Journal of Theoretical and Applied Information Technology
15th January 2024. Vol.102. No 1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CONTINUOUS AND MUTUAL LIGHTWEIGHT AUTHENTICATION FOR ZERO-TRUST ARCHITECTURE-BASED SECURITY FRAMEWORK IN CLOUD-EDGE COMPUTING-BASED HEALTHCARE 4.0

WALEED ALMUSEELEM
Assistant Professor, Faculty of Computing and Information Technology, University of Tabuk, Saudi Arabia
E-mail:waleedalmuseelem@ut.edu.sa

ABSTRACT

Healthcare 4.0 is a heterogeneous environment in which many smart medical devices are connected to provide timely healthcare services. As the next generation of Healthcare 4.0 enables more digitized and interconnected services across multiple devices and communication technologies, the possibility of potential attack also expands significantly. Critical healthcare deals with highly sensitive patient data and has to fulfill strict regulatory requirements. Thus, incorporating Zero Trust Architecture (ZTA) is paramount to offer a robust framework that ensures safety and security against evolving threats. This work proposes a framework that exploits ZTA based continuous lightweight mutual authentication strategy for Healthcare 4.0 to accomplish secure data transmissions among the devices, edges, and cloud server. It is a flexible and lightweight authentication strategy that considers all the entities in Healthcare 4.0 untrusted and enables continuous authentication during every session to ensure high security against various vulnerabilities. The continuous and mutual authentication based is accomplished on two different levels. Firstly, the dynamic Hash-based Message Authentication Code (HMAC) based continuous mutual lightweight authentication is exploited two different transmissions that are Device-to-Device (D2D) and Device-to-Edge (D2E). Thus, it attains a better tradeoff between security and resource consumption over resource-constrained healthcare 4.0 devicesSecondly, the framework employs the Elliptic Curve Cryptography-Advanced Encryption Standard (ECC-AES) based heavyweight authentication and Identity Based Access Control (IBAC) to enable secure authorization and access control in Edge to Cloud Server (E2C) transmission. Further, the framework analyzes its efficiency in three ways: Scyther-tools-based security analysis, theoretical analysis, and simulation-based analysis. Moreover, the Contiki/Cooja-based simulations proved that the proposed framework is a strong competitor among various D2D and D2E authentication protocols in healthcare 4.0 environments.

Keywords: *Zero-trust architecture, Device-to-device, Device-to-Edge, Edge-to-cloud, Authentication, Authorization and Access Control*

1. INTRODUCTION

The Internet of Things (IoT) is a groundbreaking technology that establishes a global network of interconnected machines and devices enabling the ability to communicate and exchange information via the Internet. The convergence of IoT with healthcare 4.0 has ignited a wave of innovation in personalized medical devices, such as smartwatches and wearable sensors. These breakthroughs have significantly reduced the need for costly medical machinery and uncomfortable procedures, thereby reducing the reliance of patients on medical practitioners [1,2]. Smart healthcare encompasses a dynamic framework with multifaceted dimensions, including disease prevention, identification, healthcare management, patient decision-making, assessment, evaluation, and medical research [3]. Healthcare 4.0 represents a framework for connecting, automating and empowering healthcare services. Embracing Healthcare 4.0 brings substantial benefits, including the quick and more efficient detection and management of infectious diseases through healthcare data utilization [4]. The architecture promotes seamless distribution of resources and information among healthcare providers, maximizing their efficiency [5]. However, security is a major concern in the healthcare 4.0 environment. Healthcare data is highly threatened by attackers and human interventions to increase the

financial benefits and also sensitive medical data theft in increases for third-party use [6]. Surprisingly, many of the healthcare 4.0 works are lacking in integrating adequate security levels without impacting privacy in different stages of data transmission of Device-to-Device (D2D), Device-to-Edge (D2E), and Edge-to-Cloud (E2C).

Continuous mutual authentication is a good solution to give security against different attacks, as continuous authentication can repeatedly authenticate the legitimacy of a user during the time of session login or device usage. Zero Trust Architecture (ZTA) based continuous authentication constitutes an organization's cybersecurity blueprint, harnessing zero trust principles [7]. It comprehends the connections between components, strategic workflow design, and access regulations. Consequently, a zero-trust enterprise embodies the complete network framework (physical and virtual) and operational protocols established within an organization due to a zero-trust architecture strategy [8]. This methodology carries significant weight, especially in industries as sensitive as healthcare, where safeguarding patient information and fortifying vital systems take center stage [9]. To strengthen the security of the healthcare 4.0 environment, developing the ZTA-based continuous authentication is essential. However, the computational complexity of continuous authentication is very high, and it consumes more energy for healthcare 4.0 entities. In the healthcare 4.0 environment, it is a practical and fundamental problem to accomplish continuous D2D and D2E authentication owing to the smart medical devices' constrained computing resources and storage capacity [10]. These tiny and resource-restricted medical devices cannot perform complex computations like encryption and decryption operations. Hence, the design of lightweight continuous authentication is essential to solve the tradeoffs between security and resource consumption. The continuous and mutual authentication assures that the user's identity is verified continuously for each interaction. This continuous verification appends an extra layer of security to healthcare 4.0 transmission and shrinks the risk level of unauthorized access. It also assists in real-time monitoring of healthcare users' activities and provides user-friendly experiences to healthcare professionals. Albeit the continuous and mutual authentication enhances the security and performance of healthcare 4.0 systems, it is vulnerable to some attacks like key tracing. Therefore, it is crucial to ensure dynamic and continuous mutual authentication mechanism to achieve better security in healthcare 4.0. Dynamically updating the HMAC keys minimizes the prolonged exposure risks of non-dynamic keys. Moreover, the advantage of dynamic key changes in HMAC can be well-adopt with the frequently changing healthcare 4.0 environment.

Therefore, this paper aims to propose a novel security framework in which ZTA-based lightweight continuous mutual authentication is utilized for both D2D and D2E data transmissions. Also, it applies IBAC for E2C data transmission to ensure high authorization and access control in the network.

1.1. Contribution

The main contributions of the proposed security framework are as follows,

- The main intention of the proposed framework is to secure the data transmissions of the healthcare 4.0 environment by ensuring continuous authentication in D2D, D2E, and E2C. The framework includes two mechanisms to accomplish the objectives: ZTA security in D2D and D2E and ZTA security in E2C.
- To enhance the entire security level of healthcare 4.0 data transmission, the proposed framework utilizes ZTA-based dynamic HMAC continuous mutual lightweight authentication to authenticate entities. The lightweight nature of continuous mutual authentication in the zero-trust model can minimize the computational overhead, making it well-suited for a resource-constrained healthcare 4.0 environment.
- The E2C exploits ECC-AES-based authentication to ensure secure data transmission between edge and cloud. Further, IBAC allows specific identities with the permissions required to access various edge and cloud resources where only authenticated entities with the appropriate permissions can interact with particular resources.
- Finally, the Contiki/Cooja-based simulations show the effectiveness of the proposed zero-trust-based framework. The results are obtained using various metrics, that are execution time, delay, energy consumption, and computation cost.

1.2. Paper Organization

The remaining section of the paper is organized as follows. After discussing the related work with preliminaries in Section 2, this paper addresses the system model, problem statement and

overview of the proposed methodology in Section 3. Following this, section 4 organizes a detailed discussion about the proposed methodology. Section 5 provides a security and cost analysis of the proposed model. In consequence, section 6 shows the experimental result and performance metrics of the proposed model. Finally, the paper completes the conclusion in section 6.

2. LITERATURE SURVEY

This section surveys the latest research on the Zero Trust Architecture (ZTA) employed in the cloud. The Secure Access Service Edge (SASE) framework in [11] integrates network utilities and security functions at the cloud edge, minimizing costs and enhancing remote worker connectivity. Built upon Zero Trust Architecture, SASE authenticates and authorizes every request without device or user trust. The work in [12] introduces an advanced healthcare IoT system and amalgamates lightweight attribute-based encryption, edge and cloud. The solution enables data clients to execute lightweight decryption, and at the heart of this innovation is the Server-Aided Dual-Policy Attribute-Based Encryption (SA-DP-ABE) technique, offering both lightweight and robust fine-grained access control within the healthcare environment. According to [13], a categorization of MEC entities is presented for establishing a foundation for applying Zero-Trust Security (ZTS). These security measures are structured within a maturity framework to enhance trust and security in MEC set up systematically. The research paper in [14] offers an evaluation and implementation strategy for integrating Zero Trust security in virtual power plants. It defines a Zero Trust architecture tailored to this context, addressing VPP device protection through a comprehensive cyber security framework. In [15], a zero-trust access control policy to preempt MAC spoofing attacks in cloud computing's software-defined networks is proposed. Scanning of incoming traffic at OSI layers 3 and 4 extracts key details from TCP packets to reinforce security. Leveraging a multiplicative increase and additive decrease algorithm with dynamic threshold stamping, the approach efficiently validates traffic authenticity, suppressing false positives and mitigating computational overhead. The research paper [16] presents a pioneering zero-trust strategy designed for cloud environments with a conceptual "Zero Trust Model" that establishes a trust-based authorization system within the cloud setup, benefiting providers and clients. Enabling the selection of trustworthy entities will enhance the efficiency of trust management in the cloud, representing a significant advancement in the field.

An innovative network infrastructure is introduced in [17] that establishes an explicit zero-trust approach via a steganographic overlay. Implementing the principles of zero trust, the research exhibits the efficacy of a transport access control system. A Zero-Aware Smart Home System (ZASH) in [18] is an innovative Access Control solution for Smart Home Systems (SHS) that utilizes Continuous Authentication and Zero Trust principles. It leverages real-time context and edge computing, aided by Markov Chain analysis, to counter impersonation attacks targeting residents' privacy. As outlined in [19], the research paper introduces three novel authentication protocols designed specifically for IoT-based healthcare applications. Enhancement of existing M2C protocol and proposed a more efficient, hash-based M2C protocol. These advancements promise superior security, efficiency, and scalability, revolutionizing the authentication landscape in healthcare IoT systems. In reference to [20], secure Cloud Healthcare Infrastructure (CHI) in IoMT applications, establishing a strong authentication and key agreement process involving patients, cloud servers, and doctors is designed. This process ensures data security without using a cloud database system and creates a unique session key shared exclusively between patients and doctors.

Zero-trust and Edge Intelligence (ZTEI) approaches are proposed in [21] for uninterrupted authentication in satellite networks. The enhanced ZTA integrates multiple dimensions of trust, while a continuous authentication scheme monitors variable attributes throughout request lifecycles. An Edge Intelligence algorithm based on Neural-Backed Decision Trees (NBDTs) further enhances authentication accuracy. In [22], an edge-driven zero trust architecture (ZTA) is tailored for Industrial Cyber-Physical Systems (ICPS). The proposed architecture leverages the spatial and temporal granularity inherent in ICPS, aligning with zero-trust principles. Consequently, an innovative tree-based Probabilistic Distributed Collaborative Intrusion Detection System (CIDS) [23] is introduced to detect subtle and dense anomalies in service-to-service communication across various edge clusters. Incorporating a Zero Trust Network setup, the method demonstrates remarkable improvements with a 99.4% accuracy enhancement in anomaly detection. The research paper [24] presents a dual-layer zero trust architecture (ZTA) to improve edge

computing-based 5G vertical industry access control security. It involves deploying a zero-trust policy engine within the 5G core network. The dual-layer ZTA offers a comprehensive solution for enhancing security and trustworthiness in 5G MEC applications. In [25], an identity-based anonymous authentication protocol is tailored for edge computing. The protocol achieves mutual authentication and key establishment through encrypted mutual information using a thresholded identity-based proxy ring signature. The integration with edge computing leverages MEC server computational power, reducing concerns about wireless terminals and improving overall system performance.

Local and roving identity authentication protocols within a zero-trust architecture are proposed [26]. The proposed solution includes a revocable group signature program that enhances the security of key-bound expiration times. This approach optimizes identity security within the context of a zero-trust framework. Introducing a resilient ZTA-backed intrusion detection architecture to fortify 6G edge computing against network attacks [27]. A dynamic ZTA strategy optimizes security by balancing detection accuracy, false positives, false negatives, and computational overhead. The research work [28] presents the Lightweight Continuous Device-to-Device Authentication (LCDA) protocol to produce evolving session keys for uninterrupted authentication. Rigorous informal and formal analyses validate LCDA's effectiveness against various attack sectors, highlighting its potential for secure D2D communication in critical and resource-restricted environments. Most existing authentication mechanisms are static in which the pro-longed single keys are vulnerable to key tracing and compromising attacks. Later, some works utilize continuous mutual authentication strategies to ensure high security in Healthcare 4.0. However, they incur high computational overhead and increase the resource consumption level owing to the continuous verification of ZTA. Hence, it is crucial to introduce careful designs for utilizing the advantage of continuous mutual authentication to healthcare 4.0 security. Unlike traditional ZTA-based continuous mutual authentication, the proposed model enhances security with minimum cost and energy consumption over a resource-limited healthcare 4.0 environment.

2.1. Problem Formulation

Generally, IoT healthcare applications demand high security as they incorporate the highly confidential details of the patient, medical records and medical images. Most conventional healthcare 4.0 security solutions exploit static or continuous authentication strategies to secure the data transmissions of D2D and D2E. Compared with continuous authentication models, static authentication models cannot defend against different attacks, especially session hijacking attacks that risk the entire system. By considering all the entities as untrusted and consecutively verifying the legitimacy of the users during every session login, the continuous authentication models provide high security against hijacking attacks. Albeit, they increase the computation complexity and resource consumption, which are not effective for the resource-limited healthcare 4.0 scenario. Hence, novel lightweight solutions are necessary to improve secure data transmissions in lightweight healthcare 4.0 environments and prevent humans from life hazards. Therefore, the proposed framework aims to design a lightweight security algorithm that integrates ZTA-based continuous mutual authentication and IBAC for ensuring security in D2D, D2E, and D2C data transmissions.

The proposed model leverages continuous mutual lightweight authentication throughout the process to ensure security between every interaction with a lightweight authentication scheme. Lightweight authentication scheme offers several notable advantages, primarily stemming from their efficiency and resource-friendly nature, making them particularly well-suited for resource-constrained environments like IoT devices and edge computing scenarios. These schemes are designed to execute swiftly, enabling quick authentication processes, which is essential for applications requiring rapid access authorization or real-time communication. The proposed methodology also focuses on IBAC for the authorization process. For authentication, the trust evaluation set is defined as follows:

$$\text{Maximize: } \sum_{i}^{n} t_{d_i}$$

$$t_{d_i} = \left\{ t_{w1}^{d_i}, t_{w2}^{d_j} \ldots\ldots t_{wn}^{d_n} \right\} \quad (1)$$

Where, $ED = \{d_i, d_j \ldots\ldots d_n\}$ and

$TA = \{w_1, w_2 \ldots\ldots w_n\}$

Subject to

$$\begin{cases} t_{wl}^{d_i} = 0 & d_i \text{ is insecure} \\ t_{wl}^{d_i} \in (0, 0.5] & d_i \text{ is secure but inefficient} \\ t_{wl}^{d_i} \in (0.5, 1] & d_i \text{ is secure and efficient} \end{cases}$$

In the ZTA, every element within the system is treated as untrusted, necessitating authentication for all interactions. The initial step involves evaluating the trustworthiness of IoT devices, edge gateways, and cloud components. This assessment is based on individual trust attributes calculated using Equation 1. Specifically, "ED" represents the edge device during D2D interactions, signifies edge during the interactions between devices and edge gateways and denotes cloud during the interactions between edge and cloud. The trust evaluation of an entity is subjected to predefined conditions [29].

3. PRELIMINARY BACKGROUND

The proposed ZTA in Healthcare 4.0 revolves around the concept “never trust, always verify” to enhance the security of an environment. According to ZTA, all resources, including data sources, computing services and communication services, are considered suspicious entities.

3.1. System Architecture

The ZTA of Healthcare 4.0 is demonstrated in the following Figure 1. The figure shows that the architecture comprises three types of healthcare 4.0 entities: devices, edges, and a cloud server.

Cloud Server: According to the ZTA principle, the cloud server is considered an untrusted entity in the proposed model. It has unlimited power and storage capabilities. It performs every medical device's registration process and manages the devices and edges through real identity storing and initial pseudonyms. Additionally, it assists the healthcare 4.0 devices and edges to achieve continuous mutual authentication and establish a secure session key before sharing sensitive healthcare data.

Edge Devices: It is also an untrusted entity in the proposed framework owing to ZTA principal utilization. It has adequate resources and takes cloud server services very close to wireless devices. It gathers the critical healthcare information of patients from wireless medical devices and forwards them to the cloud server to provide timely healthcare services. Before establishing communication with the wireless medical device, the identity of the edge devices should be verified by the cloud server.

Wireless Medical Devices or Sensors: According to the ZTA principle, wireless devices or sensors are always untrusted and must prove their legitimacy before establishing a connection with the network. It collects the physical phenomena of the patients and sends the collected information to nearby edge devices. Before communicating with edge, the wireless device should establish a secret session key to secure communication.

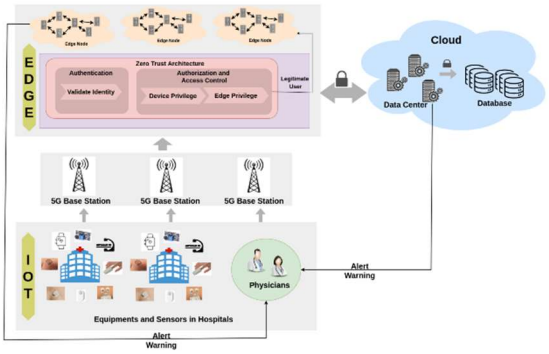


Figure 1: System Architecture of the Proposed ZTA Framework

3.2. Attack Model

In the proposed healthcare 4.0 scenario, a compromised wearable device can send incorrect data to healthcare providers. The possible threats enabling ZTA include compromised wearable devices, stolen caretaker accounts, compromised cloud servers and hacked communication networks. Zero-Trust Architecture involves authentication, authorization and access control for enhancing the security. The proposed framework intends to secure the data transmissions in edge-cloud healthcare 4.0 applications through lightweight ZTA-based continuous mutual authentication and IBAC. The proposed work can defend against the following attacks: affluent insider, password guessing, temporary information guessing, changing passwords, and traceability. In all attacks, the attacker tries to obtain information like passwords, device identity, keys, and other temporary data to launch the attack into the network. The zero-trust consideration in the proposed model can provide strong defense using lightweight and heavyweight continuous authentication mechanisms.

4. DESIGN OVERVIEW OF THE FRAMEWORK

The proposed framework exploits two authentication schemes among the healthcare 4.0 entities for enhanced security. Initially, it considers all entities untrusted and suggests continuous

verification during every session login. Initially, it implements a ZTA-based continuous mutual authentication security solution among the D2D and D2E data transmission. It significantly improves the entire security performance level using lightweight HMAC authentications with an accepted level of computational complexity and resource consumption. The proposed framework minimizes the heavyweight computations in HMAC by introducing a simple and efficient authentication procedure. Secondly, the proposed framework applies IBAC between the edge and cloud server communication, demonstrating high security in data transmissions with the assistance of ECC. Moreover, the framework escalates the entire security of Healthcare 4.0 to a remarkable level and prevents patients from hazardous healthcare situations.

ZTA-based Continuous Mutual Lightweight Authentication in D2D and D2E Data Transmission: In this phase, according to the principle of ZTA, the proposed methodology instructs the users or devices or edges to prove its legitimacy during every session login. Therefore, it involves interaction between D2D and D2E. For authenticating the interactions above of D2D and D2E, the proposed model leverages lightweight Dynamic HMAC (D-HMAC) authentication protocol for both D2D and D2E security.

E2C Authorization and Access Control: In this phase of the proposed methodology, the system will perform entity authorization and grant access control accordingly. The model utilizes IBAC to authorize access based on individual identities to achieve this. It exploits ZTA-assisted ECC-based cryptography to ensure security in E2C data transmission. When an authenticated device requests access to an edge resource, the edge component validates the device identity and permits resource utilization. Similarly, access control is implemented for cloud resources, where an authenticated edge device initiates the request to the cloud, and the identity of the edge component determines access control.

5. THE PROPOSED METHODOLOGY

The primary intention of the proposed framework is to ensure end-to-end security in Healthcare 4.0 through ZTA architecture. This approach treats all interactions and communications as potentially untrustworthy, leading to rigorous authentication, authorization, and access control measures within the environment. The proposed framework integrates two mechanisms that are ZTA-based continuous lightweight HMAC-based mutual authentication in D2D and D2E and IBAC with ECC-based E2C security, as shown in Figure 2. The ZTA-based mutual authentication continuously verifies the legitimacy of healthcare users and provides high security in D2D and D2E data transmissions. By enabling lightweight D-HMAC authentication among the D2D and D2E, the proposed work enhances the system security at a seamless level while accepting the level of computational complexity and resource consumption. Secondly, integrating strong and heavyweight IBAC with ECC among E2C data transmission significantly enhances security while providing high authentication, authorization, and access control.

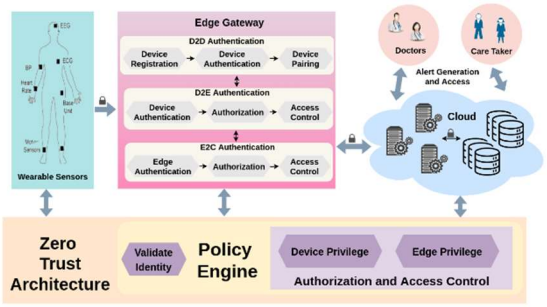


Figure 2: Overall Architecture for Proposed Model

5.1. ZTA-based Security for D2D and D2E Data Transmission

Zero Trust security is built the ZTA among the healthcare 4.0 devices, edges, and the cloud using strong identity and continuous lightweight mutual authentication. Initially, the ZTA employs Identity, the actor for several data transmissions. It restricts the identity of human users but can integrate processes and devices for independent access to valuable healthcare data. The proposed framework can assure that legitimate people have the right access level by starting with an identity to security. The proposed framework verifies the user identity before permitting them to step into the network, which is a key objective and primary function of the ZTA. Secondly, the ZTA utilizes lightweight continuous mutual authentication with HMAC to accomplish authentication. It begins with the authentication process, which involves continuous mutual authentication through the lightweight authentication process. Authentication involves confirming the identity of a user or process before granting access to the system environment. The proposed framework is employed in a real-time patient monitoring healthcare environment of a cloud-edge network. Therefore, the authentication

process is applied between D2D communication and D2E communication, which is shown in the following figure 3. The authentication between D2D and D2E is carried out using lightweight authentication, and thus, it reduces the computational complexity and resource consumption level.

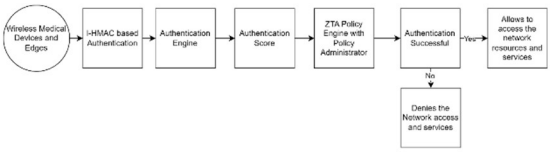


Figure 3: ZTA-based Security for D2D and D2E Data Transmission

5.1.1. D-HMAC based authentication

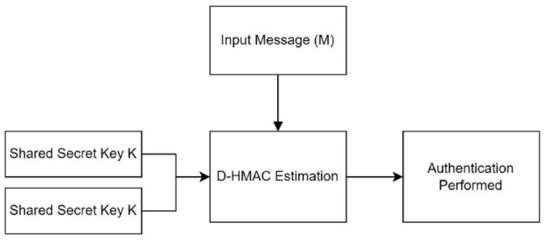


Figure 4: I-HMAC-based Authentication Process in the ZTA environment

In the ZTA healthcare environment, all network entities are considered untrusted and should be verified during every session login. The I-HMAC algorithm exploits the shared secret key and hash value to generate the HMAC authentication code for secure D2D and D2E communication, as shown in Figure 4. In the proposed D-HMAC, a partial secret key is pre-shared among the D2D entities and D2E entities during network initialization. Therefore, the entities do not need to share the shared key during every session login, reducing the HMAC calculation complexity of ZTA architecture.

D-HMAC in D2D Authentication: The authentication between D2D communication in the proposed model is carried out through dynamic Hash-based Message Authentication Code (HMAC), a cryptographic technique used to ensure the integrity and authenticity of a message. In our proposed model, the device pairing begins with the initialization phase, where two devices exchange identifiers under a secure network. After exchanging identifiers, a random number (r) is created using a Pseudo-Random Number Generator (PRNG) from a common seed value on both devices. The generated random number creates a common partial session secret key (k/2) on both devices and stores their exchanged identifiers. Once device 1 wants to pair with device 2, they request hashed identifiers to the corresponding device. On receiving the request, device 2 processes the hashed identifier to retrieve the partial session secret key and random number and searches in its database to verify the device. Further, it computes the D-HMAC value based on the input m, partial secret key during initialization, partial secret key during communication initialization and a random number. By reducing the secret key length during every session login through an initial partial key-sharing process, the proposed H-MAC minimizes the computation cost, energy consumption, and overhead in the network. Once it matches the stored identifier, it returns its hashed identifier to the corresponding device. The requested device also proceeds with the same procedure to authenticate the responded device.

Once the verification matches the same, the devices get paired and ready for transmitting the data. After the authentication process, the data to be transmitted is protected with the following process through HMAC. Mutual authentication for data (message) transmission begins with computing HMAC for outgoing messages, including timestamps and two constants, as shown in equation (2). Timestamps provide a means of time synchronization between communicating devices. Devices incorporate timestamps into the HMAC calculation. When receiving a message, a device checks that the timestamp in the message falls within an acceptable time window (not too far in the past or future). These constants (C_0 and C_1) serve as additional input for the hash function and are specific to the HMAC algorithm.

$$HMAC\_D = \begin{pmatrix} h(k/2 \oplus C_0) \parallel h(k/2 \oplus C_1) \\ \parallel M\_D \parallel T\_D \end{pmatrix} \quad (2)$$

In equation (2), the HMAC of the message from the device is computed using XOR operation between session secret key (k/2) and constant (C_0 and C_1), including message M_D and timestamp (T_D). Using equation (2), the two communication devices, Device 1 and Device 2, compute their HMAC value. Further, they match, and the timestamp is within an acceptable time window. Device 1 authenticates Device 2 within the same session. The lightweight mutual authentication between device 1 and device 2 is shown in Figure 5. This mutual device authentication is successful when the timestamp and session secret key match the same. Otherwise, it aborts the request, and the session secret key is renewed for further interaction.

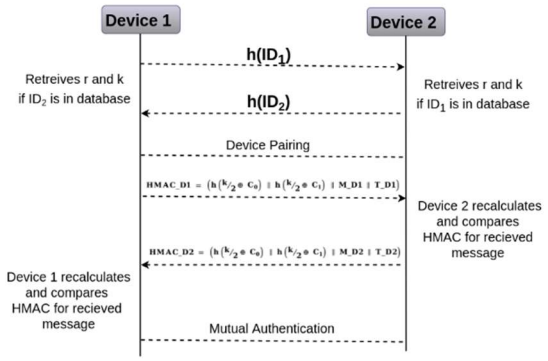


Figure 5: Sequential Diagram for D2D Authentication

Table 1: Description of Notations Used in D2D Authentication

Notation	Description
k/2	Partial Session secret key
r	Random value generated from a common seed value
C_0, C_1	Constants
M_D1, M_D2	Message or data of device1 and device2
T_D1, T_D2	Timestamp of device1 and device2
HMAC_D1, HMAC_D2	Hash-based message authentication code generated by device1 and device2

D-HMAC in D2E Authentication: The proposed framework initializes the D2E authentication whenever the data collection and transmission are performed between devices and edges. For secure data transmission to the suitable node, authentication between the device and gateway is made into progress. The proposed mutual authentication is based on a pre-shared key and comprises three phases as follows:

Initialization: The initialization setup for the device-to-edge authentication is the same as the device-to-device authentication. Unlike D2D communication, the devices exploit pre-shared keys to secure communication with edges. The D-HMAC of D2E comprises the following steps that are key pair generation and mutual authentication.

Key Pair Generation (KeyGen): KeyGen generates cryptographic key pairs: a pre-shared key (PK). These keys are essential for secure communication and authentication between the device and gateway.

Mutual Authentication (Auth): The heart of the proposed methodology, Auth is an interactive algorithm that establishes mutual authentication between edge device and gateway, denoted as A and B. It relies on the identities A and B and their key pairs (PK, k). The output of the authentication scheme is binary, and it returns one if both parties are successfully authenticated, signifying mutual trust. Otherwise, it outputs 0, indicating a failed authentication attempt.

A→B: A creates and sends a random number r_d to B along with an identifier.

$$r_d \parallel ID \quad (3)$$

B→A: B search for its corresponding pre-shared key (PK). When the pre-shared key matches the identifier, it proceeds to the next step. B creates one session secret key (k_b) gateway random number (r_g), and it sends it to A along with the device random number (r_d) in an encryption key function (e_k) through AES.

$$e_k \left(r_d \parallel r_g \parallel k_b \right) \quad (4)$$

A→B: On receiving a response from B, A decrypts through the AES technique, searches for the device random number r_d, and generates a session secret key (k_a). When the random number r_d matches the device or IoT sensors, it sends the encrypted key function (e_k) to the gateway.

$$e_k \left(r_g \parallel r_d \parallel k_a \right) \quad (5)$$

B: On receiving a response from A, B decrypts through the AES technique and searches for the gateway random number (rg); when it matches the same, a mutual authentication process is completed between the device and gateway. It returns one if both parties are successfully authenticated, signifying mutual trust. Otherwise, it outputs 0, indicating a failed authentication attempt. The session secret key expires once the request of a particular device is fulfilled. After successful mutual authentication, the device sends encrypted data to the gateway for processing. The D2E authentication is explained in Figure 6.

$$ek(data) \quad (6)$$

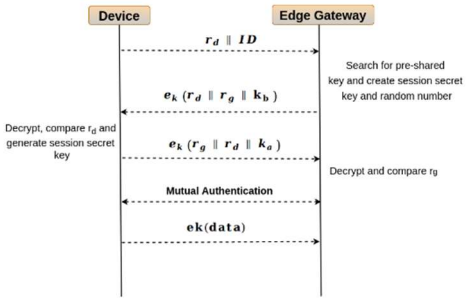


Figure 6: Sequential Diagram for D2E Authentication

Table 2: Description of Notations Used in D2E Authentication

Notations	Descriptions
r_d, r_g	Random number generated by device and gateway
PK_A, PK_B	Pre-shared key of device and gateway
k	Session secret key
e_k	Encryption function with AES technique

5.2. ZTA Security for E2C Data Transmission

The proposed framework utilizes a heavyweight ECC algorithm to secure the E2C data transmission in an enabled healthcare 4.0 environment. Hence, the cloud server is also considered an untrusted entity, comprising the entire healthcare 4.0 data. Therefore, the proposed work secures the E2C communication using a heavyweight cryptography algorithm.

Registration Phase: In the registration phase, the proposed model includes edge registration for further authentication. In the above communication or interaction, they leverage some pre-shared key for initiating the authentication process. But in this case, the proposed model begins with registration for a secured authentication process for accessing cloud resources under a secured network. The registration phase is initialized by each edge gateway to be part of the system. Gateway generates a random nonce N_g, obtains the current timestamp value T_S and computes the pseudo id of each gateway.

$$PID_g = h(N_g \parallel T\_S) \quad (7)$$

Gateway (G) sends a registration request message to cloud (C) with a pseudo id and original id to verify the gateway's validity.

$$G \rightarrow C : M_1 \{GID, PID_g\} \quad (8)$$

On receiving the requesting message from the gateway, the cloud verifies the validity of the id, and in case of correct, the cloud computes the following hashing for further authentication.

Login Phase: In the gateway, it creates a new timestamp (T_S_{new}) and new nonce value (n_{new}) and then computes h_1, h_2 and h_3 and sends M_3 to the cloud for the verification process.

ECC-based Authentication phase: The authentication process begins with verifying the legitimacy of the gateway for accepting its request. Once the registration is completed and the gateway attempts to access the cloud, it computes the below equation for initiating the authentication process.

$$H_1 = S_2 \oplus GID \quad (9)$$

$$S_2 = \begin{Bmatrix} h\left(PID_g \parallel h(ID_c \parallel c) \| h(ID_c \parallel b)\right)^* \oplus \\ h(ID_c \parallel c) \oplus h(ID_c \parallel b) \oplus GID \end{Bmatrix} \quad (10)$$

$$GID^* = \begin{Bmatrix} h\left(PID_g \parallel h(ID_c \parallel c) \| h(ID_c \parallel b)\right)^* \\ \oplus\, h(ID_c \parallel c) \oplus h(ID_c \parallel b) \oplus H_1 \end{Bmatrix} \quad (11)$$

$$S_1^* = h\left(GID^* \parallel PID_g^*\right) ?= S_1 \quad (12)$$

Above mentioned equation is computed to recover GID^* from H_1 using PID_g^*. Then, the cloud computes the second equation to obtain S_1^* and compares it with S_1. If the verification process is correct, the cloud continues by sending message M_4; otherwise, the cloud finalizes the process.

$$M_4\{h(ID_c)\} \quad (13)$$

Once the verification process is completed using the corresponding ID, the cloud sends the response to the gateway in an encrypted form. Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) represent the pinnacle of cutting-edge cryptographic techniques for safeguarding data in cloud environments. AES, with its larger key size, offers formidable security. The hybrid approach combining ECC and AES outpaces it in terms of speed. This speed gain stems from ECC's inherent property of employing smaller key sizes. Integrating ECC with AES reduces key sizes without compromising security, resulting in a more efficient data protection mechanism. ECC achieves this by establishing encryption and decryption standards that significantly shrink the key size while preserving robust security. In practice, ECC-generated keys are harnessed by AES to encrypt and decrypt data. The combined synergy of ECC and

AES makes this approach exceedingly well-suited for fortifying data security within cloud storage, ensuring a robust and efficient system.

$$G \rightarrow C : AES\{h(c \| ID_c) \| h(b \| GID) \| data\} \quad (14)$$

With the above equation, the gateway decrypts the response with the same key generated by the ECC and verifies the response. Then, the gateway sends the data in encrypted form so that a trusted cloud server can access it by decrypting it, enabling the model to be more secure. Figure 7 shows the E2C authentication process.

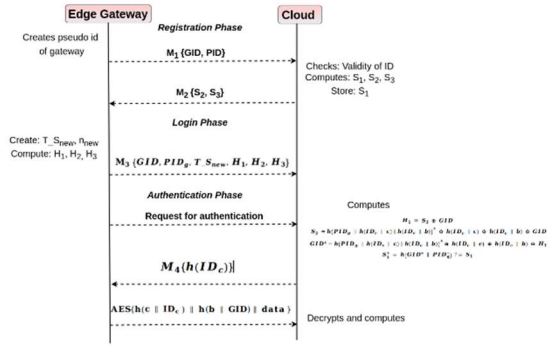


Figure 7: Sequential Diagram for E2C Authentication

Table 3: Description of Notation Used in E2C Authentication

Notations	Descriptions
PID_g	Pseudo id of edge gateway
GID	Id of gateway
ID_c	Id of cloud
N_g	Nonce number of gateways
T_S	Timestamp
M_1	A request message from the gateway
M_2	Respond to messages from the cloud.
S_1, S_2,, S_3	Security parameters
b, c	The secret key generated by ECC
H_1	Legitimacy of gateway

5.3. Edge-Cloud Authorization and Access Control

In the proposed model, the access control phase is activated when the urge to utilize the edge and cloud resource that provides access to the resource will be processed in a secure network. Once the device gets authenticated by the edge gateway, the access control alongside authorization begins within the gateway for accessing the suitable resource that includes edge and cloud resources where edge resource is merely used for computing or processing the collected data from the IoT sensors or device connected to the patients and cloud resources are used for both computing the data or signals and storing the processed data for future use.

The core focus of the model proposed revolves around utilizing Identity-Based Access Control (IBAC) as the primary method for granting access permissions and in the context of real-time healthcare monitoring within a hybrid edge-cloud environment, implementing IBAC centers on leveraging the distinct identities of sensors or devices and edge components within the hospital environment. This approach is strategically designed to establish and enforce access control policies that safeguard the security and confidentiality of patient data. Under this system, access to specific resources is granted based on the unique identity of the device linked to the task it performs. It is facilitated through an Access Control List (ACL) that necessitates system administrators to specify access privileges for resources associated with various identities. Consequently, this system ensures that only authorized entities can access and interact with critical resources, and this is achieved by implementing robust device authentication and confirming the integrity of edge components, thus enhancing overall security and data privacy.

6. FRAMEWORK AND ANALYSIS IN DIFFERENT ASPECTS

To show the efficiency and security of the framework, the scyther-tool-based analysis, security analysis, and cost analysis are performed in this section.

6.1. Scyther Tooll-based Security Analysis

The proposed model employs the well-known formal security validation tool, Scyther, to validate the security properties and correctness of the proposed scheme. The security protocol description language (SPDL) is employed to specify the proposed model by describing the protocol at a high level using formal language. This language specifies the desired security properties that define security claims the protocol should uphold, such as authentication, confidentiality, or non-repudiation. The proposed model runs the analysis to demonstrate that proclaims are satisfied as specified in the SPDL script. The proposed model is devised with the initiator IoT sensor or device, gateway and cloud. The descriptions of Nisynch and secrecy are provided in the proposed model. Even when information is sent over a public network, secrecy means no attacker will learn specific information. Furthermore, according to Nisynch, any claim that is

defined in the protocol specification that has been developed will also show up in the trace. The presented model analysis also demonstrates the validity of the additional security traits generated by Scyther, such as weak agreement (Weakagree), aliveness (Alive), and non-injective agreement (Niagree). The Scyther-based protocol verification and evaluation for the framework is explained by utilizing the following steps: creation of input, ZTA-based algorithm verification, and output generation.

a. **Creation of Input:** Initially, the Scyther tool sets the essential parameters in its window to evaluate and verify the proposed ZTA-based framework. It exploits the SPDL language to write the descriptions and coding related to the proposed model. After that, it initiates the ZTA-based algorithm verification process.

b. **ZTA-based Algorithm Verification:** The scyther protocol verification consists of the following steps that are claim, status, comments, and patterns.

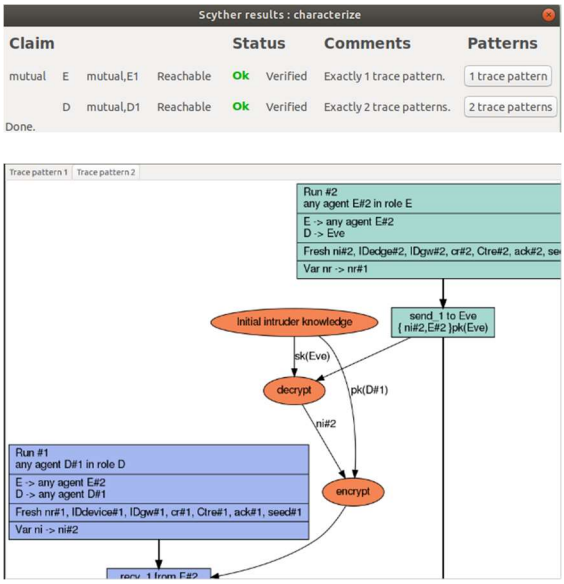
Claim: After setting the main parameters of the ZTA algorithm, it inaugurates the verification process by clicking the Verify / Verify protocol. A window appears, and each row in such window represents one claim. The claim menu shows the D2D, D2E, and E2C processes.

Status: As per the Zero-trust algorithm, the authentication parameters such as timestamps and nonce are varied. The status shows the presence of authentication attacks in terms of OK and FAIL.

Comments: It exploits the comments option to show the comments of the authentication attack. Two types of comments are presented in the verification process, such as no attacks within bounds and if there is an attack.

Pattern: It demonstrates the attack pattern of the healthcare 4.0 environment. The authentication algorithm generates Different attack patterns on the receiver side to verify the secret parameter.

c. **Output Results:** If the claim status is reachable, the trace patterns are generated. The following screenshot explains the Scyther-based evaluation and verification.



Screenshot 1: Scyther based Evaluation and Verification

6.2. Security Analysis

The proposed framework ensures security against different authentication attacks that are affluent insider attacks, password guessing attacks in both offline and online, temporary information guessing attacks, changing password attacks and traceability attacks.

Affluent Insider Attack: In this type, the attackers have high influence in the network and can extract sensitive data through different ways using their influence. By giving more careful zero-trust-based authentication steps in the login phase, the proposed framework provides high security against such attacks. The attacker has to obtain a new timestamp (T_S_{new}) and new nonce value (n_{new}) with different hash values to initiate the attacks, which is very difficult in the proposed model.

Password Guessing Attacks: In this type, the attacker retrieves the user passwords by stealing the T_S_{new}, n_{new}, and hash values in both online and offline modes. However, the framework generates new T_S_{new}, n_{new}, and dynamic hash values in every login phase and mitigates the behavior of password-guessing attacks. Also, the attackers have to guess the exact user identity to launch attacks, which is very difficult in the proposed model.

Temporary Information Guessing Attacks: In this type, the attackers utilize the known specific temporary data to launch the attacks. The framework exploits a novel timestamp and nonce generation

mechanism in the authentication phase to prevent the specific temporary information attack.

Changing Password Attacks: If an attacker wants to launch a password-changing attack, first, it must know the user identity and password data before passing to the equation verification performed in the authentication phase. As mentioned in the login and authentication phase, the attacker cannot obtain user identity and password in any way. Therefore, the proposed framework gives high security against changing password attacks.

Traceability Attacks: Generally, the traceability attacker has to eavesdrop on two various session login and authentication messages to compare them to launch attacks. If the two obtained messages have nearly similar data, the attacker can infer that the information belongs to the same user. In such a way, the attacker tracks the login activity of a single user. By providing dynamic zero-trust authentication through equation verification, the proposed framework strictly restricts the attacker from tracking any data and assures security against traceability attacks.

6.3. Cost Analysis

The cost analysis is performed in three aspects: communication, computation, and storage.

Communication Cost: This cost considers the frequency of transmission and the volume of data. Healthcare organizations must balance data transmission frequency and volume to optimize communication costs.

$$\text{Communication Cost} = CT * DS$$

Where CT refers to the communication time, and DS refers to the length of the communication data.

Computation Cost: The formula for computation cost in the context of a proposed model encapsulates several key factors. The utilized mutual authentication scheme's computational demands are considered by the encryption algorithm complexity metric in the process. The term key length describes the size of the cryptographic keys used, which affects the model's security and computational requirements. The number of rounds indicates the complexity of the mutual authentication procedure in the AES algorithm.

The fact that the cost increases with the number of authentication requests is acknowledged by multiplying by the number of authentications. The hardware/software overhead analyses the effects of choosing a hardware/software-based implementation operation. As it affects the overall effectiveness of the scheme, the server load represents the server's processing power. Cryptographic Operation Cost considers the computational cost of the various cryptographic operations involved, including hashing, encryption, and decryption. In the Healthcare 4.0 setting, this thorough formula helps evaluate the computing costs of mutual authentication.

$$\text{Computation Cost} = (\tau + K_l + n) * A_n * O_{s/h} * S_l * \omega$$

Where, τ - algorithm complexity,
K_l - key length
n - number of rounds (AES)
A_n - Authentication rounds
$O_{s/h}$ - software/hardware overhead
S_l - server overload
ω - cryptographic operation cost

Table 4 compares the computational complexity of the proposed authentication schemes under D2D, D2E, and E2C scenarios.

Table 4: Computational Complexity of the Proposed ZTA Framework

Lightweight Algorithms	Key Length	Sub-Bytes	Encryption and Decryption cost	Computational Complexity
D-HMAC in D2D	32 Bits	2L	O (n), n=1 to n times at devices	O(D-HMAC (32))=2L+(K/2+26O)+16 M
D-HMAC in D2E	64 Bits	4L	O(n) , n=1 to n times at edges	O(D-HMAC (64))=4L+(K/2+206O)+3 2M
ECC in D2C	64 Bits	4L	O(n) , n=1 to n times at cloud server	O(ECC(64))=4L +(K*42O+32M)
AES in D2C	128 Bits	8L	O(n) , n=1 to n times at cloud server	O(AES(128))=8L+13O+ 16M

Storage Cost: The storage cost for a mutual authentication scheme in Healthcare 4.0, specifically when using AES and ECC, can be estimated using the following formula,

$$\text{Storage Cost} = K_s + D_s$$

Where, K_s - Key storage and D_s - data storage

Key Storage encompasses the storage requirements for the cryptographic keys essential for the AES with the ECC mutual authentication scheme. This entails the preservation of both the public and private keys for ECC and potentially symmetric keys for AES, contingent upon the specific configuration for authentication and encryption. The sizes of the cryptographic keys vary to meet the security requirements, and their storage capacity is typically measured in bits or bytes. Data Storage refers to the distribution of storage resources

required to accommodate various types of authentication-related data, including components like session tokens, certificates, and logs important to the authentication process. Accurate assessment of key and data storage is vital for prudent resource allocation and the seamless operation of mutual authentication processes in the Healthcare 4.0 ecosystem.

7. PERFORMANCE EVALUATION

The effectiveness of the proposed ZTA-based security framework is analyzed using Contiki/Cooja-based simulations. The simulation on healthcare 4.0 nodes is conducted using Ubuntu 14.04 LTS 64bit and Instant Contiki-3.0. The Contiki/Cooja is an open-source network simulator that is highly adaptable to simulate the healthcare 4.0 environment in which the devices are restricted in power, memory, and bandwidth. It allows different levels of simulations from data to application layer. Here, it simulates the CoAP-based IoT-assisted healthcare 4.0 scenario with high flexibility. The proposed work analyzes the performance of the ZTA authentication protocol in two scenarios: device-to-device and device-to-edge. Hence, device-to-device communication comprises zero intermediary devices, whereas device-to-edge communication has zero or more devices and enables single or multi-hop communication. For evaluation, the performance of device-to-device ZTA communication of the proposed framework is compared with existing M2M [19] and LCDA [28] protocols. Secondly, the device-to-edge communication in the proposed framework is compared with the ECCbAP [30] and novel server-less mutual authentication (NSMA) [31]. The following table 5 demonstrates the simulation parameters of the proposed ZTA framework.

Table 5: Simulation Parameters

Parameters	Values
Application Protocol	CoAP
Total Number of Nodes	50
Total Number of Edges	5
Cloud Server	1
IoT Devices	Wearable, Disposable Patch, and Ambient
Number of attackers	10%
Data rates (bits/second)	128
Simulation Area	100mx100m
Transmission Range	50m
Simulation Time	5 Minutes
Algorithms	AES and ECC

7.1. Performance Metrics

The performance of the proposed ZTA authentication framework is obtained using the following metrics that are as follows.

Execution Time: It is the time taken to perform the authentication-related security functions in the network.
Delay: The amount of time the devices require to accomplish authenticated services.
Energy Consumption: The amount of energy the security algorithm needs to perform authentication, authorization, and access control.
Computational Cost: It refers to the number of authentication functions used to complete network security.

6.2. Simulation Results

The simulation results are obtained for two communication scenarios that are ZTA D2D communication and ZTA D2E. To analyze the effectiveness of the proposed model under different attack scenarios, the number of attackers is varied from 2 to 10.

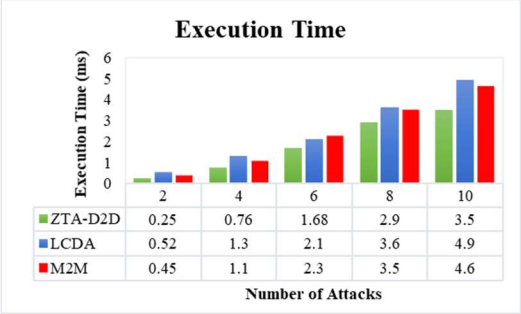


Figure 8: Number of Attackers Vs Execution Time

Figure 8 shows the execution time of three protocols, ZTA D2D, LCDA, and M2M, obtained for different attack scenarios. The results demonstrate that all protocols increase the execution time by adjusting the number of attackers from 2 to 10. For instance, the ZTA D2D, LCDA, and M2M attain 0.25, 0.52, and 0.45 seconds of execution time for two attackers, and it is varied by 3.5, 4.9, and 4.6 seconds for ten attackers. However, the performance of the proposed ZTA-D2D is higher than the existing algorithms due to the design of lightweight authentication using D-HMAC. For example, the proposed ZTA-D2D decreases the execution time by 1.4 and 1.1 seconds than the LCDA and M2M protocols.

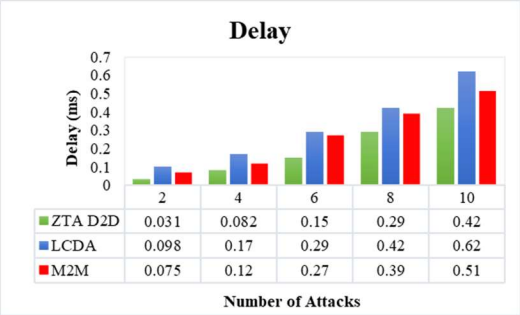


Figure 9: Number of Attackers vs. Delay

Figure 9 illustrates the delay of ZTA-D2D, LCDA, and M2M protocols obtained for various attack scenarios. All protocols escalate the delay with increasing the number of attacks, as the authentication is performed against many attacks. For example, the ZTA-D2D attains 0.031 seconds and 0.42 seconds of delay for 2 and 10 attackers, respectively. Albeit, it shows its superior performance over the other two protocols under all attack scenarios. The zero-trust architecture and lightweight authentication diminish the delay in the proposed ZTA-D2D communication. For example, the ZTA-D2D, LCDA, and M2M protocols attain 0.42, 0.62, and 0.51 seconds of delay for ten attack scenarios, respectively.

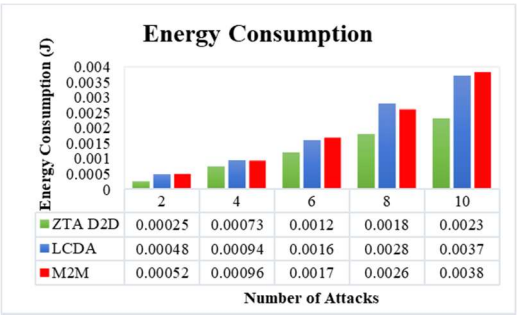


Figure 10: Number of Attackers vs. Energy Consumption

The energy consumption comparison results of ZTA-D2D, LCDA, and M2M protocols are depicted in Figure 10. The results are obtained by varying the number of attacks from 2 to 10. Initially, the ZTA-D2D consumes 0.00025 joules of energy for two attack scenarios; after, it is varied by 0.0023 joules to provide authentication against ten attackers. It is minimal when compared with the other two existing protocols. The ZTA-based improved lightweight D2D authentication significantly reduces the energy consumption level in the proposed strategy. For instance, the energy consumption of ZTA-D2D, LCDA, and M2M protocols are 0.0023, 0.0037, and 0.0038 joules for ten attackers.

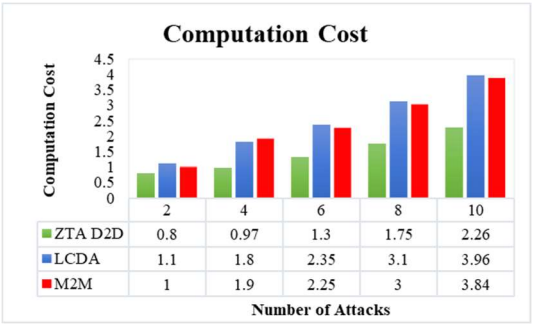


Figure 11: Number of Attackers vs. Computation Cost

Figure 11 shows the computation cost of three protocols that are ZTA-D2D, LCDA, and M2M, obtained for various numbers of attackers. The computation cost is increased by adjusting the number of attackers from low to high. The main reason behind this is that the protocols should have to perform authentication against many attacks. However, the proposed ZTA-D2D minimizes the computation cost through its lightweight design. For example, the ZTA-D2D, LCDA, and M2M protocols obtain 2.26, 3.96, and 3.84 computation cost values when ten authentication attacks are presented in the network.

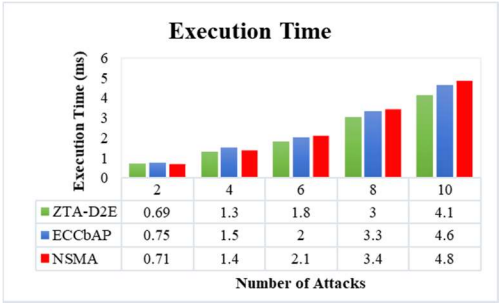


Figure 12: Number of Attackers Vs Execution Time

Figure 12 shows the execution time of various authentication mechanisms, that are ZTA-D2E, ECCbAP, and NSMA. For effective analysis, the simulation results are obtained for diverse attack scenarios. The protocols increase the execution time by varying the number of attacks from 2 to 10. It is caused due to perform authentication for a huge number of devices in the network. For example, the execution time of ZTA-D2E is 0.69 seconds and 4.1 seconds, respectively, for 2 and 10 attackers. Albeit, the proposed ZTA-D2E utilizes zero-trust lightweight mutual authentication to enable device-to-edge communication. Thus, it significantly minimizes the execution time without compromising the security level. For instance, the execution time of ZTA-D2E, ECCbAP, and NSMA are 4.1, 4.6, and

4.8 seconds, respectively, when 10 attackers are in the network.

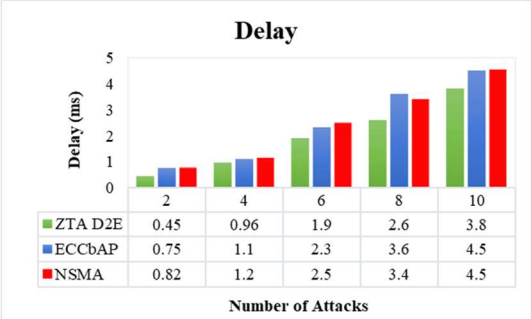


Figure 13: Number of Attackers vs. Delay

Figure 13 illustrates the delay of ZTA-D2E, ECCbAP, and NSMA protocols obtained by adjusting the number of attacks from 2 to 10. The ZTA-D2E attains 0.45 and 3.8 seconds of delay, respectively, for 2 and 10 attackers in the network. The proposed ZTA-D2E minimizes the delay compared to ECCbAP and NSMA by incorporating lightweight mutual authentication to perform secure device-to-edge communication. For example, the ZTA-D2E, ECCbAP, and NSMA accomplish 3.8, 4.5, and 4.5 delay when 10 attackers are available in the network. Hence, the ZTA-D2E delay is reduced by 15.6% than the other two protocols.

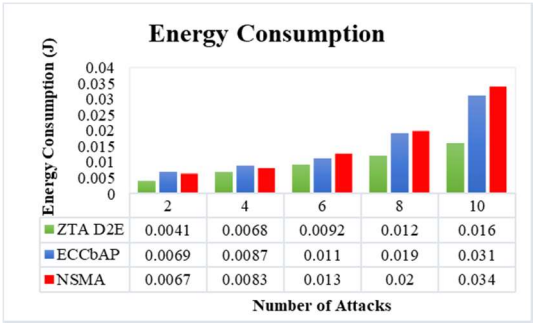


Figure 14: Number of Attackers vs. Energy Consumption

Figure 14 demonstrates the energy consumption results of ZTA-D2E, ECCbAP, and NSMA protocols. The results are obtained by increasing the number of attackers from 2 to 10. The ZTE-D2E increases the energy consumption by varying the attacker density from low to high. The number of hops between D2E communication also escalates the energy consumption level. For instance, the ZTA-D2E accomplishes 0.0041 and 0.16 joules of energy consumption results, respectively, for 2 and 10 attackers. However, the lightweight design of ZTA-D2E significantly minimizes the energy consumption results those the other two protocols. For example, the ZTA-D2E, ECCbAP, and NSMA consume 0.016, 0.031, and 0.034 joules of energy to provide authentication against 10 attackers, respectively.

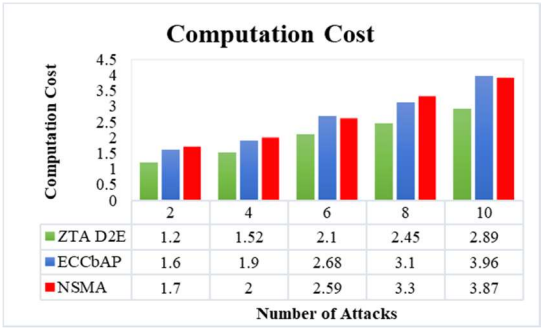


Figure 15: Number of Attackers Vs Computation Cost

Figure 15 compares the computation cost of ZTA-D2E, ECCbAP, and NSMA protocols for different attack scenarios. Each protocol increases the computation cost by adjusting the attacks from 2 to 10. It is caused due to the protocols that have to perform mutual authentication against many attacks. For instance, the proposed ZTA-D2E obtains 1.2 and 2.89 computation cost values for 2 and 10 attack scenarios, respectively. However, it is minimal when compared to the existing works. The zero-trust and lightweight mutual authentication in every iteration can increase the security level without escalating the computation cost as high. For example, the computation costs of ZTA-D2E, ECCbAP, and NSMA are 2.89, 3.96, and 3.87, respectively, when ten numbers of attackers are presented in the network.

Result Discussions:

The proposed framework integrates the continuous lightweight HMAC to authenticate the healthcare users at every data transmission. Compared to the existing continuous lightweight strategies, the continuous lightweight HMAC of the proposed work minimizes the secret key length without impacting the security level. Also, the proposed D-HMAC shrinks the computation cost, energy consumption, and overhead in the healthcare 4.0 environment by reducing the secret key length during the login of every session and an initial partial key sharing strategy. Here, is a discussion of how the proposed continuous lightweight D-HMAC authentication is varied from existing lightweight models.

Strong Security: The conventional lightweight authentication strategies employ fixed and long-terms keys to minimize the computational cost and overhead vulnerable to key compromise-related attacks. The proposed H-MAC reduces the

secret key length and dynamically changes the keys over a particular period, resulting in minimum cost without impacting the security level.

High Adoptability to Evolving Threats: Conventional lightweight solutions might lack the flexibility to rapidly adapt to evolving threat landscapes. Dynamically updating the proposed D-HMAC keys permits the healthcare 4.0 system to adapt highly to emerging threats. It also ensures that any key compromise may occur, limiting the threat impact over the hot period.

Handling of Resource Limitation Issues: The proposed D-HMAC utilizes the minimum length secret keys and a partial initial key strategy to ensure security, significantly reducing resource consumption with less computation cost and ensuring high security.

Suitability of Healthcare 4.0 Environment: The conventional works are lacking to address the challenges in authentication of healthcare 4.0 environment, resulting in poor suitability of lightweight authentication. Despite this, the proposed D-HMAC design considers the healthcare 4.0 characteristics and improves authentication performances.

Furthermore, the continuous and lightweight D-HMAC authentication employs periodic updates of keys and the management of dynamic keys. The adaptability of such algorithms can effectively mitigate the security risks associated with long-term lightweight key usage algorithms in existing works. The healthcare 4.0-specific design considerations also make the proposed D-HMAC well-suited for scenarios like healthcare 4.0 applications in which security and resource efficiency are critical.

8. CONCLUSION

The proposed model establishes a secure network environment by implementing ZTA within the cloud-edge Healthcare 4.0 application context. This work contributes to the foundation of secure, efficient, and compliant healthcare systems in our increasingly interconnected and data-driven world. Adopting Zero-Trust Architecture in healthcare settings that rely on cloud-edge computing is feasible and crucial. Security is improved through continuous lightweight HMAC mutual authentication in all interactions, with access control based on identity privileges. Mutual authentication between devices, edge components and the cloud is pivotal in building trust within the un-trusted environment. This bidirectional D-HMAC authentication ensures that only verified and authorized entities engage in data exchange, safeguarding patient privacy and data integrity with acceptable computational costs. Albeit, the proposed D-HMAC significantly minimizes the cost of resource-limited healthcare devices by reducing the secret key length without affecting the security level. This bidirectional authentication ensures that only verified and authorized entities exchange data, safeguarding patient privacy and data integrity. The proposed model also leverages a lightweight authentication scheme. Access authorization to requested resources is granted based on identity privilege with IBAC, offering a versatile and effective access management approach. This approach enhances security, scalability, flexibility, and compliance while simplifying access policy administration.

In the future, the framework will be extended to defend against wider attacks and provide security awareness in 5G healthcare scenarios with minimum computational cost and resources. Hence, the wider attack knowledge will be obtained through a comprehensive analysis of evolving threats in the 5G healthcare environment. Future work will be planned to extend the proposed D-HMAC authentication to digitally sensitive patient record-maintaining applications with high interoperable data sharing. Also, the proposed work will be planned to conduct an in-depth analysis of implementing zero-trust-based security architecture in real-time healthcare 4.0 and 5.0 scenarios.

REFERENCES

[1] Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., Niyato, D., … Poor, H. V. (2021). 6G Internet of Things: A comprehensive survey. Retrieved from http://arxiv.org/abs/2108.04973

[2] Wu, Y. (2021). Cloud-edge orchestration for the Internet of things: Architecture and AI-powered data processing. *IEEE Internet of Things Journal*, *8*(16), 12792–12805. doi:10.1109/jiot.2020.3014845

[3] Azimi, I., Anzanpour, A., Rahmani, A. M., Pahikkala, T., Levorato, M., Liljeberg, P., & Dutt, N. (2017). HiCH: Hierarchical fog-assisted computing architecture for healthcare IoT. *ACM Transactions on Embedded Computing Systems*, *16*(5s), 1–20. doi:10.1145/3126501

[4] Jayaraman, P. P., Forkan, A. R. M., Morshed, A., Haghighi, P. D., & Kang, Y.-B. (2020). Healthcare 4.0: A review of frontiers in digital health. *Wiley Interdisciplinary Reviews. Data*

Mining and Knowledge Discovery, *10*(2). doi:10.1002/widm.1350

[5] Khelassi, A., Estrela, V. V., Monteiro, A. C. B., França, R. P., Iano, Y., & Razmjooy, N. (2019). Health 4.0: Applications, Management, Technologies and Review. *Medical Technologies Journal*, *2*(4), 262–276. doi:10.26415/2572-004x-vol2iss4p262-276

[6] Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. *Computer Communications*, *153*, 311–335. doi:10.1016/j.comcom.2020.02.018

[7] He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing*, *2022*, 1–13. doi:10.1155/2022/6476274

[8] Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (ZTA): A comprehensive survey. *IEEE Access: Practical Innovations, Open Solutions*, *10*, 57143–57179. doi:10.1109/access.2022.3174679

[9] Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., … Zhai, Y. (2021). A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. *IEEE Internet of Things Journal*, *8*(13), 10248–10263. doi:10.1109/JIOT.2020.3041042

[10] Li, S., Iqbal, M., & Saxena, N. (2022). Future industry Internet of Things with zero-trust security. *Information Systems Frontiers: A Journal of Research and Innovation*. doi:10.1007/s10796-021-10199-5

[11] Yiliyaer, S., & Kim, Y. (2022). Secure access service edge: A zero trust based framework for accessing data securely. *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE.

[12] Xu, S., Li, Y., Deng, R. H., Zhang, Y., Luo, X., & Liu, X. (2022). Lightweight and expressive fine-grained access control for healthcare internet-of-things. *IEEE Transactions on Cloud Computing*, *10*(1), 474–490. doi:10.1109/tcc.2019.2936481

[13] Ali, B., Hijjawi, S., Campbell, L. H., Gregory, M. A., & Li, S. (2022). A maturity framework for zero-trust security in multiaccess edge computing. *Security and Communication Networks*, *2022*. https://doi.org/10.1155/2022/3178760

[14] Alagappan, A., Venkatachary, S. K., & Andrews, L. J. B. (2022). Augmenting Zero Trust Network Architecture to enhance security in virtual power plants. *Energy Reports*, *8*, 1309–1320. doi:10.1016/j.egyr.2021.11.272

[15] Mandal, S., Khan, D. A., & Jain, S. (2021). Cloud-based zero trust access control policy: An approach to support work-from-home driven by COVID-19 pandemic. *New Generation Computing*, *39*(3–4), 599–622. doi:10.1007/s00354-021-00130-6

[16] Mehraj, S., & Banday, M. T. (2020). Establishing a zero trust strategy in cloud computing environment. *2020 International Conference on Computer Communication and Informatics (ICCCI)*. IEEE.

[17] DeCusatis, C., Liengtiraphan, P., Sager, A., & Pinelli, M. (2016). Implementing zero trust cloud networks with transport access control and first packet authentication. *2016 IEEE International Conference on Smart Cloud (SmartCloud)*. IEEE.

[18] da Silva, G. R., Macedo, D. F., & dos Santos, A. L. (2021). Zero Trust Access Control with context-aware and behavior-based Continuous Authentication for smart homes. *Anais Do XXI Simpósio Brasileiro de Segurança Da Informação e de Sistemas Computacionais (SBSeg 2021)*. Sociedade Brasileira de Computação - SBC.

[19] Merabet, F., Cherif, A., Belkadi, M., Blazy, O., Conchon, E., & Sauveron, D. (2020). New efficient M2C and M2M mutual authentication protocols for IoT-based healthcare applications. *Peer-to-Peer Networking and Applications*, *13*(2), 439–474. doi:10.1007/s12083-019-00782-8

[20] Kumar, V., Mahmoud, M. S., Alkhayyat, A., Srinivas, J., Ahmad, M., & Kumari, A. (2022). RAPCHI: Robust authentication protocol for IoMT-based cloud-healthcare infrastructure. *The Journal of Supercomputing*, *78*(14), 16167–16196. doi:10.1007/s11227-022-04513-4

[21] Fu, P., Wu, J., Lin, X., & Shen, A. (2022). ZTEI: Zero-trust and edge intelligence empowered continuous authentication for satellite networks. *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*. IEEE.

[22] Lei, W., Pang, Z., Wen, H., Hou, W., & Zhang, X. (2023, May). Edge-enabled Zero Trust Architecture for ICPS with Spatial and Temporal Granularity. In *2023 IEEE 6th International Conference on Industrial Cyber-Physical Systems (ICPS)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICPS58381.2023.10127999

[23] Sharma, R., Chan, C. A., & Leckie, C. (2023, May). Probabilistic Distributed Intrusion Detection For Zero-Trust Multi-Access Edge Computing. In *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium* (pp. 1-9). IEEE. https://doi.org/10.1109/NOMS56928.2023.10154326

[24] Feng, Z., Zhou, P., Wang, Q., & Qi, W. (2022, August). A dual-layer zero trust architecture for 5g industry mec applications access control. In *2022 IEEE 5th International Conference on Electronic Information and Communication Technology (ICEICT)* (pp. 100-105). IEEE. https://doi.org/10.1109/ICEICT55736.2022.9908891

[25] Meng, L., Huang, D., An, J., Zhou, X., & Lin, F. (2022). A continuous authentication protocol without trust authority for zero trust architecture. *China Communications*, *19*(8), 198–213. doi:10.23919/jcc.2022.08.015

[26] Liu, H., Ai, M., Huang, R., Qiu, R., & Li, Y. (2022). Identity authentication for edge devices based on zero-trust architecture. *Concurrency and Computation: Practice & Experience*, *34*(23). doi:10.1002/cpe.7198

[27] Sedjelmaci, H., & Ansari, N. (2023). Zero trust architecture empowered attack detection framework to secure 6G edge computing. *IEEE Network*. https://doi.org/10.1109/MNET.131.2200513

[28] Shah, S. W., Syed, N. F., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2021). LCDA: Lightweight continuous device-to-device authentication for a zero trust architecture (ZTA). *Computers & Security*, *108*(102351), 102351. doi:10.1016/j.cose.2021.102351

[29] Zhang, L., Zou, Y., Wang, W., Jin, Z., Su, Y., & Chen, H. (2021). Resource allocation and trust computing for blockchain-enabled edge computing system. *Computers & Security*, *105*(102249), 102249. doi:10.1016/j.cose.2021.102249

[30] Rostampour, S., Safkhani, M., Bendavid, Y., & Bagheri, N. (2020). ECCbAP: A secure ECC-based authentication protocol for IoT edge devices. *Pervasive and Mobile Computing*, *67*(101194), 101194. doi:10.1016/j.pmcj.2020.101194

[31] Sheu, R.-K., Pardeshi, M. S., & Chen, L.-C. (2022). Autonomous mutual authentication protocol in the edge networks. *Sensors (Basel, Switzerland)*, *22*(19), 7632. doi:10.3390/s22197632