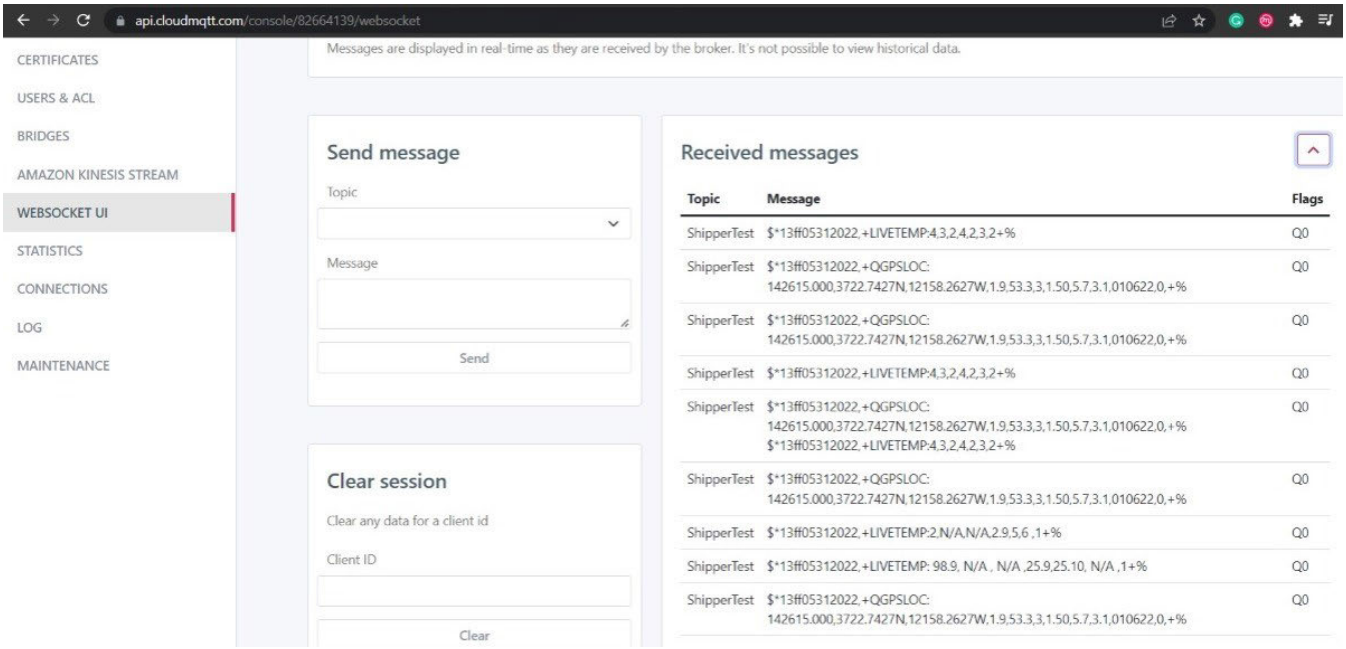

FIGURE 10. Data packets on cloud mqtt.

TABLE 5. Confusion matrix calculations.

Evaluation Metrics	Formula	Result
Accuracy	(True positive + True negative) / (Total records)	(93 + 662) / 840 = 89.88%
Error rate	1 - Accuracy	1 - 0.89 = 0.101
Precision	True positive / Predicted with alert	93 / 100 = 0.86
True positive rate	True positive / Actual with alert	93 / 163 = 0.570
False positive rate	False positive / Actual without alert	15 / 677 = 0.02
True negative rate	True negative / Actual without alert	662 / 677 = 0.97
Prevalence	Actual with alert / Total	163 / 840 = 0.19
F-score	True positive / True positive + (FP + FN) / 2	93 / 93 + (15+70) / 2 = 0.686

requirements, regularly updating shared keys for secure data transmission, employing best practices for key management, and implementing protocols for detecting and mitigating security breaches to ensure the authenticity of transmitted data may also reduce FNR and FPR.

V. USING NEW TEMPERATURE DETECTION METHODS

The proposed solution does not introduce or invent any novel methods for temperature detection. Instead, it leverages state-of-the-art temperature sensing technology to conduct temperature measurements. This concise explanation assists in making informed decisions when selecting the most suitable approach for the given scenario. For instance, the LM35 temperature sensor is conventionally semiconductor-based and can be interfaced with Arduino; there are others that are not semiconductor-based but provide high precision and can be interfaced with Arduino. The most relevant are given below.

1) The DS18B20 is a OneWire temperature sensor with a wide temperature range, high accuracy, and programmable resolution. It supports multiple sensors on a single bus and communicates over a single digital pin. It has good accuracy, which is +/-0.5∘C (at -10 to 85∘C) [45], [46].
2) TMP1826 is a OneWire sensor, that is also compatible with Arduino libraries. It offers high precision and a OneWire interface for simplified wiring [47].
3) Infrared thermopile sensors such as the MLX90616ESF-HCA use the Seebeck effect to measure temperature and can be interfaced with Arduino using protocols like I2C. They offer non-contact temperature measurements and are suitable for measuring surface temperatures. Some models offer digital outputs [48].

These sensors are not traditional semiconductor-based but provide digital output and can be easily interfaced with Arduino microcontrollers. It is important to consider the specific requirements of an application, such as temperature range, accuracy, and interfacing preferences, along with checking datasheets and Arduino libraries for compatibility and ease of integration.

VI. LIMITATIONS AND CHALLENGES

1) The proposed solution is based on cellular networks; communications may be disrupted if the service is

not available in any region, and information about medicines exposure to hostile environmental factors cannot be obtained. Multiple service providers may be required to ensure the robustness of the proposed system.

2) sensors may behave poorly and may report inaccurate readings due to moisture, aging of the sensor hardware, electromagnetic interference, voltage fluctuations, direct contact with the heating surface, and an abrupt change in temperature.
3) MQTT supports three QoS levels (0, 1, 2), but higher QoS levels come with increased overhead and may impact performance, especially in low-bandwidth or high-latency environments.

VII. CONCLUSION AND FUTURE WORK

An innovative system has been introduced to monitor medication distribution and regulate the temperature of medicines during transportation, addressing the issue of medicine waste and potential harm caused by environmental factors. The system uses electronic sensors, GPS, and temperature sensors to reduce errors and cater to those who may not be computer professionals. The cloud-based system allows supervisors to remotely connect and monitor data, ensuring medicines are consistently maintained within a reasonable temperature range. The system also proactively notifies users of temperature fluctuations, providing real-time awareness of the medicine's status. This technology demonstrates the effectiveness of IoT in integrating digital devices and transforming the global landscape into a real-time display. Despite the security mechanisms used by MD5 and SHA, CRC excels in speed, making it a recommended choice for enhanced performance. Statistical measures like accuracy and F1-score confirm the credibility and effectiveness of the proposed solution.

In the future, we want to enhance the proposed solution with blockchain-based technology that can make the real-time readings of sensors and the state of the medicine container immutable. Blockchain technology offers a promising solution for data protection and distributed sharing as it is a decentralized and distributed ledger technology that ensures transparency, security, and immutability of data. Blockchain's immutability makes it difficult to alter data, providing a robust layer of protection against unauthorized modifications or tampering.

REFERENCES

[1] M. Majid, S. Habib, A. R. Javed, M. Rizwan, G. Srivastava, T. R. Gadekallu, and J. C.-W. Lin, "Applications of wireless sensor networks and Internet of Things frameworks in the industry revolution 4.0: A systematic literature review," *Sensors*, vol. 22, no. 6, p. 2087, Mar. 2022.

[2] I. Azimi, A. M. Rahmani, P. Liljeberg, and H. Tenhunen, "Internet of Things for remote elderly monitoring: A study from user-centered perspective," *J. Ambient Intell. Humanized Comput.*, vol. 8, no. 2, pp. 273–289, Apr. 2017.

[3] V. S. Naresh, S. S. Pericherla, P. S. R. Murty, and S. Reddi, "Internet of Things in healthcare: Architecture, applications, challenges, and solutions," *Comput. Syst. Sci. Eng.*, vol. 35, no. 6, pp. 411–421, 2020.

[4] D. Oladimeji, K. Gupta, N. A. Kose, K. Gundogan, L. Ge, and F. Liang, "Smart transportation: An overview of technologies and applications," *Sensors*, vol. 23, no. 8, p. 3880, Apr. 2023.

[5] *World Summit on the Information Society Outcome Documents*, Int. Telecommun. Union, Geneva, Switzerland, 2005.

[6] G. Mao, Y. Hui, X. Ren, C. Li, and Y. Shao, "The Internet of Things for smart roads: A road map from present to future road infrastructure," *IEEE Intell. Transp. Syst. Mag.*, vol. 14, no. 6, pp. 66–76, Nov. 2022.

[7] S. Chakraborty, T. Chakravorty, and V. Bhatt, "IoT and AI driven sustainable practices in airlines as enabler of passenger confidence, satisfaction and positive WOM : AI and IoT driven sustainable practice in airline," in *Proc. Int. Conf. Artif. Intell. Smart Syst. (ICAIS)*, Mar. 2021, pp. 1421–1425.

[8] S. Aslam, M. P. Michaelides, and H. Herodotou, "Internet of Ships: A survey on architectures, emerging applications, and challenges," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9714–9727, Oct. 2020.

[9] W. D. Hoyer, M. Kroschke, B. Schmitt, K. Kraume, and V. Shankar, "Transforming the customer experience through new technologies," *J. Interact. Marketing*, vol. 51, pp. 57–71, Aug. 2020.

[10] A. El Attaoui, S. Largo, A. Jilbab, and A. Bourouhou, "Wireless medical sensor network for blood pressure monitoring based on machine learning for real-time data classification," *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 9, pp. 8777–8792, Sep. 2021.

[11] A. Musamih, K. Salah, R. Jayaraman, J. Arshad, M. Debe, Y. Al-Hammadi, and S. Ellahham, "A blockchain-based approach for drug traceability in healthcare supply chain," *IEEE Access*, vol. 9, pp. 9728–9743, 2021.

[12] E. N. Mambou, S. M. Nlom, T. G. Swart, K. Ouahada, A. R. Ndjiongue, and H. C. Ferreira, "Monitoring of the medication distribution and the refrigeration temperature in a pharmacy based on Internet of Things (IoT) technology," in *Proc. 18th Medit. Electrotech. Conf. (MELECON)*, Apr. 2016, pp. 1–5.

[13] BBC news. (2017). *South Sudan Vaccination Error Kills 15 Children*. [Online]. Available: https://www.bbc.com/news/world-africa-40135814

[14] AirCargo News. (2019). *Failures in Temperature-Controlled Logistics Cost Biopharma Industry Billions*. [Online]. Available: https://www.aircargonews.net/sectors/pharma-logistics/failures-in-temperature-controlled-logistics-cost-biopharma-industry-billions/

[15] H. Zhuoyu and L. Yongzhen, "Design and implementation of efficient hash functions," in *Proc. IEEE 2nd Int. Conf. Power, Electron. Comput. Appl. (ICPECA)*, Jan. 2022, pp. 1240–1243.

[16] V. Gatteschi, F. Lamberti, G. Paravati, A. Sanna, C. Demartini, A. Lisanti, and G. Venezia, "New frontiers of delivery services using drones: A prototype system exploiting a quadcopter for autonomous drug shipments," in *Proc. IEEE 39th Annu. Comput. Softw. Appl. Conf.*, vol. 2, Jul. 2015, pp. 920–927.

[17] S. K. Nanda, S. K. Panda, and M. Dash, "Medical supply chain integrated with blockchain and IoT to track the logistics of medical products," *Multimedia Tools Appl.*, vol. 82, no. 21, pp. 32917–32939, Sep. 2023.

[18] Ü. Kartoğlu, E. Nelaj, and D. Maire, "Improving temperature monitoring in the vaccine cold chain at the periphery: An intervention study using a 30-day electronic refrigerator temperature logger (fridge-tag®)," *Vaccine*, vol. 28, no. 24, pp. 4065–4072, May 2010.

[19] J. Lloyd, P. Lydon, R. Ouhichi, and M. Zaffran, "Reducing the loss of vaccines from accidental freezing in the cold chain: The experience of continuous temperature monitoring in Tunisia," *Vaccine*, vol. 33, no. 7, pp. 902–907, Feb. 2015.

[20] C. Sykes, "Time- and temperature-controlled transport: Supply chain challenges and solutions," *Pharmacy Therapeutics*, vol. 43, no. 3, p. 154, 2018.

[21] I. Konovalenko and A. Ludwig, "Comparison of machine learning classifiers: A case study of temperature alarms in a pharmaceutical supply chain," *Inf. Syst.*, vol. 100, Sep. 2021, Art. no. 101759.

[22] J. Loisel, S. Duret, A. Cornuéjols, D. Cagnon, M. Tardet, E. Derens-Bertheau, and O. Laguerre, "Cold chain break detection and analysis: Can machine learning help?" *Trends Food Sci. Technol.*, vol. 112, pp. 391–399, Jun. 2021.

[23] S. Balachandar and R. Chinnaiyan, "Reliable pharma cold chain monitoring and analytics through Internet of Things edge," in *Emergence of Pharmaceutical Industry Growth With Industrial IoT Approach*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 133–161.

[24] X. Liu, A. V. Barenji, Z. Li, B. Montreuil, and G. Q. Huang, "Blockchain-based smart tracking and tracing platform for drug supply chain," *Comput. Ind. Eng.*, vol. 161, Nov. 2021, Art. no. 107669.
[25] F. Vivaldi, B. Melai, A. Bonini, N. Poma, P. Salvo, A. Kirchhain, S. Tintori, A. Bigongiari, F. Bertuccelli, G. Isola, and F. Di Francesco, "A temperature-sensitive RFID tag for the identification of cold chain failures," *Sens. Actuators A, Phys.*, vol. 313, Oct. 2020, Art. no. 112182. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0924424720301606
[26] B. Mishra and A. Kertesz, "The use of MQTT in M2M and IoT systems: A survey," *IEEE Access*, vol. 8, pp. 201071–201086, 2020.
[27] E. Dubrova, M. Näslund, and G. Selander, "CRC-based message authentication for 5G mobile technology," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Aug. 2015, pp. 1186–1191.
[28] S. Ricci, P. Dzurenda, J. Hajny, and L. Malina, "Privacy-enhancing group signcryption scheme," *IEEE Access*, vol. 9, pp. 136529–136551, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID
[29] A. Menezes. (2005). *An Introduction to Pairing-Based Cryptography*. [Online]. Available: https://api.semanticscholar.org/CorpusID
[30] B. Buchanan. (Apr. 30, 2023). *Elliptic Curve Integrated Encryption Scheme (ECIES): Encrypting Using Elliptic Curves, ASecuritySite: When Bob Met Alice*. Accessed: Mar. 10, 2024. [Online]. Available: https://medium.com/asecuritysite-when-bob-met-alice/elliptic-curve-integrated-encryption-scheme-ecies-encrypting-using-elliptic-curves-dc8d0b87eaa
[31] W. J. Buchanan. (2024). *Tripartite Diffie–Hellman Algorithm With BN256*. Accessed: Feb. 7, 2024. [Online]. Available: https://asecuritysite.com/keyexchange/go_bn256
[32] P. Dzurenda, S. Ricci, J. Hajny, and L. Malina, "Performance analysis and comparison of different elliptic curves on smart cards," in *Proc. 15th Annu. Conf. Privacy, Secur. Trust (PST)*, Aug. 2017, pp. 365–36509.
[33] A. Joux, "A one round protocol for tripartite Diffie–Hellma," in *Algorithmic Number Theory*. Berlin, Germany: Springer, 2000, pp. 385–393.
[34] H. Krawczyk and P. Eronen, "HMAC-based extract-and-expand key derivation function (HKDF)," IBM Res. Nokia, Internet Eng. Task Force (IETF), NY, USA, Tech. Rep. 5869, 2010. [Online]. Available: https://www.rfc-editor.org/rfc/rfc5869
[35] W. J. Buchanan. (2024). *Ecdh With Golang and Kryptology*. Accessed: Mar. 10, 2024. [Online]. Available: https://asecuritysite.com/ecdh/go_ecdh
[36] D. S. Bhatti and S. Saleem, "Ephemeral secrets: Multi-party secret key acquisition for secure IEEE 802.11 mobile ad hoc communication," *IEEE Access*, vol. 8, pp. 24242–24257, 2020.
[37] D. S. Bhatti, N. A. Saqib, and Z. Anwar, "SCEAMS: Secure corporate environment adhered to mobile & smartphones," in *Proc. 6th Int. Conf. Innov. Comput. Technol. (INTECH)*, Aug. 2016, pp. 561–566.
[38] R. Yacouby and D. Axman, "Probabilistic extension of precision, recall, and F1 score for more thorough evaluation of classification models," in *Proc. 1st Workshop Eval. Comparison NLP Syst.*, 2020, pp. 79–91.
[39] D. van Ravenzwaaij and J. P. A. Ioannidis, "True and false positive rates for different criteria of evaluating statistical evidence from clinical trials," *BMC Med. Res. Methodol.*, vol. 19, no. 1, pp. 1–10, Dec. 2019.
[40] C. Goutte and E. Gaussier, "A probabilistic interpretation of precision, recall and F-score, with implication for evaluation," in *Proc. Eur. Conf. Inf. Retr.* Santiago de Compostela, Spain: Springer, Mar. 2005, pp. 345–359.
[41] D. Chicco and G. Jurman, "The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation," *BMC Genomics*, vol. 21, no. 1, pp. 1–13, Dec. 2020.
[42] X. Zhang, H. Liang, J. Feng, and H. Tan, "Kalman filter based high precision temperature data processing method," *Frontiers Energy Res.*, vol. 10, Apr. 2022. [Online]. Available: https://www.frontiersin.org/articles/10.3389/fenrg.2022.832346, doi: 10.3389/fenrg.2022.832346.
[43] Y. Zhang, R. Wang, S. Li, and S. Qi, "Temperature sensor denoising algorithm based on curve fitting and compound Kalman filtering," *Sensors*, vol. 20, no. 7, p. 1959, Mar. 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/7/1959
[44] R. H. Dodier, "Unified prediction and diagnosis in engineering systems by means of distributed belief networks," Ph.D. dissertation, Dept. Civil, Environ., Architectural Eng., Univ. Colorado, Boulder, CO, USA, 1999.
[45] D. Yulizar, S. Soekirno, N. Ananda, M. A. Prabowo, I. F. P. Perdana, and D. Aofany, "Performance analysis comparison of DHT11, DHT22 and DS18B20 as temperature measurement," in *Proc. 2nd Int. Conf. Sci. Educ. Sci.*, 2022, pp. 37–45, doi: 10.2991/978-94-6463-232-3_5.
[46] ANSpecified. (2024). *DHT11 Vs DHT22 Vs LM35 vs DS18B20 Vs BME280 Vs BMP180*. Accessed: Mar. 7, 2024. [Online]. Available: https://randomnerdtutorials.com/dht11-vs-dht22-vs-lm35-vs-ds18b20-vs-bme280-vs-bmp180/
[47] T Instruments. (May 2023). *TMP1826 1-Wire®, 4±0.2°C Accurate Temperature Sensor With 2Kb EEPROM*. Accessed: Mar. 7, 2024. [Online]. Available: https://www.ti.com/lit/ds/symlink/tmp1826.pdf?ts=1709754722978&ref_url=https%253A%252F%252Fwww.ti.com%252Fproduct%252FTMP1826
[48] Melexis. (Aug. 2012). *MLX90616ESF-HCA Infra Red Thermometer in to-39 for High Temperature Thermometer Guns*. Data Sheet. Accessed: Mar. 7, 2024. [Online]. Available: https://www.melexis.com/en/product/MLX90616/Thermal-Infrared-Thermopile-Sensor-High-Temperature-Measurements

DAVID SAMUEL BHATTI received the Ph.D. degree in computer science (information security) from the School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Islamabad, Pakistan, in 2020. He is currently an Assistant Professor with the University of Central Punjab (UCP), Lahore, Pakistan. His research interests include networks, mobiles, and smartphones security. His expertise extends to secure routing protocols, secret key establishment, and device authentication, particularly in low-resource devices like wearable, body-worn, and wireless body area network (WBAN) devices. His current research interests include the design of security protocols using probabilistic data structures. The aim is to optimize time and space complexity in low-resource devices, enhancing their efficiency, and robustness in the realm of information security.

MUHAMMAD MUEED HUSSAIN received the B.S.C.S. degree from Virtual University and the M.Phil. degree in computer science from the Institute of Management Sciences, Pakistan. He is currently a Renowned AI and IoT Researcher with expertise in information security, wireless networks, and software programming. With over ten years of experience, he is also a Senior Software Engineer with Invensify Ltd. He focuses on securing communication protocols, optimizing wireless network performance, and developing robust software solutions.

BEOMKYU SUH received the B.S. and M.S. degrees in computer engineering from Chungnam National University, Daejeon, South Korea, in 2022 and 2024, where he is currently pursuing the Ph.D. degree. His research interests include wireless sensor networks and deep reinforcement learning.

ZULFIQAR ALI received the Ph.D. degree in computer science from the National University of Computer and Emerging Sciences, Islamabad. He is currently an accomplished Assistant Professor. With extensive teaching experience, he is also with the National University of Technology. His research interests include AI, optimization, and networks, particularly in computational intelligence and swarm intelligence. He received a Research Exchange Fellowship with Arizona State University, in 2014. Apart from his teaching roles, he actively contributes to conferences, including the Frontiers of Information Technology. He has supervised research projects and published extensively in reputable journals. His commitment to academic excellence is evident in his continuous contributions to the field of computer science.

ISMATOV AKOBIR received the B.S. degree from Woosong University, Daejeon, South Korea, in 2023. He is currently pursuing the M.S. degree with Chungnam National University. His research interests include machine learning and wireless networks.

KI-IL KIM received the M.S. and Ph.D. degrees in computer science from Chungnam National University, Daejeon, South Korea, in 2002 and 2005, respectively. He is currently with the Department of Computer Science and Engineering, Chungnam National University. He has been with the Department of Informatics, Gyeongsang National University, since 2006. His research interests include machine learning for networks, wireless/mobile networks, fog computing, MANET, QoS for wireless, and wireless sensor networks.