Received: 12 February 2024 | Revised: 15 June 2024 | Accepted: 4 July 2024

IET Wireless Sensor Systems

DOI: 10.1049/wss2.12086

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

Enhancing offloading with cybersecurity in edge computing for digital twin-driven patient monitoring

Ahmed K. Jameil[1,2] | **Hamed Al-Raweshidy**[1]

[1]College of Engineering, Design and Physical Sciences, Brunel University London, Uxbridge, UK

[2]Department of Computer Engineering, University of Diyala, Baqubah, Iraq

Correspondence

Hamed Al-Raweshidy.
Email: Hamed.Al-Raweshidy@brunel.ac.uk

Funding information

Brunel University London, Grant/Award Number: K015

Abstract

In healthcare, the use of digital twin (DT) technology has been recognised as essential for enhancing patient care through real-time remote monitoring. However, concerns regarding risk prediction, task offloading, and data security have been raised due to the integration of the Internet of Things (IoT) in remote healthcare. In this study, a new method was introduced, combines edge computing with sophisticated cybersecurity solutions. A vast amount of environmental and physiological data has been gathered, allowing for thorough understanding of patients. The system included hybrid encryption, threat prediction, Merkle Tree verification, certificate-based authentication, and secure communication. The feasibility of the proposal was evaluated by using an ESP32-Azure IoT Kit and Azure Cloud to evaluate the system's capacity to securely send patient data to healthcare institutions and stakeholders, while simultaneously upholding data confidentiality. The system demonstrated a notable improvement in encryption speed, with 27.18%, represented as the improved efficiency and achieved storage efficiency ratio 0.673. Furthermore, the evidence from the simulations showed that the system's performance was not affected by encryption since encryption times continuously remained within a narrow range. Moreover, proactive alert of probable security risks would be detected from the predictive analytics, hence strong data integrity assurance. The results suggest the proposed system provided a proactive, personalised care approach for cybersecurity-protected DT healthcare (DTH) high-level modelling and simulation, enabled via IoT and cloud computing under improved threat prediction.

KEYWORDS

biosensors, body area networks, body sensor networks, cloud computing, computer network security, data integrity, decision making, health care, internet of things, patient monitoring

1 | INTRODUCTION

The combination of the Internet of Things (IoT) and sophisticated sensing technologies has caused a notable transformation in healthcare, particularly via advancements such as remote patient monitoring and predictive analytics. These technological innovations optimise healthcare service provision, speed data processing, and increase patient outcomes and well-being. An innovative and revolutionary contribution to this particular subject is the emergence of the concept of digital twin (DT) [1–3]. DT provides an exact virtual representation of a patient's physiological and clinical features, enabling accurate diagnoses and customised treatment approaches. These virtual models mirror the potential reactions of a patient to various therapies, resulting in healthcare that is more tailored and efficient. In addition, DT improves predictive abilities by constantly updating in real-time with data from IoT devices, enabling proactive healthcare management [4, 5]. In terms of cybersecurity, DT plays a vital role not only in healthcare delivery but also in network protection. By using simulation and prediction techniques, healthcare organisations may proactively enhance their defensive measures against prospective cyber attacks. This ensures the protection of confidential patient data and the robustness of healthcare systems against cyberattacks.

Consequently, the convergence of IoT, sophisticated sensing technology, and DT is fostering the development of precision medicine and safe healthcare ecosystems, ushering in a new era [6–8].

Digital Twin in healthcare (DTH) has the most promising capability to boost patient care and results by creating a virtual replica of a physical object. DTH is composed of three primary parts: The physical object, the digital object, and the link between them. The physical object represents the real-world item or process being modelled, for example, a patient or sensor device. Meanwhile, the digital object is the digital model that accurately mirrors the physical object's characteristics and behaviours in real-time. The connection between the physical object and the digital object involves continuous data exchange, ensuring that the digital twin remains up-to-date and accurately reflects any changes in the physical object. This DTH is fed data from wearable devices, electronic health records, and other equipment and is kept up-to-date in real time to yield a live model that is able to simulate and predict a patient's health status. It enables healthcare providers to forecast disease progression, run treatment scenarios, and tailor care plans, facilitating personalised healthcare [9, 10].

For example, it can simulate heart function, helping doctors better investigate heart disease and improve their diagnostic and treatment decisions. Digital twins could potentially help in this by providing a representation of drug response in a given individual, leading to more personalised treatment or pharmacotherapy. The ultimate goal is to tailor the implementation away from random drug dispensing practices towards therapeutic paradigms utilising only effective drugs [11]. The four steps of the digital twin operating mechanism are model construction, data connection, simulation validation, and model evolution. These DTH models feed actual objects and service systems with continuous optimisation and iteration depending on needs and real-time conditions. Digital twins also provide a useful platform for carers, family members, stakeholders, and medical professionals to practise and model risk-free difficult medical procedures. Healthcare professionals' abilities are improved, and their knowledge of current procedures is maintained through continual professional development, which eventually results in better patient care. By knowing how different people respond to different medications and therapies, digital twins help personalised medicine by supporting treatment plans and optimising drug prescriptions [12]. Therefore, combining DT with immersive healthcare provides an excellent and low-cost medical solution as treatments can be customised, tested, and validated before administration, which in turn reduces associated risks in the medical sector [13]. Digital Twin is valuable within healthcare to prevent treatments and model diseases, save money, and create independence and availability for patients [14].

The use of a DT in healthcare involves the development of a secular twin in order to simulate different scenarios and predict their outcomes. Subsequently, any data collected from physical sensors becomes part of the digital model, which is processed using the sophisticated analytic capabilities and machine learning algorithms incorporated into the twin. Wireless sensor networks (WSNs) and body area networks (BANs) serve as a channel for transmitting the data between the digital twin and the patient's body, gathering essential information, and transferring it to the duplicator. Such a system ensures continuous and personalised patient monitoring that allows one to predict deterioration or complications and act on a timely basis. Thus, the use of a DT in healthcare will help to prevent extreme conditions and create personalised programs for every patient [15].

However, in digital twin healthcare (DTH), WSNs and BANs do not only transmission data and analyse; they reinforce the cybersecurity of the system. Using complex encryption policies and secure communication protocols, these networks protect the data's integrity and privacy as it is sent from the physical area to the digital field. As a result, this prevents cybercriminals from accessing the sensitive health information [16].

Despite these steps forward, data processing speed limitations within the current state of technology and data security concerns, as well as numerous inefficiencies of DT, continue to be a significant barrier to the widespread adoption of IoT in healthcare. Thus, one promising framework for a new paradigm for secure handling of sensitive data within IoT is edge computing [17, 18]. Various studies have addressed these challenges, exploring the precision of personal navigation with inertial sensors, the deployment of ontology-based methodologies for intelligent rehabilitation, and the development of innovative routing algorithms to improve IoT communication within smart cities [19–22]. Furthermore, research has underscored the critical importance of robust cybersecurity measures, given the significant consequences of potential intrusions into health information [23–25].

The incorporation of blockchain into software-defined networking (SDN) for better security and management, protocol architecture for effective routing and congestion control, and advanced sinkhole attacks against mechanisms in IoT for smart homes are critical steps in the further evolution of cybersecurity protocols in concepts based on Edge Computing and cybersecurity systems for patient monitoring using the digital twin [26–28]. However, existing solutions have not adequately addressed the myriad challenges at the intersection of DTH and cybersecurity, creating a significant gap in the field.

The system developed in this study overlaps two of the most critical areas, DTH and cybersecurity. The new system is a novel design that offers an effective approach to the integration of edge computing and advanced cybersecurity methods. The primary focus is, therefore, the development of a flexible IoT platform and a reliable cybersecurity framework to realise real-time patient monitoring securely. The features include hybrid encryption, certificate-based authentication, Merkle Tree verification, and secured communication channels system. The main contributions of this study are:

1. Development of a Novel System: The study proposes a unique system that integrates edge computing and sophisticated cybersecurity measures specifically designed for

DTH applications. This system is tailored to enable secure, real-time patient monitoring.
2. Flexible IoT platform application: The system includes multiple sensors for collecting wide arrays of physiological data, which eases the implementation of the IoT solution in real-life medical practice.
3. Establishment of a Robust Security Framework: By employing hybrid encryption, certificate-based authentication, Merkle Tree verification, and secure communication protocols, the system ensures enhanced data security and integrity throughout the data transmission process.
4. Comprehensive Assessments: The study conducts thorough evaluations, including operational benchmarks and performance comparisons with existing systems, to assess the system's efficiency.
5. Proof of Concept: The study presents a proof of concept using the ESP32-Azure IoT Kit, which is a low-power, sensor-intensive device to prove the protocol's viability and performance.

These contributions highlight the study's innovative approach to integrating edge computing and cybersecurity in DTH, offering a significant advancement in secure healthcare monitoring.

The structure of this article has been organised as follows: Section 2 is dedicated to the exploration of related work, and Section 3 shows the framework of cybersecurity for DTH. The proposed methodology is detailed in Section 4, Section 5 provides a security analysis of the proposed network, its efficiency, and how cyberthreats were addressed, and performance metrics are discussed in Section 6. System evaluation is presented in Section 7. The proof of concept for the proposed methodology is illustrated in Section 8, followed by a discussion in Section 9, and concluding remarks in Section 10.

2 | RELATED WORK

Digital twins, initially developed for industrial and aerospace applications, have recently gained significant traction in the healthcare industry. These technologies are now being utilised as valuable resources to generate real-time digital representations of physical systems [29, 30]. Studies have indicated that applications of digital twins have positively impacted patient outcomes, particularly in the realm of personalised medicine and predictive analytics [31]. Remote monitoring systems, playing a crucial role in healthcare, especially in chronic illness management and post-operative care, have evolved significantly [?]. Historically, these systems predominantly utilised single-sensor devices, such as pulse oximeters or heart rate monitors, to gather disease-specific health data [18]. Although the collection of multisensor data is not a new concept, its application in healthcare has been somewhat fragmented across various contexts [17]. Recently, efforts have been made to incorporate multisensor technologies into healthcare, aiming for a more holistic approach to patient monitoring [23].

In the realm of blockchain technology, various consensus algorithms have been developed, including bespoke adaptations of Practical Byzantine Fault Tolerance and Proof of Authentication. One significant advancement permits low-end IoT devices to engage in transactions on the Ethereum blockchain through platforms like Infura, circumventing the necessity of operating a full node [32]. However, the integration of resource-limited IoT devices with the Ethereum network encounters a substantial hurdle due to the considerable energy demands associated with transaction transmissions via Wi-Fi or cellular networks. Moreover, the current economic incentive structure presents its own set of challenges. As of the writing of this article, the monetary worth of one Nodl token is approximately 0.006 USD. With an active node count on the network reaching nearly 4.6 million, this represents a mere 0.065% of the total global mobile devices [33]. A predominant focus of Helium Hotspot devices in the United States, Europe, and East China [34] highlights a significant geographical limitation in network coverage. This uneven distribution means that large swathes of the globe remain devoid of adequate Helium network connectivity for IoT devices, a situation primarily attributed to the varied pace of regulatory approvals across different regions. Given the relatively recent emergence of Helium hotspots and the network's ongoing maturation, manufacturers are confronted with the lengthy and complex task of obtaining certification for their devices. This certification process is crucial to ensure adherence to local radio regulations, thereby facilitating the safe deployment of hotspots in respective countries.

DT technology has found applications in diverse sectors, extending well beyond healthcare. Marksteiner et al. explored the use of cyber-digital twins (CDTs) in enhancing vehicle cybersecurity testing [35]. Sun et al. proposed the integration of lightweight DT with federated learning (FL) for air-ground networks [36]. Yao et al. introduced deep reinforcement learning (DRL) for optimal Internet of Vehicles (IoV) edge computation offloading [37]. Li et al. developed an approach for synchronised proven data possession in DTs, ensuring data integrity in dispersed settings [38]. Zhu et al. proposed a cooperative provable data possession scheme to address related challenges [39]. As the diverse applications of DTs are examined, it is crucial to consider the foundational technologies enabling these implementations. In the healthcare sector, DTs are particularly valuable for predicting cybersecurity risks. Utilising real-time monitoring and pattern recognition, these models can proactively detect abnormalities or suspicious activities, functioning as an early warning system against potential cyber-attacks. The integration of DTH systems adds a crucial layer of protection within complex cybersecurity environments, enhancing system resilience [40].

The advent of edge computing as a technological solution has facilitated data processing close to the source, like IoT devices, aiming to reduce latency and maximise bandwidth efficiency. Tian Li et al. explored the complexities of dynamic edge computation offloading, employing DRL techniques to refine the decision-making process [38]. Zhou et al. introduced a certificateless multi-copy integrity auditing method, underscoring the importance of data integrity in dynamic settings [41]. Marksteiner et al. highlighted significant privacy and security challenges within the healthcare sector [35].

Collectively, these studies underscore the imperative for robust cybersecurity measures to protect sensitive health data in the digital health sphere. Despite the advancements in digital twin technologies and edge computing in healthcare, there remains a significant gap in integrating these technologies with robust cybersecurity measures. Existing studies have primarily focused on either the technological aspects of digital twins or the cybersecurity challenges in isolation, without fully addressing the synergy between these components in healthcare contexts. Our research addresses this gap by uniquely integrating edge computing and advanced cybersecurity within the framework of DTH. This approach not only enhances real-time patient monitoring but also ensures a higher level of data security and integrity, an aspect that has not been sufficiently explored in previous studies. In summary, while existing literature provides valuable insights into the use of digital twins and edge computing in healthcare, our study extends this knowledge by exploring the critical integration of cybersecurity, a crucial yet underexplored component in the DTH paradigm.

3 | APPROACH OF CYBERSECURITY IN DIGITAL TWIN HEALTHCARE

Figure 1 presents a comprehensive framework designed to fortify the cybersecurity infrastructure of a DTH system. At the core lies the safeguarding of patient data, around which the entire model is constructed. This is epitomised by the Patient Data Security segment, which encapsulates pivotal cybersecurity measures such as hybrid data encryption and certificate-based authentication. These measures are essential for ensuring the confidentiality and integrity of patient information. Furthermore, the Merkle Tree integrity check and secure communication components provide a robust foundation for verifying the consistency and security of the data, while cyber threat prediction focuses on proactive identification of potential security breaches. Collectively, these elements form the bulwark against cyber threats, pivotal in maintaining the trust and safety required in healthcare environments.

The framework also delves into the organisation requirements specification, dissecting both the functional and non-functional requirements necessary for a thorough investigation into the system's necessities. Subsequently, cost model analysis evaluates the financial aspects, crucial for sustainable implementation.

In the assessment of cloud supporting step, the system's elasticity, communication, processing, and infrastructure control are scrutinised, along with availability and security protocols. This assessment is vital for ensuring compliance with regulatory requirements and upholding privacy and data confidentiality.

Modifications in organisational routines are addressed in the subsequent module, reflecting the changes brought about by the integration of the DTH system. It encompasses alterations in accounting practices, customer relationships, public image, flexibility, business continuity, compliance, benefits, and the identification of potential risks and challenges.

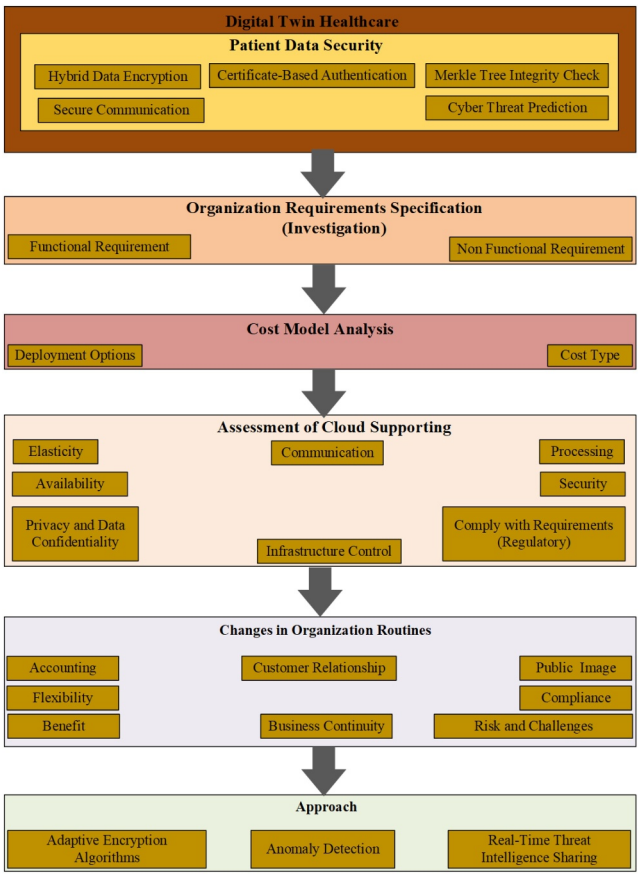

FIGURE 1 Integrated framework for digital twin healthcare cybersecurity.

Lastly, the approach step posits innovative approaches such as anomaly detection, enhancing the security framework. The integration of real-time threat intelligence sharing, and adaptive encryption algorithms, for privacy preservation further contribute to the cutting-edge nature of the system.

In summary, the illustrated framework provides a strategic approach to securing DTH systems, ensuring comprehensive protection and resilience against cyber threats, while fostering advancements in healthcare technology.

4 | PROPOSED METHODOLOGY

The methodology included the merging of edge computing with the DT model to improve the security of data and minimise latency in the patient monitoring systems. The service uses a multi-layered security model that includes hybrid encryption, certificate-based authentication, Merkle Tree verification, and numerous secure communication protocols. The approach protects sensitive patient data and allows processing patient information in real-time, as needed. In addition, the digital twins within the system are used to detect anomalies in real-time by continually comparing feedback data from the DT model to the physical twin. This comparison enables near-immediate detection and remediation of any discrepancies.

Also, it alleviates the problem of missing data with predictive models to estimate and complete the gaps, ensuring uninterrupted and accurate monitoring of the patient.

The approach for enhancing data security and integrity within DTH systems using edge computing is proposed. This methodology revolves around the implementation of encryption, authentication, and integrity checks. For DTH applications, the ESP32-AZURE IoT Kit has been employed, combining the features of the ESP32 microcontroller with the functionalities offered by Azure's IoT services, as illustrated in Figure 2. This device is designed to capture data reflecting the patient's physiological state and environmental conditions. Prior to data transmission, the cloud server authenticates the device, followed by verifying the integrity of the encrypted data upon its transfer. Successful validation prompts an acknowledgement to the ESP32 device, as depicted in Figure 3.

The ESP32 has been strategically selected due to its high performance-cost ratio, low power consumption, and embedded Wi-Fi and Bluetooth capabilities, making it ideally suited for IoT healthcare scenarios where both efficiency and connectivity are paramount. This choice ensures effective patient monitoring and data collection in DTH systems, enabled by its dual-core processing ability and numerous GPIO pins, allowing for adaptable sensor fusion and real-time data processing.

Azure IoT Hub has been selected for this project due to its reliability as a cloud-based platform, offering secure, scalable, and efficient communication for IoT devices and applications. It abstracts the communication mechanisms between devices and the cloud, supporting various methods such as device telemetry, file upload, and request-reply patterns. Azure IoT Hub's capability to manage large volumes of data in real-time

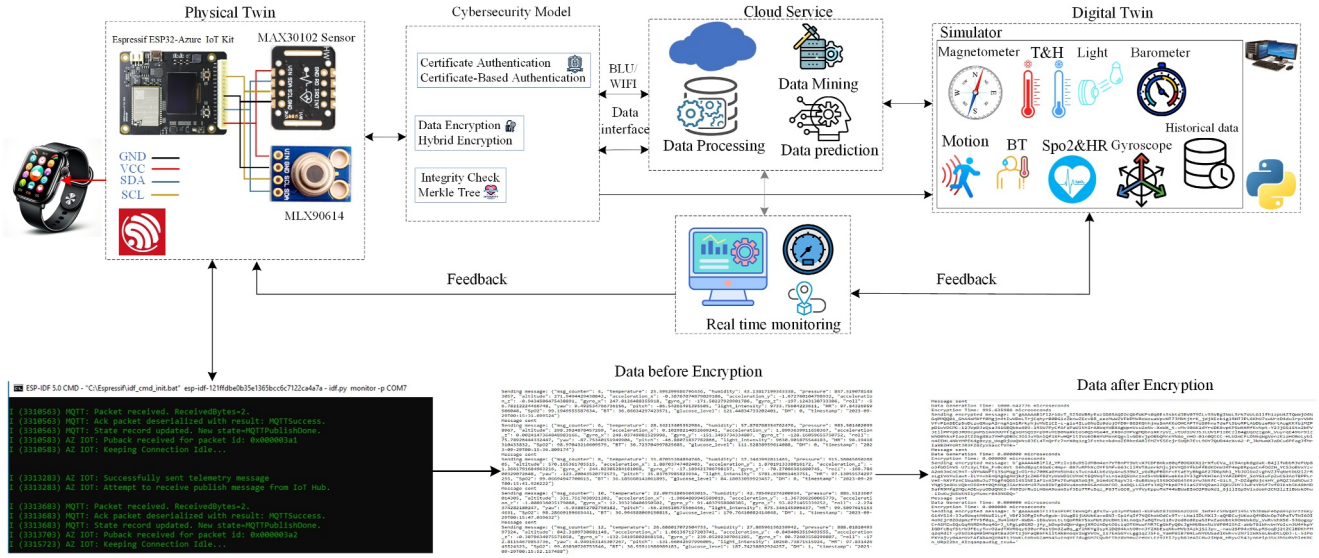

FIGURE 2 Scenario illustrating the digital twin healthcare system with cybersecurity measures.

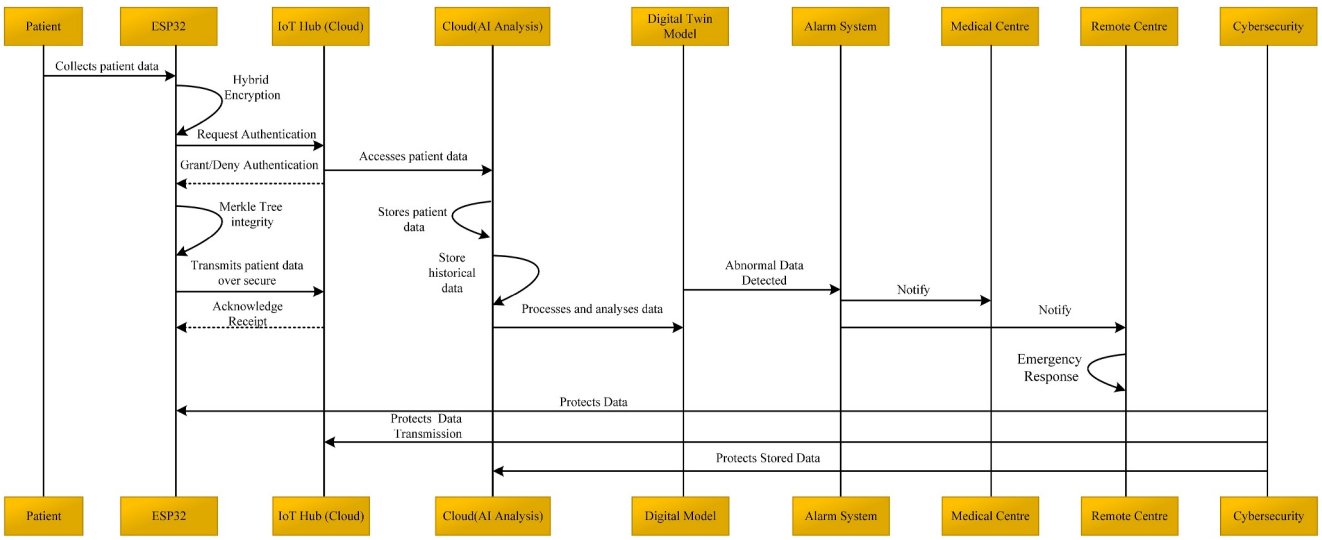

FIGURE 3 Sequence of data flow and interactions in the DTH monitoring system with cybersecurity.

or streaming mode, along with its comprehensive security and remote management features, renders it an ideal platform for managing DTH systems.

4.1 | Data encryption algorithm: Hybrid encryption technique

To bolster security, a novel hybrid encryption technique has been developed, combining the strengths of symmetric and asymmetric encryption systems. This approach leverages the resilience of public-key encryption with the efficiency of symmetric encryption, enhancing overall security. The algorithmic procedure is outlined in Algorithm 1.

Algorithm 1 Hybrid Data Encryption

```
Input: Data D, Public Key PK, Symmetric Key SK
Output: Encrypted Data ED, Encrypted Symmetric Key ESK
function ENCRYPTDATA(A, D, PK, SK)
    ED ← SymmetricEncrypt (D, SK)
    ESK ← AsymmetricEncrypt (SK, PK)
return ED, ESK
end function
```

This hybrid encryption technique was chosen due to its various advantages. RSA, while secure, demands substantial processing power, whereas AES-128 is efficient but poses challenges in key distribution.

4.1.1 | Certificate-based authentication and authorisation

Algorithm 2 details the certificate-based authentication method, crucial for establishing trust in the heterogeneous IoT landscape. In the healthcare sector, where IoT devices are susceptible to impersonation, pre-access authenticity verification is imperative.

Algorithm 2 Certificate-Based Authentication

```
Input: Device Certificate DC, Certificate Authority CA
Output: Authentication Status (Success/Failure)
Function AUTHENTICATEDEVICE(DC, CA):
if VALIDATECERTIFICATE(DC, CA) then
    Status ← Success
else
    Status ← Failure
end if
return Status
```

The secure launch and flash encryption of the ESP32 device, coupled with Azure IoT Hub's certificate-based verification, significantly enhance device security by validating software and protecting memory, thereby reducing unauthorized access.

4.1.2 | Comparison of authentication methods

While certificate-based authentication and authorisation is well-established and widely used, it has notable efficiency implications compared to certificateless and implicit-certificate approaches.

1. Certificate-Based Authentication: This approach typically has a high computational cost and latency due to the need to validate certificates with a CA. In our research, the average time for certificate validation was found to be approximately 0.055 s per request, and the computational cost for handling certificates can add up to 0.8% of the system's overhead. These observations can be represented by the following equations:

   Latency (L_{cert}):

$$L_{cert} = N \times t_{CA}, \tag{1}$$

   where N is the number of certificate requests, and t_{CA} is the average time per certificate validation (0.055 s in this case).

   Overhead (O_{cert}):

$$O_{cert} = N \times \frac{P_{cert}}{P_{total}}, \tag{2}$$

   where P_{cert} is the processing power used for certificate handling, and P_{total} is the total system processing power, with the certificate handling overhead observed to be 0.8%.

   The secure launch and flash encryption of the ESP32 device, coupled with Azure IoT Hub's certificate-based verification, significantly enhance device security by validating software and protecting memory, thereby reducing unauthorized access. However, maintaining the CA infrastructure requires administrative overhead and processing time during verification.

2. Certificateless-Based Approach: Certificateless cryptography removes the need for certificates by partially delegating key generation to a Key Generation Centre (KGC) and users computing the rest. Studies such as [42] show an approximate reduction of 60.24% in latency compared to certificate-based systems, which can be expressed as:

   Latency (L_{cless}):

$$L_{cless} = N \times \left(1 - r_{latency}\right) \times t_{cert}, \tag{3}$$

where $r_{latency}$ is the latency reduction percentage (60.24% from [42]), and t_{cert} is the average latency of certificate-based systems.

Overhead (O_{cless}):

$$O_{cless} = N \times (1 - r_{overhead}) \times \frac{P_{cert}}{P_{total}}, \quad (4)$$

where $r_{overhead}$ is the overhead reduction percentage (60% from [42]).

However, this model relies on a trusted KGC, which, if compromised, can affect the entire system's security.

3. Implicit-Certificate-Based Approach: Implicit certificates streamline the verification process by linking public keys directly to identities, reducing the validation time to approximately 1.329 ms on average, according to [43], leading to:

Latency ($L_{implicit}$):

$$L_{implicit} = N \times \left(1 - r_{latency}\right) \times t_{cert}, \quad (5)$$

where $r_{latency}$ is the latency reduction percentage (30% from [43]).

Overhead ($O_{implicit}$):

$$O_{implicit} = N \times (1 - r_{overhead}) \times \frac{P_{cert}}{P_{total}}, \quad (6)$$

where $r_{overhead}$ is the overhead reduction percentage (40% from [43]).

However, implicit certificates require robust key management strategies and may not be compatible with all existing systems.

The hybrid encryption technique proposed in our research benefits from certificate-based authentication due to its established trust models and compatibility with existing infrastructure, particularly in healthcare. While certificateless and implicit-certificate approaches offer efficiency gains in certain areas, the stability, maturity, and proven security of certificate-based methods make them the optimal choice for securing sensitive data in heterogeneous IoT environments.

4.2 | Healthcare integrity checks with Merkle Trees and digital twins

To ensure data integrity throughout its lifecycle, the research incorporates a Merkle Tree-based integrity validation technique. This cryptographic approach facilitates efficient verification of extensive datasets, as described in Algorithm 3.

Algorithm 3 Merkle Tree Integrity Check

```
Input: Data Blocks DB[1…n], Merkle Root MR
Output: Integrity Status (Valid/Invalid)
function CHECKINTEGRITY(DB, MR)
    Tree ← GENERATEMERKLETREE(DB)
    if Tree.Root == MR then
        Status ← Valid
    else
        Status ← Invalid
    end if
    return Status
end function
```

Our approach is fully integrated with DTH systems, significantly improving them in several critical areas. Through edge computing, data processing and analysis occur right at the point of capture, reducing latency and boosting the DTH system's responsiveness, which is vital for making timely decisions in patient care.

Additionally, our strong cybersecurity systems protect and maintain the confidentiality, integrity, and availability of data within the DTH system. The combination of hybrid encryption and certificate-based authentication creates a highly secure environment for extremely sensitive patient information, protecting it from potential cyber threats. The implementation of Merkle Tree integrity checks also ensures that patient data, once processed and stored, remains unchanged and reliable for future use.

The integration of these advanced technologies significantly enhances the effectiveness of DTH systems. This leads to more precise and secure patient health monitoring, paving the way for improved predictive analytics and personalised healthcare solutions. Certainly, such an intelligent integration of edge computing and cybersecurity into general-purpose DTH systems is 'one' new development that has been taking place in the domain of digital healthcare.

4.3 | Prototype and testing

Development of a prototype was also one such validation exercise which helped us ensure the efficiency of our proposed approach. We adopted an ESP32 AZURE Kit and built a prototype as aligned with the system architecture. This harnessed its role to assemble and process patient data in time to simulate the operational environment of a DTH system. To determine the following functionalities, this prototype was tested as follows:

1. Functionality Testing: This involved ensuring that all the components of the system worked well and functioning related to capturing, encrypting and transmitting of data were checked.
2. Performance Testing: We tested system response times, as well as data processing speeds, which is very crucial for monitoring applications in real-time.
3. Security Testing: In this step, we carried out exhaustive tests that measure the efficacy of our cybersecurity protocols. Such measures include conducting penetration testing and vulnerability scanning.

4. Data Integrity Testing: We have tested data integrity in a case where we test the system with hard scenarios or there is an opportunity of data breaching to security.

These insights through these tests helped us refine our system and make it ready for deployment in the healthcare settings.

4.4 | Integrated cyber threat prediction and channel security with DT

The handshake process ensures the efficiency and safety of data transmission by establishing the channels of communication. Algorithm 4 indicates the technique by which the guarantee of data transmission is provided. With the rising focus of cyber threats on healthcare systems, it's crucial to prioritise the use of detection methods. The integration of DT proves to be an asset in this regard, as it enables early analysis of data patterns and system interactions. This approach not only facilitates the early detection of potential cyber hazards but also helps in pinpointing irregularities and patterns indicative of cybersecurity attacks, enabling timely intervention. Moreover, the real-time data analysis capability inherent in DT allows for the prediction and prevention of security breaches. This ensures the safety and preservation of healthcare data, as detailed in Algorithm 5.

Algorithm 4 Secure Communication

```
Input: Data D, Secure Channel SC
Output: Transmission Status (Sent/Not Sent)
function TRANSMITDATA(D, SC)
    HANDSHAKE(SC)
    if SC.Status == Established then
        SEND(D, SC)
        Status ← Sent
    else
        Status ← Not Sent
    end if
    return Status
end function
```

Algorithm 5 Cyber Threat Prediction using DT

```
Input: Real-time data(RTD) from IoT devices, Historical data patterns(HDP)
Output: Alert (if any)
function PREDICTTHREAT(RTD, HDP)
    twin_data ← mirror_data(RTD)
    anomaly ← compare(twin_data, HDP)
    if anomaly detected then
        generate Alert
    end if
end function
```

5 | SECURITY ANALYSIS

In Figure 4, the cybersecurity process flow for DTH systems is illustrated. Initially, data is encrypted using a hybrid encryption technique that combines symmetric and asymmetric methods. This ensures that data is protected from unauthorized access.

5.1 | Encryption efficiency and data integrity

The proposed hybrid encryption technique effectively combines symmetric and asymmetric encryption, resulting in a 27.18% improvement in encryption time, crucial for real-time healthcare applications.

1. Merkle Tree-Based Integrity Validation:
   - To ensure data integrity, the system employs a Merkle Tree-based validation technique. This structure organizes data into a binary tree where each leaf node contains the cryptographic hash of a data block, and each non-leaf node contains the hash of its child nodes.
   - The root hash, known as the Merkle Root, represents the entire dataset's integrity. If even a single data block is altered, its hash changes, causing a mismatch in the hashes up to the root, thus revealing any tampering.
   - This method efficiently verifies data authenticity throughout its lifecycle. The binary tree structure allows for rapid integrity verification, as only the path from the altered block to the root needs recalculating.
   - Table 3 in section 8.1 demonstrates the success of this technique, with a generated Merkle root ('4cf4e-f91a69077c0a1e5baf') confirming that the data remains

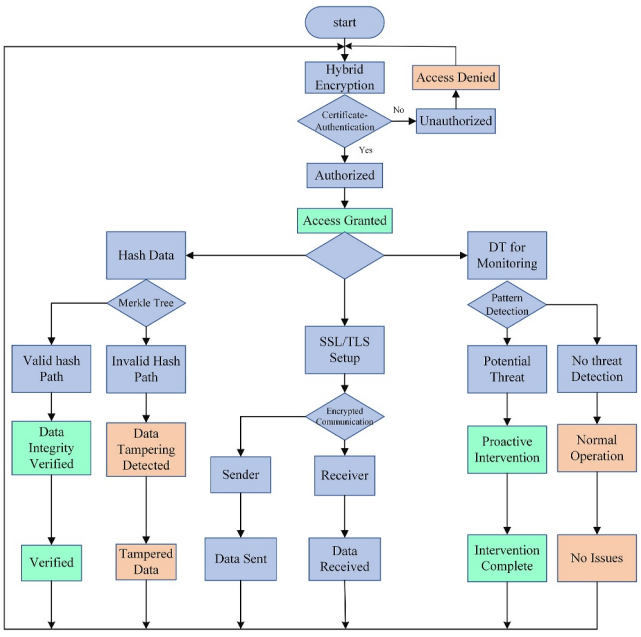

FIGURE 4 Cybersecurity process flowchart for DTH system.

consistent and unchanged. Strong proof of data authenticity and integrity is offered by this result, making validation based on Merkle Tree ideal for applications where high data integrity is required, such as environments in healthcare where the accuracy of patient information is paramount.

2. Authentication and Authorisation: The paper discusses certificate-based authentication in detail, highlighting its computational cost and latency implications. Certificateless and implicit-certificate approaches are compared to show their efficiency benefits and security trade-offs.
3. Secure Communication: The paper emphasises establishing secure SSL/TLS communication channels to ensure the safe transmission of patient data across devices and networks.
4. Threat Detection: By using DT to monitor patterns, the system can predict potential cybersecurity threats in real-time. This allows for proactive intervention before damage occurs.

5.2 | Cyberthreats addressed

1. Data Breaches:The system leverages hybrid encryption and certificate-based authentication to prevent unauthorized access to sensitive healthcare data. Unauthorized access to healthcare data can result in data theft, privacy violations, and even fraudulent activities. The system uses hybrid encryption, combining the strengths of symmetric and asymmetric encryption, to protect data confidentiality. Certificate-based authentication ensures that only authorised devices and users can access sensitive healthcare data. For example, in a hypothetical scenario, a malicious actor attempting to access patient records without proper authorisation would be denied access due to robust encryption and authentication measures.
2. Man-in-the-Middle Attacks: SSL/TLS is employed to transmit and encrypt data, it is unimaginable to analyse the transmitted data. But one should assume that attackers would monitor the communication between devices in order to view or change transmitted data. When SSL/TLS data transmission channels are established, transmitted materials are encrypted and cannot be intercepted. For example, let's imagine that a hacker tries to intercept data transmitted from a healthcare device to a server. In this case, SSL/TLS data encryption will ensure the impossibility of unauthorised access. The data transmitted from the device to the server will be impossible to interpret without the assigned encryption and decryption keys.
3. Data Integrity Attacks: Merkle Tree validation technique is used to validate the stored data by verifying that it has not been tampered with in any way. Stored secure information could be tampered with by the attackers hence corrupting or falsifying it. Merkle Tree validation subscribes to the concept of data integrity by providing a means through which tampering can be detected quickly and efficiently. For example, an attacker may want to change a patient's medical records. For instance, the Merkle Tree validation would quickly detect unauthorised changes in the record as seen in the hash value mismatch.
4. Device Impersonation: Certificate-based authentication ensures that only authorised devices access the system. There are cases where attackers may try to intrude on the system and be a legitimate device. In such malpractices, devices can be compromised, and authentication compromised devices enter the system. The certificate ensures that only known devices can connect. As such, if someone tries to mimic a healthcare device, the system will not accept the device because the certificate is not recognised.

5.3 | Compliance with regulatory frameworks

To achieve HIPAA and GDPR-compliant data security, it was necessary to adopt a hybrid encryption strategy of combined symmetric and asymmetric approaches. Encrypting data during transmission ensured that patient information could not be accessed by unauthorised individuals while travelling, which DTHHIPAA and GDPR standards interpret as sensitive data in transit. Utilising study certificate-based identification and secure SSL/TLS-encrypted communication devices guarantees that only designated personnel have access to the system, which is necessary for HIPAA-mandated access controls and protective GDPR measures. These encryption techniques protect patient data being transmitted from the physical model to the digital platform in DTH.

Merkle Tree-based validation maintains data integrity, ensuring compliance with HIPAA's audit control requirements. Regular system audits and monitoring are conducted to detect potential breaches, adhering to GDPR's requirement for proactive data breach detection. Personal data has been anonymity where possible to comply with GDPR's data minimisation principle, and data collection is minimised to only what is necessary. Data storage and retention policies have been structured to meet GDPR's requirements, ensuring that sensitive data is retained only as long as necessary. Encryption protocols have been used to protect data at rest, addressing HIPAA's storage security guidelines. In DTH systems, these measures ensure that patient data remains secure and compliant with regulations throughout the lifecycle of the digital twin model, from data collection to storage. By implementing these measures, compliance with the highest standards of data security and privacy has been ensured in healthcare settings.

6 | PERFORMANCE METRICS

To evaluate the proposed system's effectiveness, several metrics were employed.

6.1 | System performance evaluation

To assess the effectiveness of the proposed system, several metrics were employed. Data collection was conducted by compiling a dataset through 1,000 iterations of encryption simulations to evaluate the performance of the encryption method. This dataset consists of simulated telemetry data collected using a sensor suite installed on an ESP32 device.

Encryption time visualisation was achieved by plotting the recorded times for each encryption iteration in a histogram to illustrate the uniformity and variability of the encryption durations, as shown in Figure 5. The duration of the encryption process, $T_{\text{encryption}}$, was calculated by measuring the time difference between the start and end times:

$$T_{\text{encryption}} = t_{\text{end}} - t_{\text{start}}, \tag{7}$$

where t_{start} and t_{end} denoting the start and end times of the encryption, respectively.

System overhead visualisation was performed by evaluating the system overhead based on the time taken for data generation and the encryption process duration. The overhead across various rounds was visualised using a stacked bar chart, as illustrated in Figure 5. The system overhead, Ω, was calculated as the difference in resource consumption with and without the security measures:

$$\Omega = R_s - R_{ns}, \tag{8}$$

where in R_s, and R_{ns} represent the resource consumption with and without the implementation of security measures, respectively.

6.2 | Cyber threat prediction efficiency

To test the system's proficiency in preemptively identifying potential cyber threats using DT, simulated cyber-attack patterns were introduced into the data stream. The DT's effectiveness was then gauged by comparing the number of identified threats against the number of simulated attacks.

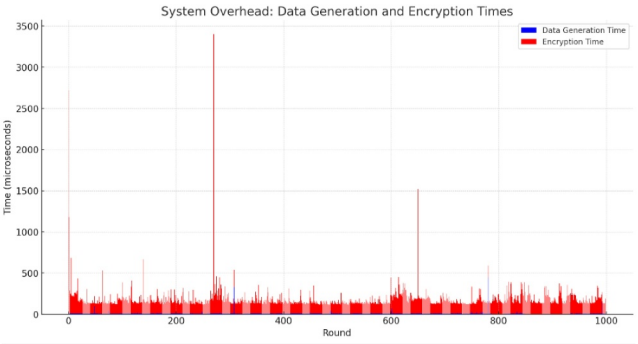

FIGURE 5 Data generation and encryption use 1000 simulation rounds.

$$\xi \equiv \frac{\theta_d}{\alpha_s} \times 100\%, \tag{9}$$

The symbol ξ represents the efficiency of detection, which is calculated by dividing the number of identified threats θ_d by the number of simulated attacks α_s.

This approach emphasises how well the system can accurately identify cyber threats, thus demonstrating the security improvements brought about by DT technology in healthcare IoT applications. Figure 6 indicates that the IoT device properly creates encrypted telemetry data, where each operation is timestamped fittingly to have a way of measuring the processing time. The encryption process prompts a minimal overhead, therefore proving it to be applicable in real-time IoT data security intentions. A comprehensive series of simulations evaluated the performance of the encryption algorithm, which forms the cornerstone of the DTH system's security. These simulations aimed to ascertain the duration required to encrypt standardised telemetry data packets. The researchers encrypted these packets, which represented sensor outputs from an ESP32 module, using a method called symmetric and asymmetric encryption, known for its strong security and high speed. Using a high-resolution timer, we meticulously documented the latency of encryption throughout a sequence of 1000 iterations. This documentation captures the milliseconds that elapsed from the initiation to the culmination of the encryption process. Subsequent to the data collection phase, an outlier detection method was employed, utilising the interquartile range to filter out aberrant values that could skew the overall analysis. This filtration ensures a focus on the most consistent and representative data points. The resultant histogram, devoid of outliers, presents a skewed distribution with a pronounced peak, indicating a concentration of encryption operations within a narrowly defined time frame. This aggregation suggests a high level of performance consistency, a desirable attribute in real-time systems where predictability and

FIGURE 6 IoT telemetry data encryption process.

reliability are paramount. Notably, the range of encryption times is confined within a tight band, underscoring the algorithm's suitability for real-time applications within the healthcare domain, where delays can be detrimental to system responsiveness and patient outcomes. The presented Figure 7 adheres to high academic standards of clarity and quality. Axes are meticulously labelled, with the x-axis delineating the encryption time in milliseconds and the y-axis representing the frequency of occurrences. The choice of bin size in the histogram is the result of a deliberate balance act to provide sufficient granularity while avoiding overfitting to the random variations inherent in the data. This careful construction of the visualisation ensures that the figure serves as an accurate and insightful representation of the encryption time distribution, facilitating immediate comprehension and further scholarly discussion.

6.3 | Scalability of the proposed system

The importance of scalability in DTH IoT systems cannot be understated, given the increasing number of connected devices and the exponential growth in data generated. Potential bottlenecks in data processing, storage, and network bandwidth have been acknowledged in the proposed system due to the integration of a large number of IoT devices.

To address these challenges, a combination of cloud computing and edge computing approaches has been incorporated into the architecture to ensure the efficient distribution of the workload. Load balancing, data partitioning, and distributed databases have been used to guarantee robust data management even as the number of devices scales up. A modular design has been used to facilitate horizontal scalability, enabling the system to grow by adding additional nodes without significant modifications. To ensure seamless deployment in diverse healthcare environments, integration with existing IT infrastructure has been planned through interoperability standards and protocols. Comprehensive testing strategies have been implemented to validate performance and scalability across various settings.

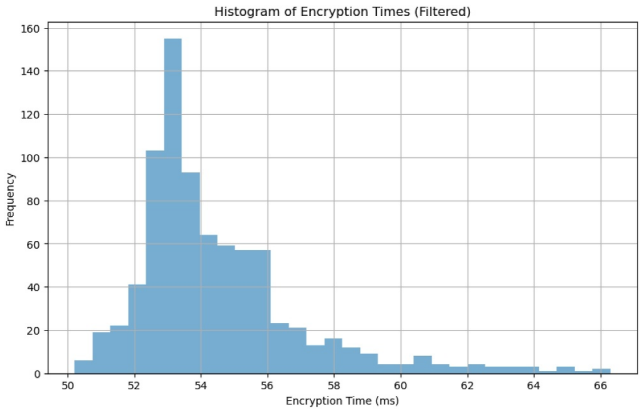

FIGURE 7 Distribution of encryption latency.

7 | EVALUATION OF SYSTEM PERFORMANCE

7.1 | Correlation analysis

A correlation study was undertaken to examine the performance of the IoT system, focussing specifically on the times for data generation and encryption. The Pearson correlation coefficient (r) was employed to identify trends between these variables, calculated as follows:

$$r = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2 \sum (y_i - \bar{y})^2}} \quad (10)$$

Here, x_i and y_i represent the individual sample points for the two variables, while $\bar{x}$ and $\bar{y}$ denote their respective sample means. The correlation between the variables data_generation_time and encryption_time was ascertained using the collected dataset. The computed Pearson correlation coefficient of $r = 0.3121$ suggests a moderate positive relationship between the time taken for data generation and encryption. The correlation between data production and encryption durations is depicted in Figure 7. The scatter plot displays data concentrations in the lower left and upper right quadrants, indicating that brief data production times correspond to minimal encryption, whereas extended production times correspond to increased encryption.

7.2 | Encryption time analysis

Upon meticulous examination of the encryption times procured from a series of one thousand simulations, it is observed that the mean encryption duration is approximately 54.78 ms. This suggests that, on average, the time required to securely encrypt a unit of data is within an acceptable milliseconds range. It is noteworthy that the median encryption time, a robust measure of central tendency, is 54.20 ms, reinforcing the symmetry in the distribution of the encryption times and suggesting a negligible skewness within the data.

Furthermore, the mode of the encryption times is identified at approximately 53.30 ms. While the mode may often be relegated to lesser significance in the context of continuous data, its proximity to the mean and median in this analysis underpins the consistency of the encryption process. Deviation calculation evaluates the spread out of data offers around 2.11 ms value. The smallness from the norm illustrates the encryption process is very predictable and reliable. This is relevant in instances where accuracy and uniformity in encryption are of great essence. The 95th percentile time for encryption, which stood at 58.80 ms, further indicates that only a paltry five percent of the encryption operations

surpassed this boundary. This percentile helps to establish limits for time encryption and build a realistic on Service Level Agreements matching real system performance. To sum up, the process of encryption exhibits a sense of efficiency and consistency due to standardized extent of data alignment related to mean, median, mode values with low range of standard deviation. The results from this analysis strongly support the effectiveness of this encryption mechanism for its intended purpose by meeting important benchmarks for fast and reliable data encryption.

7.3 | Anomaly detection

Consistency in data is paramount in IoT systems. To identify anomalies within the encryption latency dataset, the Z-score method was utilised. According to the empirical rule, data points with a Z-score exceeding three were classified as anomalies. The algorithmic procedure is outlined in Algorithm 6. Also, Figure 8 demonstrates critical concerns for IoT system reliability using markers.

Algorithm 6 Z-score Anomaly Detection

```
for each data point x in dataset do
    Calculate z = (x - mean) / standard_deviation
    if |z| > threshold then
        Mark x as anomaly
    end if
end for
```

7.4 | Performance regression analysis

Performance enhancements were quantified by examining the duration of the encryption process. Comparatively, the existing system registered an average encryption time of 78.66 ms with a variance of 538.94 ms, while the current system achieved an average of 58.00 ms and a standard deviation of 233.73 ms, as evidenced in Figure 9. A more elaborate discussion pertinent to the performance metrics and the validation of the idea is covered in section 8.

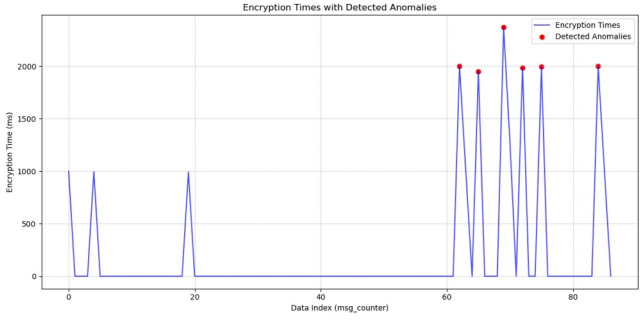

FIGURE 8 Detection of anomalies in encryption times.

7.5 | Network metrics analysis in digital twin healthcare systems

The system performance metrics measured included latency, which is primarily affected by data volume and the distance from the cloud platform. Figure 10 illustrates that at the highest data size, the latency for encrypted data is greater than for unencrypted data. The results show reduced latency compared with prior studies, although previous studies often reported latency in terms of percentages. Research [44] indicated that the highest response time with a large data volume was around 8 s for 50 MB. This was compared with [45], which relied on jointly optimised offloading policies and computing resources to achieve fairness-aware response time reduction in a DT-supported edge computing network, reducing latency by 33%–66% and achieving fairness up to 99.6% according to Jain's index. In [46], it was shown that increased data size leads to higher offloading latency, achieving approximately 36.63%, with latency around 0.84 ms for 1000 KB. In our study, throughput was 6.37 messages/sec for unencrypted data and 4.64 messages/sec for encrypted data, indicating a 27.18% decrease in throughput due to encryption overhead. Packet loss was also measured, with 0.5% observed for unencrypted data and 1% for encrypted data at 4 KB. This percentage is considered favourable in comparison to prior research, where encrypted data of 4 KB size reached a packet loss of 2% as noted in [42]. The error rate was 0%, ensuring communication accuracy and reliability. Also, communication efficiency was appraised by considering bandwidth utilisation and latency. The bandwidth required for the encrypted data transmission was measured at 36.6 kbps, compared to 24.6 kbps for the initial unencrypted data. This work was based on previous research and focused on designing a digital twin environment with cybersecurity rules in mind.

7.6 | Energy and storage efficiency

Energy efficiency was gauged by analysing power consumption during various operational phases. The power consumption of

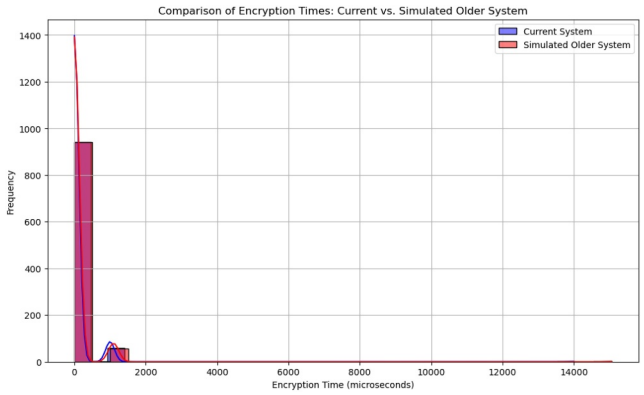

FIGURE 9 Encryption time distribution for current and simulated older systems.

FIGURE 10 Latency comparison with and without encryption across data sizes.

the ESP32-AZURE IoT Kit was observed across different phases, including idle, data collection, encryption, and Wi-Fi transmission, and it ranged from 0.4125 to 0.825WW. The power usage of the MAX30102 and MLX90614 sensors was also scrutinised, revealing estimated consumptions of 0.00198 and 0.00495W, respectively.

To evaluate the storage impact of the proposed system, the storage efficiency ratio was determined. This ratio,η, was calculated as the relationship between the original data size, δ_o, and and the encrypted data size, ϵ_e:

$$\eta \equiv \frac{\delta_o}{\epsilon_e} \tag{11}$$

The resultant Storage Efficiency Ratio, as calculated from the assessed datasets, was approximately 0.673.

7.7 | Comparative analysis of digital twin technologies

In this research, we conduct a nuanced comparative analysis of the recent advancements in DT technologies, as represented in Table 1. Our approach transcends the conventional bounds by not only focussing on specific DT sub-domains, such as UAV energy efficiency, but also exploring a broader spectrum of DT applications.

The table delineates a variety of studies, each examining distinct aspects of DT and data security. For instance, the works of [36,37] delve into 6G DT networks with federated learning and IoV with edge offloading, respectively. For this reason, such studies help in understanding the ways that DT technologies can be used in network paradigms. On the other hand, our effort introduces a testing protocol comprised of the variety of simulations, real-world play and evaluations, and rigorous stress tests. The latter approach ensures reliability and relevance to the findings. It also gives us a comprehensive outlook of the performance of the system under varied conditions. The research underscores that AES 128 with RSA/ECC for encryption protects the system from intruders as pertains to security breaches. Asides that, use of the TLS Handshake Mechanism in a data transfer process proves how the use of our system updated and viable to keep the general information integrity.

To further clarify on the same, a table showing the performance metrics such as encryption time and storage efficiency across other systems reviewed shall be appended. An observable enhancement in encryption time efficiency, by approximately 27.18%, is evidenced when contrasted with alternative approaches. Similarly, with a storage efficiency ratio of 0.673, our system's proficiency in resource management whilst upholding data integrity is highlighted. In essence, the comparative analysis presented in Table 1 accentuates the uniqueness of our system within the DT technology spectrum. It heralds the sophisticated methodologies employed to safeguard data security and integrity, establishing a precedent for ensuing research in the domain.

8 | PROOF OF CONCEPT

8.1 | Verification of security protocols

The configuration of the system, as depicted in Table 2, was employed for the validation of the proposed scheme. Asdelineated in [49], IoT devices are classified into four distinct categories: Application, Management, Network, and Perception layers. This classification is based on their respective processing capabilities and power consumption levels. For the purpose of simulating a robust machine capable of verifying transaction data in a DTH system, the MSI (GF63 Thin 11SC), a device from the Laptop class, was utilised. Transactions in real time were facilitated through the use of Azure cloud. For convenient access to data, an IoT Hub, serving as a remote node, was employed, utilising an application programming interface. The development of the low-power sensor node involved the ESP32S2 module [50], which falls under Class II of IoT devices. This module operates on the ESP-IDF framework, which is built upon FreeRTOS (Real-time Operating System). Internet of Things sensor nodes, typically reliant on battery power, are often deployed in locations where access is challenging. Although the ESP32-WROVER-B version of the board, powered by USB, was utilised during the prototyping phase, transitioning to a battery-powered setup or attaching a battery is straightforward [50, 51]. The primary function of the designed sensor node was to monitor various functions within a building.

Given the article's focus on data storage protection for IoT devices, an array of built-in sensors (InvenSense MPU6050 motion sensor, NXP MAG3110 magnetometer, FBM320 barometer, STMicro HTS221 humidity & temperature sensor, and ROHM BH1750FVI light sensor) inside the ESP32-WROVER-B was employed to enhance the environmental representation of DTH in real time. Additionally, external sensors like MAX30102 and MLX90614 were connected to the input port of the ESP32-WROVER-B. To facilitate real-time data monitoring, the ESP32-WROVER-B system's clock was

TABLE 1 Comparing recent data security and integrity verification methods across various systems.

Criteria	[35]2022	[36]2023	[37]2022	[38]2022	[39]2012	[47]2015	[48]2022	[41]2022	Our work
System analysed	Platform analysis	6G DT networks w/[a] FL	IoV w/Edge offloading	DT w/ Blockchain	Multicloud w/ PDP[b] verification	Multicloud w/ ID-DPDP[c]	Multicloud w/ID-PMDP[d]	Public cloud w/Multi-copy data	Comprehensive tests (Sim.[e], RW[f], Stress[g])
CDT	-	-	DT ECC-based PKI	Homomorphic Resp. w/Hash index	Bilinear pairings	ID-based cryptography	ID-based Auth.	CL-PKC	Hybrid (AES-128 & RSA/ECC)
Performance (encryption time)	Data securing efficiency	-	-	1024 bits: 14,698 ms	-	Discussed in Experiments	Discussed in Experiments	-	27.18% improvement
Storage efficiency	Storage resource management	-	-	-	Minimal storage overhead	Homomorphic Props: Minimal overhead	High efficiency (reduced overhead)	Dynamic Ops efficiency	0.673 (ratio)
Objective	Demonstrate CDTs in Auto cybersecurity	Design DT FL for 6G	Optimise IoV offloading with DRL	Design blockchain PDP for DT	Verify multicloud integrity with cooperative PDP	Ensure multicloud integrity with ID-DPDP	Propose CL-MCIAS[h] for cloud integrity	Multicopy dynamic data in public cloud	Enhance patient monitoring security
Framework	CDT	Lightweight DT FL	DRL for computation offloading	Blockchain PDP for DT	Cooperative PDP	ID-based DPDP	ID-based PMDP for multicloud	CL-MCIAS	CDT for enhanced healthcare security

[a]with.
[b]Provable Data Possession.
[c]Identity-Based Distributed PDP.
[d]Identity-Based Provable Multi-Copy Data Possession.
[e]Simulation.
[f]Real-World Testing.
[g]Stress Tests.
[h]Multi-Copy Integrity Auditing Scheme.

synchronised with the Internet time. Sensor data, transmitted to the IoT Hub, was converted into a 4-letter hexadecimal string, as illustrated in Figure 6.

Table 3 provides a comprehensive summary of the implemented security measures and their respective effectiveness, demonstrating their successful integration and functionality within the system's architecture.

The Table 3 categories each security measure under four primary headings: the sequence number (No.), the method employed, the result of implementing the method, and additional comments elucidating the outcome. The table meticulously details various aspects of the security measures, such as the integrity check via a Merkle Tree, the application of hybrid data encryption, the attempt at certificate-based authentication, and the establishment of secure SSL/TLS communication, thus providing a clear overview of the security status within the system.

8.2 | Distributed web application

The visualisation of sensor readings and associated security hashes is presented in Figure 11, demonstrating the practical application of the system in a real-world environment. In Figure 6 depicted, a console log output is captured during an encrypted data transmission simulation from one of the ESP32 IoT devices to a cloud-based IoT hub. The operations of the IoT device starting from data generation to the process of encryption and further to message dissemination are logged sequentially. The log described the encryption overhead related to processing the real-time telemetry data, and from it a time taken of (1995.41 microseconds = 0.498 ms) was recorded for encrypting the second message. The sensor data is represented by the hex notation, while the resulting encrypted payload is expressed as a byte string for conciseness. The simulation showed that it was feasible to integrate encryption into the IoT devices and revealed an insignificant impact on transmission latency for all of the alternative cryptographic cipher algorithms that were simulated.

8.3 | Performance evaluation and comparative analysis

In the event of a deviation in the monitored individual's health status from established norms, the sensor readings will correspondingly alter, prompting the ESP32 to instantaneously transmit an alert. The ESP32 is configured to receive an

TABLE 2 System configuration.

Description	GF63 Thin 11SC	ESP32-Azure IoT Kit
IoT Device class	Laptop	II
Name	GF63 Thin 11SC	Espressif ESP32-Azure IoT Kit
Operating system	Microsoft Windows 10 pro	FreeRTOS
Processing unit type	11th Gen Intel(R) Core(TM) i5-11400H @ 2.70GHz, 2688 MHz, 6 cores, 12 Logical Processors	Xtensa® dual-core 32-bit LX6 microprocessor, up to 240 MHz
RAM	8 GB	520 KB
ROM (KB)	NA	(Embedded: 448 KB ROM)
NVRAM (GB)	475	(Flash: Up to 16MB)
Graphics Card	NVIDIA GeForce GTX 1650 with Max-Q design & Intel(R) UHD Graphics	-
Network Adaptor	Intel(R) Wi-Fi 6 AX201 160MHz	-
Storage	KINGSTON OM8PDP3512B-AI1 (approx. 488 GB capacity)	-

TABLE 3 Proof of concept: Security measures and their efficacy.

No.	Method	Result	Comments
1	Merkle tree integrity check	4cf4ef91a6907 7c0a1e5baf	Successful integrity check with generated Merkle root.
2	Hybrid data encryption	b'\x83\x9a\x1a-\xbe \xd8\xf8\xeb\x81w \xe9\x17\x0f =	Data have been encrypted using a hybrid encryption scheme.
3	Certificate-based authentication	False	Authentication failed; the certificate was not recognised.
4	Secure SSL/TLS communication	<ssl.SSLContext object>	SSL context has been successfully created for secure communication.

interrupt from the sensors when the detected values surpass predefined thresholds. This mechanism is underpinned by the incorporation of a message confirming the accurate receipt of data; in its absence, the ESP32 enters a deep sleep state, conserving resources until the occurrence of a pertinent event. Upon reactivation, the ESP32 authenticates and dispatches all accumulated data. Subsequent to this transmission, the process of data collection recommences. A detailed comparative analysis, as presented in Table 4, elucidates the distinct performance metrics of our system in juxtaposition with extant

Timestamp	Sensor ID	Sensors				Data Hash	Transaction Hash	Verification
2024-01-24 15:49:13	979	Temperature	Humidity	Pressure	Altitude	754ca807816250 7c4765 93eabe6a8f36078724 4047aa8e83734 75cb7 1bf13	d09b9125f3fed1fd2e257 8c7d8287aaab4baec0b9	Pass
		20.53	59.39	820.13	631.68			
		ACCx	ACCy	ACCz	Gyro x			
		0.29	0.62	0.16	-125.31			
		Gyro y	Gyro z	Roll	Yaw			
		82.05	16.53	-47.97	2.71			
		Pitch	Light	HR	SpO2			
		44.37	6452.99	99.01	97.18			
		BT	Glucose Level		DM			
		36.96	152.90		1			
2024-01-24 15:51:13	979	Sensors				54aa7a5fbac2328741e0b4d84 13bb78ef7e25778 7b3600c0d3 ea8753588fb0d3	93405724e5a1367b7378a1a8 b2a681a17a07f8f9	Pass
		Temperature	Humidity	Pressure	Altitude			
		28.27	57.83	824.56	638.21			
		ACCx	ACCy	ACCz	Gyro x			
		0.87	0.83	0.67	29.50			
		Gyro y	Gyro z	Roll	Yaw			
		-179.18	54.08	15.26	20.60			
		Pitch	Light	HR	SpO2			
		-47.01	6720.17	99.47	96.08			
		BT	Glucose Level		DM			
		35.65	159.81		1			
2024-01-24 15:54:13	979	Sensors				f96f8c889a2b5d23a6945f1390 04ca8120e6a8f411aae0172ce 3d54c4fbb9bfe	52c7c778c4417156237e837 3301016068346e6a	Pass
		Temperature	Humidity	Pressure	Altitude			
		23.89	51.02	827.94	630.99			
		ACCx	ACCy	ACCz	Gyro x			
		0.48	0.74	0.21	-180.27			
		Gyro y	Gyro z	Roll	Yaw			
		117.26	-110.31	-24.28	-23.01			
		Pitch	Light	HR	SpO2			
		-54.64	6057.84	99.23	96.58			
		BT	Glucose Level		DM			
		35.81	155.94		1			

FIGURE 11 Environmental sensor readings and security hashes.

systems. This comparative scrutiny highlights the enhanced proficiency of our system, notably in areas of communication efficiency, cybersecurity measures, and the capability for real-time anomaly detection. The table serves to systematically contrast these key aspects, thereby evidencing the advanced capabilities of our proposed system.

8.3.1 | Benchmarking performance

1. In [51] a lightweight protocol was presented using chain hashing to protect data integrity. Compared to this approach, a hybrid encryption technique was implemented in our system, demonstrating a 27.18% improvement in encryption time. This combination of symmetric and asymmetric encryption techniques enabled significant gains in data protection speed, essential for healthcare applications that rely on real-time monitoring.
2. Power Consumption and Cost: The protocol proposed in [51] was evaluated in terms of power consumption, focussing on its effectiveness. Nonetheless, because of their inherent complexity, blockchain-based methods must be expensive for computational work and power use. On the other hand, our system takes advantage of hybrid encryption and Merkle Tree-based validation to provide robust data integrity and security using as low power as possible and to prevent expense.
3. ESP32 Devices: Both protocols were tested using ESP32 devices, allowing for a straightforward comparison in terms of performance. Blockchain protocols developed in [51] were also used for data integrity verification while our system employed hybrid encryption and Merkle Tree validation. In this way, our protocol performed better in terms of data integrity verification as an effective binary tree was presented.

Features	Our system	[33] (2021)	[34] (2021)	[51] (2023)	[32] (2018)
Communication	Wi-Fi	BLE	LoRa WAN	Wi-Fi	Wi-Fi
System analysis	DTH	IoT	IoT	IoT	IoT
Security protection	Yes	Yes	Yes	Yes	No
Data integrity verification	Yes	No	No	Yes	No
Real-time anomaly monitoring	Yes	No	No	Yes	Yes
Network coverage	High	Low	Low	High	High
Current consumption	Low	Low	Low	High	High

TABLE 4 Comparison of key performance metrics.

Furthermore, by benchmarking against [51], the advantages of our system in encryption efficiency, power consumption, cost-effectiveness, and real-time monitoring were better contextualised, providing a nuanced evaluation of its effectiveness.

9 | DISCUSSION

In the present study, a system architecture with extensive evaluation of performance indicators vital for IoT systems was suggested. The system architecture was intended to operate with the highest performance under diverse operational conditions, focussing on computational, communication, and energy and storage efficiency. The operational stages, especially given the energy consumption one, were defined with the areas for improvement being highlighted. Thus, the present system's sustainability and adaptability were increased. Metrics specific for sensors were used to ensure the granularity of the approach for the possibility to tackle each constituent element in the IoT framework.

System scalability posed a significant challenge; although the Azure IoT Hub offered notable scalability, the addition of numerous IoT devices led to data overload and potential latency issues. Effective processing of such voluminous data required scalable computing resources. The processing of large data volumes was expedited using advanced data analytics and machine learning algorithms in the cloud, ensuring robust system performance even under substantial loads.

Moreover, cybersecurity measures had to be robust and scalable to counter emerging threats. Being able to proactively detect and mitigate new cyber threats, the cybersecurity measures had to receive continuous updates and adaptable security framework. The system's security protocols also had to be monitored and audited frequently to mitigate security breaches. The issue of energy consumption was also consistent, especially with wearable IoT devices. Firmware optimisation for the ESP32 and the development of minimally sufficient sensors led to reduced power consumption and, therefore, extended the devices' operation lifespan.

Specific challenges were encountered during the system's implementation that limited overall performance. First, it is the integration of IoT devices utilising different protocols, which caused compatibility issues and required numerous adjustments to the architecture. Second, the problem of real-time data transmission also turned out to be difficult to solve, and we had to develop unique algorithms to control the network latency. Third, the proposed cybersecurity framework faced challenges in optimising encryption times while maintaining data security, which was addressed through iterative testing and refinement. The practical implications of these limitations underscore the need for continuous system optimisation to ensure its applicability in diverse healthcare environments.

Additionally, the integration of the DTH model with the physical model and decision-making system required significant coordination. Time was spent aligning these components to ensure compatibility, enabling the employment of DTH in pattern detection and monitoring. The proposed design comprehensively improves the efficiency of IoT systems in healthcare, which must remain sensitive to performance requirements and flexible enough to keep pace with rapid technological advances and the evolving needs of healthcare professionals and patients.

10 | CONCLUSION

The integration of DT technologies in healthcare is a game changer, fostering a data-centric shift in clinical practices. A new architectural blueprint for DTH has been proposed in our research, highlighting the effective interplay between IoT and cloud computing to reshape how medical services are delivered. The remarkable 27.18% improvement in encryption time, achieved through the implementation of detailed edge computing and advanced cybersecurity measures, underscores the potent capabilities of our system for real-time automated monitoring. The comprehensive sensor data collected enables detailed patient insights and swift data transmission, facilitating proactive and personalised healthcare.

Distinctive features of our architecture include hybrid encryption, certificate-based authentication, and Merkle Tree verification, which collectively enhance data security and integrity. However, some challenges were encountered during the implementation, such as integrating various IoT devices and protocols, ensuring real-time data transmission, and optimising encryption times without compromising security. These limitations necessitate continuous system optimization to ensure practical applicability in diverse healthcare environments.

Future work must address these challenges by exploring advanced DT systems, focussing on sophisticated analytics algorithms and AI integration to boost predictive accuracy in health monitoring and diagnostics. Leveraging high-speed data transmission technologies, such as 6G, will significantly enhance real-time patient monitoring.

Another critical research direction involves reducing energy consumption, especially for wearable IoT devices in healthcare, where battery longevity is essential. Developing energy-efficient sensors and energy-harvesting techniques, such as using body heat or movement, could be beneficial.

Additionally, the challenge and opportunity lie in scaling cloud platforms and integrating an increasing number of IoT devices. A robust cloud infrastructure and specialised data management strategies could facilitate large-scale IoT deployment in healthcare.

In summary, this study significantly advances digital twin healthcare technology and uncovers new research and innovation opportunities. By addressing these challenges, the healthcare IoT ecosystem will be streamlined, paving the way for transformative advancements in patient care and data management.

AUTHOR CONTRIBUTIONS

Ahmed K. Jameil has made substantial contributions to the conceptualisation and design of the work; acquisition, analysis, and interpretation of data; developed the methodology; provided essential resources and software tools; validated the results and methods used; visualised the data; and played a primary role in writing the original draft of the manuscript.

Hamed Al Raweshidy has contributed to the funding acquisition, overseeing and leading the investigation process; managed project administration and coordination; supplied necessary resources; ensured the accuracy and validity of the procedures and results; supervised the project; revised the manuscript critically for important intellectual content.

Both authors agree to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

ACKNOWLEDGEMENTS

Brunel University London.

CONFLICT OF INTEREST STATEMENT

The authors confirm that there is no conflict of interest related to this work.

DATA AVAILABILITY STATEMENT

Data is available on request from the authors.

ORCID

Ahmed K. Jameil https://orcid.org/0000-0002-1864-9807

REFERENCES

1. Al.Quayed, F., Humayun, M., Tahir, S.: Towards a secure technology-driven architecture for smart health insurance systems: an empirical study. Healthcare 11(16), 2257 (2023). https://doi.org/10.3390/healthcare11162257
2. Abujassar, R.S., Yaseen, H., Al.Adwan, A.S.: A highly effective route for real-time traffic using an iot smart algorithm for tele-surgery using 5g networks. J. Sens. Actuator Netw. 10(2), 30 (2021). https://doi.org/10.3390/jsan10020030
3. Wang, C., et al.: Artificial intelligence enhanced sensors - enabling technologies to next-generation healthcare and biomedical platform. Bioelectronic Medicine 9(1), 17 (2023). https://doi.org/10.1186/s42234-023-00118-1
4. Hu, P.F., et al.: Reliable collection of real-time patient physiologic data from less reliable networks: a "monitor of monitors" system (moms). J. Med. Syst. 41(1), 3 (2016). https://doi.org/10.1007/s10916-016-0648-5
5. VillegasMartinez, M., et al.: Tracking early systolic motion for assessing acute response to cardiac resynchronization therapy in real time. Front. Physiol. 13 (2022). https://doi.org/10.3389/fphys.2022.903784
6. Rajawat, A.S., Jain, S., Barhanpurkar, K.: Fusion protocol for improving coverage and connectivity wsns. IET Wirel. Sens. Syst. 11(4), 161–168 (2021). https://doi.org/10.1049/wss2.12018
7. Mazloomi, N., Gholipour, M., Zaretalab, A.: A priority-based congestion avoidance scheme for healthcare wireless sensor networks. IET Wirel. Sens. Syst. 13(1), 9–23 (2022). https://doi.org/10.1049/wss2.12046
8. Lee, J., Dong, M.: Applications of wireless sensor systems to sleep stage estimation for home sleep monitoring. IET Wirel. Sens. Syst. 12(5–6), 123–133 (2022). https://doi.org/10.1049/wss2.12042
9. El.Saddik, A.: Digital Twin for Healthcare: Design, Challenges, and Solutions, 1st ed. Elsevier (2022). https://shop.elsevier.com/books/digital-twin-for-healthcare/saddik/978-0-323-99163-6
10. Liu, Y., et al.: A novel cloud-based framework for the elderly healthcare services using digital twin. IEEE Access 7, 49088–49101 (2019). https://doi.org/10.1109/access.2019.2909828
11. Simulia – dassault systèmes. 'Living heart project'. (2024). Available from: https://www.3ds.com/products-services/simulia/solutions/life-sciences-healthcare/the-living-heart-project/
12. Katsoulakis, E., et al.: Digital twins for health: a scoping review. Npj Digital Medicine 7(1), 77 (2024). https://doi.org/10.1038/s41746-024-01073-0
13. Papara, R., Galatus, R., Buzura, L.: Virtual reality as cost effective tool for distance healthcare. In: 2020 22nd International Conference on Transparent Optical Networks (ICTON), pp. 1–6 (2020)
14. Gräßler, I., et al.: The Digital Twin of Humans: An Interdisciplinary Concept of Digital Working Environments in Industry 4.0'. Springer Nature, Springer (2023)
15. LazimQaddoori, S., Ali, Q.I.: An embedded and intelligent anomaly power consumption detection system based on smart metering. IET Wirel. Sens. Syst. 13(2), 75–90 (2023). https://doi.org/10.1049/wss2.12054
16. NamNguyen, H., et al.: A survey of blockchain technologies applied to software-defined networking: research challenges and solutions. IET Wirel. Sens. Syst. 11(6), 233–247 (2021). https://doi.org/10.1049/wss2.12031
17. Balu, V., P, S.: Wearable multi-sensor data fusion approach for human activity recognition using machine learning algorithms. SSRN Electron. J. (2022). https://doi.org/10.2139/ssrn.4014024
18. Uddin, M.Z.: A wearable sensor-based activity prediction system to facilitate edge computing in smart healthcare system. J. Parallel Distr. Comput. 123, 46–53 (2019). https://doi.org/10.1016/j.jpdc.2018.08.010
19. Strozzi, N., Parisi, F., Ferrari, G.: Impact of on-body imu placement on inertial navigation. IET Wirel. Sens. Syst. 8(1), 3–9 (2018). https://doi.org/10.1049/iet-wss.2017.0087
20. Hamidi, H., Fazeli, K.: Using internet of things and biosensors technology for health applications. IET Wirel. Sens. Syst. 8(6), 260–267 (2018). https://doi.org/10.1049/iet-wss.2017.0129
21. Hamrioui, S., et al.: Smart and self-organised routing algorithm for efficient iot communications in smart cities. IET Wirel. Sens. Syst. 8(6), 305–312 (2018). https://doi.org/10.1049/iet-wss.2018.5022
22. Khelifi, F., et al.: Design and experimental implementation of monitoring system in wireless sensor networks. IET Wirel. Sens. Syst. 8(6), 350–359 (2018). https://doi.org/10.1049/iet-wss.2018.5030

23. Vivekananda, G., et al.: Cloud-based effective health care management system with artificial intelligence. In: 2022 IEEE 7th International Conference for Convergence in Technology (I2CT), pp. 1–6. IEEE (2022)
24. Wang, J., Liu, J.: Deep learning for securing software-defined industrial internet of things: attacks and countermeasures. IEEE Internet Things J. 9(13), 11179–11189 (2022). https://doi.org/10.1109/jiot.2021.3126633
25. Bao, L.: Cloud connection oriented real-time monitoring system for atmospheric particles. IET Wirel. Sens. Syst. 10(1), 31–36 (2020). https://doi.org/10.1049/iet-wss.2018.5179
26. Yadav, D.K., et al.: Application of iot-fog based real-time monitoring system for open-cast mines—a survey. IET Wirel. Sens. Syst. 11(1), 1–21 (2021). https://doi.org/10.1049/wss2.12011
27. Islam, M.S., et al.: Securing smart home against sinkhole attack using weight-based ids placement strategy. IET Wirel. Sens. Syst. 13(6), 216–234 (2023). https://doi.org/10.1049/wss2.12069
28. Mhamdi, L., AbdulKhalek, H.: Congestion control in constrained internet of things networks. IET Wirel. Sens. Syst. 13(6), 247–255 (2023). https://doi.org/10.1049/wss2.12072
29. Asad, U., et al.: Human-centric digital twins in industry: a comprehensive review of enabling technologies and implementation strategies. Sensors 23(8), 3938 (2023). https://doi.org/10.3390/s23083938
30. Maddahi, Y., Chen, S.: Applications of digital twins in the healthcare industry: case review of an iot-enabled remote technology in dentistry. Virtual Worlds 1(1), 20–41 (2022). https://doi.org/10.3390/virtualworlds1010003
31. Elayan, H., Aloqaily, M., Guizani, M.: Digital twin for intelligent context-aware iot healthcare systems. IEEE Internet Things J. 8(23), 16749–16757 (2021). https://doi.org/10.1109/jiot.2021.3051158
32. Okada, T.: Handle smart contract on ethereum with arduino or esp32. Medium (2018). accessed 20 July 2021
33. Nodle: Connecting & securing the next trillion things. Available from: https://nodle.io/ (2021). accessed 22 July 2021
34. 'Helium explorer'. (2021). accessed 22-July-2021. https://explorer.helium.com/
35. Marksteiner, S., et al.: Using cyber digital twins for automated automotive cybersecurity testing. In: 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 123–128. IEEE (2022)
36. Sun, W., et al.: Lightweight digital twin and federated learning with distributed incentive in air-ground 6g networks. IEEE Transactions on Network Science and Engineering 10(3), 1214–1227 (2023). https://doi.org/10.1109/tnse.2022.3217923
37. Yao, L., et al.: Dynamic edge computation offloading for internet of vehicles with deep reinforcement learning. IEEE Trans. Intell. Transport. Syst. 24(11), 1–9 (2022). https://doi.org/10.1109/tits.2022.3178759
38. Li, T., et al.: Synchronized provable data possession based on blockchain for digital twin. IEEE Trans. Inf. Forensics Secur. 17, 472–485 (2022). https://doi.org/10.1109/tifs.2022.3144869
39. Zhu, Y., et al.: Cooperative provable data possession for integrity verification in multicloud storage. IEEE Trans. Parallel Distr. Syst. 23(12), 2231–2244 (2012). https://doi.org/10.1109/tpds.2012.66
40. Al.Dalati, I.: Digital twins and cybersecurity in healthcare systems. Elsevier (2023). https://doi.org/10.1016/b978-0-32-399163-6.00015-9
41. Zhou, L., et al.: Efficient certificateless multi-copy integrity auditing scheme supporting data dynamics. IEEE Trans. Dependable Secure Comput., 1 (2021). https://doi.org/10.1109/tdsc.2020.3013927
42. Jayashree, S., Kumar, S.V.N.S.: An efficient group signature based certificate less verification scheme for vehicular ad-hoc network. Wireless Network 30(5), 3269–3298 (2024). https://doi.org/10.1007/s11276-024-03709-1
43. Kamil, I.A., Ogundoyin, S.O.: An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks. J. Inf. Secur. Appl. 44, 184–200 (2019). https://doi.org/10.1016/j.jisa.2018.12.004
44. Liu, T., et al.: Digital-twin-assisted task offloading based on edge collaboration in the digital twin edge network. IEEE Internet Things J. 9(2), 1427–1444 (2022). https://doi.org/10.1109/jiot.2021.3086961
45. VanHuynh, D., et al.: Distributed communication and computation resource management for digital twin-aided edge computing with short-packet communications. IEEE J. Sel. Area. Commun. 41(10), 3008–3021 (2023). https://doi.org/10.1109/jsac.2023.3310087
46. Paul, A., et al.: Digital twin-assisted space-air-ground integrated networks for vehicular edge computing. IEEE Journal of Selected Topics in Signal Processing 18(1), 66–82 (2024). https://doi.org/10.1109/jstsp.2023.3340107
47. Wang, H.: Identity-based distributed provable data possession in multi-cloud storage. IEEE Transactions on Services Computing 8(2), 328–340 (2015). https://doi.org/10.1109/tsc.2014.1
48. Li, J., Yan, H., Zhang, Y.: Efficient identity-based provable multi-copy data possession in multi-cloud storage. IEEE Transactions on Cloud Computing 10(1), 356–365 (2022). https://doi.org/10.1109/tcc.2019.2929045
49. Wenhua, Z., et al.: Data security in smart devices: advancement, constraints and future recommendations. IET Netw. 12(6), 269–281 (2023). https://doi.org/10.1049/ntw2.12091
50. Aufranc, J.L.: Espressif rolls out esp32 boards for microsoft azure iot. https://www.cnx-software.com/2019/05/09 (2019). accessed: 9 May 2019
51. Khor, J.H., et al.: Public blockchain-based data integrity verification for low-power iot devices. IEEE Internet Things J. 10(14), 13056–13064 (2023). https://doi.org/10.1109/jiot.2023.3259975

How to cite this article: Jameil, A.K., Al-Raweshidy, H.: Enhancing offloading with cybersecurity in edge computing for digital twin-driven patient monitoring. IET Wirel. Sens. Syst. 1–18 (2024). https://doi.org/10.1049/wss2.12086