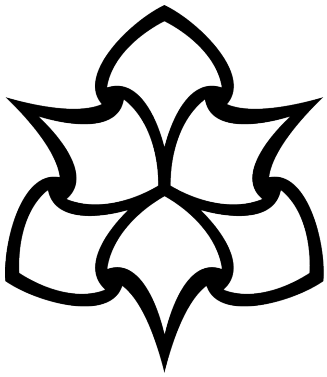

An Anonymous Device to Device Access Control based on Secure Certificate for Internet of Medical Things Systems

Shehzad Ashraf Chaudhry, Azeem Irshad, Jamel Nebhen, Ali Kashif Bashir, Nour Moustafa, Yasser D. Al-Otaibi, Yousaf Bin Zikria*

Abstract

The Internet of Medical Things (IoMT) is structured upon both the sensing and communication infrastructure and computation facilities. The IoMT provides the convenient and cheapest ways for healthcare by aiding the remote access to the patients' physiological data and using machine learning techniques for help in diagnosis. The communication delays in IoMT can be very harmful to healthcare. Device to device (D2D) secure communication is a vital area that can reduce communication delays; otherwise, caused due to the mediation of a third party. To substantiate a secure D2D communication framework, some schemes were recently proposed to secure D2D based communication infrastructure suitable for IoMT-based environments. However, the insecurities of some schemes against device physical capture attack and non-provision of anonymity along with related attacks are evident from the literature. This calls for a D2D secure access control system for realizing sustainable smart healthcare. In this article, using elliptic curve cryptography, a certificate based D2D access control scheme for IoMT systems (D2DAC-IoMT) is proposed. The security of the proposed D2DAC-IoMT is substantiated through formal and informal methods. Moreover, the perfor-

mance analysis affirms that the proposed scheme provides a good trade-off between security and efficiency compared with some recent schemes.
Keywords: IoMT, Key Establishment, Device Access Control ,Certificate, Stolen IoMT device

1. Introduction

Internet of Things (IoT) is an infrastructure of connected devices to communicate and exchange information, and it is an integral part of smart city realization. The connected devices include all digital devices like home appliances, cameras, smartphones, vehicles, PDAs, RFID tags, etc. The connectivity of these objects is realized through the public internet to extend continuous global access. The IoT connects heterogeneous systems and provides a broad range of applications such as smart cities, intelligent transportation systems, smart grids, smart parking systems, and digital healthcare systems called the Internet of Medical Things (IoMT). The connected IoT devices are expected to reach 500 billion by 2025 as predicted by Cisco (Ni et al., 2018), which may lead to huge data and require massive storage, computing, and bandwidth capacities to store, manipulate and communicate huge data(Evans, 2011; Deebak, 2020).

The heterogeneity of the devices in IoMT as a sub-application of the smart city is not limited to network infrastructure, but it also applies to resource availability. Many such devices have low computation communication and storage powers and are also battery operated and demand lightweight protocols for in-device and remote operations.

The improvement in hardware and usage techniques like efficient band-

width utilization also plays a part in IoMT growth. Many systems like cyber physical systems, machine to machine, and wireless sensor networks are evolved as integral parts of IoMT. Thus securing these requires a customized solution to provide direct device to device (D2D) communication, without any third party mediation cause a delay in delay sensitive D2D architecture (Laufs et al., 2020; Shafiq et al., 2020). Moreover, the underlying open communication architecture and heterogeneity of connecting devices consequent to more security and privacy threats than traditional networks (Khan and Salah, 2018). The sustainable healthcare and other applications of the sustainable smart city concept can only be realized subject to the proper security measures (Deebak, 2020; Reddy et al., 2018). Moreover, the security solution adopted should comply with resource constrained nature of IoMT devices(Deebak and Al-Turjman, 2021).Recently, some articles identified the need for security and privacy in IoT and/or IoMT systems (Khan and Salah, 2018; Yang et al., 2017; Park et al., 2020).Among other challenges, device access control is considered an utmost vital method to secure the IoMT system, and lightweight methods must provide domain-specific access control mechanisms.

The wireless and resource constrained nature (sensing, storage, and computation) of IoMT devices calls for a lightweight IoMT security solution (Bhavsar et al., 2021; Arul et al., 2019). Specifically, the device physical capture attack (DPC) can adversely affect the whole IoMT network. Along with the device anonymity, the DPC attack is not given due importance in recent works. This article proposes a direct D2D access control scheme to provide security against the known attacks. Specifically, the pitfalls of device physical capture attack and device anonymity provision are given much importance

while designing the proposed scheme. We used functional and formal security analysis to show the proposed protocol's resilience against various attacks, including DPC. The proposed scheme provides device authentication and key agreement among different IoMT devices in homogeneous and heterogeneous IoMT networks.

1.1. Contributions

The contributions of this article are manifold and are described as follows:

- A direct device to device (D2D) access control scheme "D2DAC-IoMT" is proposed in this paper using the symmetric key primitives and Elliptic-curve cryptography ECC based device specific certificates.
- D2DAC-IoMT provides certificate based direct device to device access control. Once a device is registered with the gateway and gets its device specific certificate, it can establish a secure connection with registered peers. The registered devices first mutual authenticate each other to establish a secure connection and then share a session key.
- The proposed D2DAC-IoMT is provably secure under the RoR (real or random) model. The RoR security proves, and discussion on security requirements shows that the proposed scheme provides resistance to various known attacks, including device physical capture attacks.
- The proposed D2DAC-IoMT is compared with related exiting schemes using security requirements, communication, and computation costs for comprehensive performance and security evaluations.

Table 1: Notation guide

Notations	Description
$\|\|, \oplus$	concatenation and xor operators
$h(.), \stackrel{?}{=}$	Hash function, Equality Verification
$SD_x,\ ID_{sdx}$	Sensing Device, Identity of SD_x
$GWD,\ ID_{gwd}$	Gateway Device, Identity of GWD
$E_\alpha(i,j),\ G$	Elliptic Curve, Base point over $E_\alpha(i,j)$
$(k_{gwd}, K_{gwd} = k_{gwd}G)$	Private and Public key pair of GW_d
$(k_{sdx}, K_{sdx} = k_{sdx}G)$	Private and Public key pair of SD_x
cer_{sdx}, sig_{sdx}	Certificate and Signature of SD_x
$T_{sdx},\ \Delta T$	Time-stamp of SD_x, Allowable delay
$\mathcal{A}, \mathcal{U}_\mathcal{A}$	Notations for Adversary

The rest of the paper is organized as follows, Table 1 illustrates the notations used in this paper and their representations. In Section 2, we present related work and Section 3 briefly discusses the adopted system model. Section 4 presents our proposed scheme. In Section 5, a discussion on functional security of the proposed scheme is presented, the formal security analysis of the proposed scheme is shown in Section 6. The performance and security features analysis is provided in Section 7. Finally, the concluding remarks are given in Section 8.

2. Related Work

Recently, many access control schemes are proposed to secure sensing based IoT systems. In such an attempt, Zhou et al. (2007) presented an ECC and

certificate based protocol to secure devices in wireless sensor networks (WSN). In 2011, Huang (2011) designed another scheme using schnorr's signature (Schnorr, 1991). Later in 2014,Chatterjee et al. (2014) proved that Huang's scheme could not resist a man in the middle attack. They also designed another access control scheme using ECC and hash functions. Huang and K. C. Liu (2008) also proposed another certificate less access control scheme. Soon Kim and Lee (2009) proposed an improved access control scheme after showing the insecurity of Huang (2009)'s scheme against the replay attack. However, Zeng et al. (2010) found some weaknesses in the scheme of Kim and Lee (2009). In 2016, Li et al. (2016) presented an access control system for WSN using computation hungry bilinear parings. Braeken et al. (2016) also presented an access scheme for smart homes using only lightweight symmetric key operations. Luo et al. (2018) also proposed an identity based scheme using computation extensive bilinear pairing operations. Moreover, Luo et al.'s scheme does not provide mutual authentication and anonymity. The schemes presented in (Zeng et al., 2010; Li et al., 2016; Braeken et al., 2016) use the mediating gateway to access IoT device.

Recently in 2019, Malani et al. (2019) presented a new certificate based scheme for access control in IoT based devices using ECC (DACS-IoT) and claimed that their scheme is secure against various attacks, including device physical capture attacks. However, the device specific certificate cer_{sdz} generated by GWD in Malani et al.'s DACS-IoT scheme is not secure and can be used to expose the private key of GWD. Any adversary $\mathcal{A}$ after physical capturing of a single device, say SD_z can easily extract GWD's private key k_{gwd}. The adversary, after capturing the private key of GWD

can create a certificate for any other device SD_a, and the whole IoT device network will be compromised. Moreover, DACS-IoT does not provide device anonymity. An adversary $\mathcal{A}$ after physically capturing a device SD_z using power analysis (Kocher et al., 1999; Dolev and Yao, 1983) can extract all information $\{ID_{sdz}, k_{sdz}, K_{sdz}, cer_{sdz}, ID_{gwd}, K_{gwd}, h(.), E_\alpha(i,j), G\}$ stored in SD_z. Using the extracted information $\mathcal{A}$ can easily extract GWD's private key.

1. In DACS-IoT, using extracted K_{sdz} and ID_{gwd}, the attacker $\mathcal{A}$ can compute $X = h(ID_{gwd}||K_{sdz})$ and modular inverse $X^{-1} = h(ID_{gwd}||K_{sdz})^{-1}$. Now using X^{-1} and extracted private key k_{sdz} of SD_z, $\mathcal{A}$ can directly compute private key k_{gwd} of the gateway $k_{gwd} = (cer_{sdz} - k_{sdz}).X^{-1}$. Hence, the private key of the gateway is insecure under device physical capture attack.

2. In addition to the device's physical capture attack, the DACS-IoT does not provide user anonymity. In every access request or response message by a particular device, say SD_z, the certificate and the public key (cer_{sdz}, K_{sdz}) pair is sent in each message, which remains the same for all communicating sessions. Therefore, any adversary $\mathcal{A}$ just by listening to the channel can confidently trace out whether or not the one or both communicating parties in different sessions are the same. Therefore, DACS-IoT does not provide device anonymity.

Das et al. (2019) also proposed an access control scheme (LACKA-IoT). The scheme was proposed using ECC based certificates. LACKA-IoT was proved as insecure against device forgery and man in middle attacks (Chaudhry et al.,

2020b). In the same year, Zhou et al. (2019) also proposed another ECC and pairing based unlikable authentication scheme for IoT. Like LACKA-IoT, Zhou et al.'s scheme was proved as insecure against responding device impersonation attack (Chaudhry et al., 2020). A signature based and certificate less scheme for medical systems was proposed in (Peng et al., 2021). (Das et al., 2018) also proposed another scheme for cloud bases IoT systems. Hussain and Chaudhry (2019) commented on some critical pitfalls of the Das et al.'s scheme. Challah et al. also designed two separate authentication schemes (Challa et al., 2020, 2017). The former scheme was proposed for the cyber-physical system based smart grid environments, and the latter scheme was specifically designed for IoT based systems. However, both schemes were argued as incorrect (Chaudhry et al., 2020a). The scheme proposed in (Chaudhry et al., 2020a) provides authentication and is claimed to be secure against several threats. However, the framework suggested can provide authentication among two smart devices through a mediating agent and cannot accommodate direct D2D based security.

3. System Model

In this section, we introduce the network and adversarial models considered for proposed and related schemes.

3.1. Network Model

Fig. 1 depicts the undertaken network model of an IoMT environment, which contains the 1) in and outpatients (IOP) communicating smart devices, 2) the gateways, and 3) the underlying communication framework. The gateway nodes provide connectivity of different devices through a communication

framework. The sensors embedded in the bodies of in or outpatients may be configured to communicate with various wireless technologies and protocols, including Zigbee, Bluetooth, WIFI, and other technologies. Besides, suppose the corporal sensors in patients are configured as LoRA device technology. In that case, those sensors may directly communicate with LoRA client and MQTT broker protocols to communicate the critical data towards the cloud on a real-time basis. The MQTT protocols may provide low latency and quick communication compared to HTTP-based high payload communication protocols to promote real time feedback from the consultants. IoMT domain owns its gateway and connected devices through communication frameworks. After registering with the gateway (GWN), the IOP smart devices can securely establish a direct connection with their peers. This secure connection is established after both smart devices authenticate each other, resulting in sharing a session key among the IOP smart devices and ultimate sharing of medical/physiological data with intelligent medical information systems.

3.2. Adversarial Model

In this paper, we consider the common adversarial model as mentioned in (Dolev and Yao, 1983; Chaudhry, 2021; Chaudhry et al., 2021; Ali et al., 2021). Where according to capabilities of the adversary $\mathcal{A}$, the following realistic assumptions are made:

1. $\mathcal{A}$ fully controls the public communication channel. $\mathcal{A}$ can capture, replay, modify, insert a new message, and delete any message.

2. $\mathcal{A}$ after getting registered with GW can get his own smart card and can extract information stored in that smart card (Kocher et al., 1999;

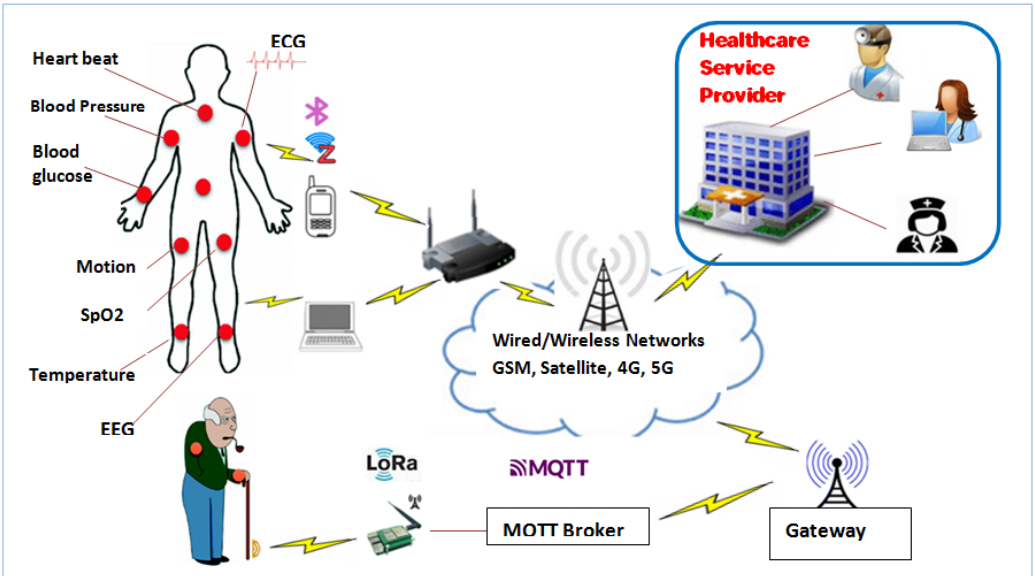

Figure 1: A typical IoMT scenario

Chaudhry et al., 2020).

3. $\mathcal{A}$ being insider can extract Verifier table from GW database.

4. D2DAC-IoMT: Proposed Scheme

This section explains the proposed device access control for IoMT based systems. The proposed scheme is designed carefully after analyzing the insecurities of related proposals. The proposed scheme, as illustrated in Fig. 2 is explained in the following subsections:

4.1. System Setup

For initialization and setting up the system, the gateway device (GWD) using elliptic curve based public key infrastructure (PKI) selects the system parameters. Following steps are performed by GWD during this phase:

Step SS1: GWD selects collision resistant hash function $h(.)$ as $h : \{0,1\}^* \rightarrow \{0,1\}^n$, which can either by SHA1 or SHA2 based on the sensitivity of the application.

Step SS2: Then an elliptic curve $E_\alpha(i,j)$ satisfying $4i^3 + 27j^2 \neq 0$ is selected along with an arbitrary base point $G \in E_\alpha(i,j)$.

Step SS3: GWD then selects random private key k_{gwd} and corresponding public key $K_{gwd} = k_{gwd}.G$.

Finally, GWD publicizes $\{h(.), E_\alpha(i,j), G, K_{gwd}\}$ and keeps k_{gwd} as confidential.

4.2. Device Enrollment

Before any access system, the communicating IoMT devices must enroll themselves and acquire the GWD created certificate and other related parameters. An IoMT device initiates this phase, and the following steps are completed:

Step DR1: For each device $SD_z : \{0 < z \leq n\}$, GWD assigns a unique identity ID_z and selects it's private key $k_{sdz} \in Z_p^*$, then GWD computes public $K_{sdz} = k_{sdz}.G$.

Step DR2: After assigning identity, private and public keys, GWD constitutes certificate for each sensing device: $cert_{sdz} = (A_{sdz}, b_{sdz})$, where $a_{sdz} = h(h(k_{gwd})||k_{sdz})$, $A_{sdz} = a_{sdz}G$, $d_{sdz} = h(ID_{gwd}||K_{gwd}||A_{sdz})$ and $b_{sdz} = a_{sdz} + k_{gwd}.d_{sdz}$. GWD finally, pre-loads $\{ID_{sdz}, k_{sdz}, K_{sdz}, \{cert_{sdz} = (A_{sdz}, b_{sdz})\}, ID_{gwd}, K_{gwd}, h(.), E_\alpha(i,j), G\}$.

4.3. Device Access Control

An IoMT device initiates this phase in the proposed scheme, say SD_x, when SD_x wants to access another IoMT device, say SD_y. The following steps are executed between SD_x and SD_y to complete this phase:

DC 1: $\boldsymbol{SD_x \rightarrow SD_y}$: $\boldsymbol{\{m_x\}}$

The SD_x randomly generates r_x and time-stamp T_{sdx} and computes $P_x = r_x.K_{sdy}$, $R_x = r_x.G$, $PA_{sdx} = A_{sdx} \oplus R_x$, $PK_{sdx} = K_{sdx} \oplus R_x$ and pseudo certificate $cerm_{sdx} = b_{sdx} + r_x$.The SD_x then generates $h_{sdx} = h(cerm_{sdx}||R_x||K_{sdx}||ID_{gwd}||T_{sdx})$ and signatures $sig_{sdx} = r_x + k_{sdx}.h_{sdx}$. Then SD_x sends $m_x = \{cerm_{sdx}, sig_{sdx}, T_{sdx}, PA_{sdx}, PK_{sdx}, P_x\}$ to SD_y.

DC 2: $\boldsymbol{SD_y \rightarrow SD_x}$: $\boldsymbol{\{m_y\}}$

Upon receiving $\{m_x\}$ from SD_x, the SD_y checks the time-stamp freshness of the received message. Aborts the message if fails to verify $T_{sdx} - T_{current} \leq \Delta T$. In success scenario, SD_y computes $R_x = P_x.k_{sdy}^{-1}$, $K_{sdx} = R_x \oplus PK_{sdx}$, $A_{sdx} = PA_{sdx} \oplus R_x$ and $j_{sdy} = h(ID_{gwd}||K_{gwd}||A_{sdx})$. The SD_y verifies the certificate $cerm_{sdx}.G \stackrel{?}{=} A_{sdx} + R_x + K_{gwd}.j_{sdy}$ and computes $h_{sdx} = h(cerm_{sdx}||R_x||K_{sdx}||ID_{gwd}||T_{sdx})$ and verifies the signatures $sig_{sdx}.G \stackrel{?}{=} R_x + h_{sdx}.K_{sdx}$. The session is aborted if verification of any one of the $cerm_{sdx}$ or sig_{sdx} fails. In success scenario, SD_y randomly generates r_y and time-stamp T_{sdy} and computes $P_y = r_y.K_{sdy}$, $R_y = r_y.G$, $PA_{sdy} = A_{sdy} \oplus R_y$ and pseudo certificate $cerm_{sdy} = b_{sdy} + r_y$. The SD_y further computes $h_{sdy} = h(cerm_{sdy}||R_y||K_{sdy}||ID_{gwd}||T_{sdy})$ and signatures $sig_{sdy} = r_y + k_{sdy}.h_{sdy}$. The SD_y further computes session key $SK_{xy} = h(R_x||R_y||cerm_{sdx}||cerm_{sdy}||ID_{gwd})$ along with key verifier

$SKV_{xy} = h(SK_{xy}||T_{sdy})$ and sends $m_y = \{cerm_{sdy}, sig_{sdy}, T_{sdy}, PA_{sdy}, PK_{sdy}, P_y\}$ to SD_x.

DC 3: Upon receiving m_y from SD_y, the SD_x checks the time-stamp freshness of the received message. Aborts the message if fails to verify $T_{sdy} - T_{current} \leq \Delta T$. In success scenario, SD_x computes $R_y = P_y.k_{sdx}^{-1}$, $A_{sdy} = PA_{sdy} \oplus R_y$, $j_{sdx} = h(ID_{gwd}||K_{gwd}||A_{sdy})$ and verifies the certificate $cerm_{sdy}.G \stackrel{?}{=} A_{sdy} + R_x + K_{gwd}.j_{sdy}$. The SD_y further computes $h_{sdy} = h(cerm_{sdy}||R_y||K_{sdy}||ID_{gwd}||T_{sdy})$ and verifies the signature $sig_{sdy}.G \stackrel{?}{=} R_y + h_{sdy}.K_{sdy}$. The session is aborted if verification of any one of the $cerm_{sdy}$ or sig_{sdy} fails. In success scenario, SD_x computes the session key $SK_{xy}^{'} = h(R_x||R_y||cerm_{sdx}||cerm_{sdy}||ID_{gwd})$. Finally, SD_x validates the verifier $SKV_{xy} \stackrel{?}{=} h(SK_{xy}^{'}||T_{sdy})$. Abort the session if validation fails. Otherwise, keeps SK_{xy} as legitimate shared session key with SD_y.

4.4. Dynamic Device Addition

In the proposed scheme, a new device can be added dynamically to an existing network. This procedure is very similar to the device enrollment phase, as described in subsection 4.2. For any new device, steps DR1 and DR2 in subsection 4.2 are executed between new device say SD_n and GWN. Finally, after getting its own certificate and pre-loaded values SD_n can be deployed in an existing network and can communicate securely with peers based on its own certificate.

SD_x	SD_y

Generate T_{sdx}, r_x and Compute:

$P_x = r_x.K_{sdy}$, $R_x = r_x.G$, $PA_{sdx} = A_{sdx} \oplus R_x$

$PK_{sdx} = K_{sdx} \oplus R_x$, $cerm_{sdx} = b_{sdx} + r_x$

$h_{sdx} = h(cerm_{sdx}||R_x||K_{sdx}||ID_{gwd}||T_{sdx})$

$sig_{sdx} = r_x + k_{sdx}.h_{sdx}$

$\xrightarrow{m_x=\{cerm_{sdx},sig_{sdx},T_{sdx},PA_{sdx},PK_{sdx},P_x\}}$

$T_{sdx} - T_{current} \leq \Delta T$, abort if not fresh

$R_x = P_x.k_{sdy}^{-1}$

$K_{sdx} = R_x \oplus PK_{sdx}$, $A_{sdx} = PA_{sdx} \oplus R_x$

$j_{sdy} = h(ID_{gwd}||K_{gwd}||A_{sdx})$

$cerm_{sdx}.G \stackrel{?}{=} A_{sdx} + R_x + K_{gwd}.j_{sdy}$

$h_{sdx} = h(cerm_{sdx}||R_x||K_{sdx}||ID_{gwd}||T_{sdx})$

$sig_{sdx}.G \stackrel{?}{=} R_x + h_{sdx}.K_{sdx}$

Generate T_{sdy}, r_y and Compute:

$P_y = r_y.K_{sdy}$ and $R_y = r_y.G$

$PA_{sdy} = A_{sdy} \oplus R_y$, $cerm_{sdy} = b_{sdy} + r_y$

$h_{sdy} = h(cerm_{sdy}||R_y||K_{sdy}||ID_{gwd}||T_{sdy})$

$sig_{sdy} = r_y + k_{sdy}.h_{sdy}$

$SK_{xy} = h(R_x||R_y||cerm_{sdx}||cerm_{sdy}||ID_{gwd})$

$SKV_{xy} = h(SK_{xy}||T_{sdy})$

$\xleftarrow{m_y=\{cerm_{sdy},sig_{sdy},T_{sdy},PA_{sdy},PK_{sdy},P_y,SKV_{xy}\}}$

$T_{sdy} - T_{current} \leq \Delta T$, abort if not fresh

$R_y = P_y.k_{sdx}^{-1}$,$A_{sdy} = PA_{sdy} \oplus R_y$

$j_{sdx} = h(ID_{gwd}||K_{gwd}||A_{sdy})$

$cerm_{sdy}.G \stackrel{?}{=} A_{sdy} + R_x + K_{gwd}.j_{sdy}$

$h_{sdy} = h(cerm_{sdy}||R_y||K_{sdy}||ID_{gwd}||T_{sdy})$

$sig_{sdy}.G \stackrel{?}{=} R_y + h_{sdy}.K_{sdy}$

$SK_{xy}^{'} = h(R_x||R_y||cerm_{sdx}||cerm_{sdy}||ID_{gwd})$

$SKV_{xy} \stackrel{?}{=} h(SK_{xy}^{'}||T_{sdy})$ Abort if not true

$SK_{xy}^{'} = h(R_x||R_y||cerm_{sdx}||cerm_{sdy}||ID_{gwd}) = SK_{xy}$

Figure 2: Proposed Device Access Control Procedure

5. Discussion on Functional Security

This section briefly discusses the functional security of the proposed D2DAC-IoMT scheme along with a comparison of the security features extended by proposed and related schemes under the realistic adversarial model, as mentioned in subsection 3.2 of proposed and related schemes. Investigation proves that the proposed scheme withstands all potential attacks and provides known security features. The functional security of the proposed scheme is explained in the following subsections:

1. Impersonation Attack: To impersonate as an IoMT device SD_x, the attacker $\mathcal{A}$ needs to generate valid message $m_x = \{cerm_{sdx}, sig_{sdx}, T_{sdx}, PA_{sdx}, PK_{sdx}, P_x\}$. Out of these parameters, $\mathcal{A}$ can generate current time stamp $T_{s\bar{dx}}$, random $r_{\bar{x}}$ and $P_{\bar{x}}$, then $\mathcal{A}$ tries to compute pseudo certificate $cerm_{sdx}$ and signatures sig_{sdx} based on original certificate cer_{sdx} and private key k_{sdx} along with ID_{sdx}, as none of these parameters are sent in plain text. Therefore, without knowing the private credentials, $\mathcal{A}$ will not succeed in generating valid tuple $\{cerm_{sdx}, sig_{sdx}, T_{sdx}, PA_{sdx}, PK_{sdx}, P_x\}$. Similarly, without knowing the secret credentials $\{cer_{sdy}, k_{sdy}, ID_{sdy}\}$, $\mathcal{A}$ will fail to compute response message. Therefore, proposed scheme provides resistance against initiator and responder impersonation attacks.

2. Replay Attack: Let an adversary $\mathcal{A}$ intercepts request m_x and/or response messages m_y and replays any message. The receiver, whether it is initiator SD_x or the responder SD_y will check the time stamp freshness. The old messages replayed later will not pass the freshness

test, and the receiver will simply ignore the message. Therefore, the proposed scheme withstands a replay attack.

3. Man in Middle Attack: To launch man in the middle attack, $\mathcal{A}$ has to generate a valid request or response message. $\mathcal{A}$ can modify an intercepted message and can modify some parameters. However, to generate the interconnected valid tuple, including the pseudo certificate, the signature, identity, and time stamp, $\mathcal{A}$ should know the private key and certificate of the IoMT device. Computing private keys and certificates by using only intercepted messages are infeasible. Therefore, the proposed scheme strongly resists man in middle attacks.

4. Malicious Device Deployment Attack: To deploy a malicious device in the communication system, $\mathcal{A}$ needs to install a valid certificate based on the public key of the malicious device and the private key of GWD. Moreover, identity is also hidden and is not sent over an insecure public channel. Hence, without knowing the private key of GWD, the adversary $\mathcal{A}$ cannot deploy any malicious device in an existing communication system.

5. Physical capture: The device specific public/private key pair (k_{sdz}, K_{sdz}) and certificate cer_{sdz} are unique for each device. Let the adversary $\mathcal{A}$ physical captures an IoMT device SD_z and extracts $\{ID_{sdz}, k_{sdz}, K_{sdz}, cer_{sdz}, ID_{gwd}, K_{gwd}, h(.), E_\alpha(i,j), G\}$ using power analysis, $\mathcal{A}$ can access all information related to SD_Z. However, $\mathcal{A}$ will have no benefit in finding the credentials of other IoMT devices or gateways because of the uniqueness of the parameters stored in the IoMT device. Even

if $\mathcal{A}$ captures 'n' devices, it will not affect the secure communication among other non-compromised devices. Therefore, the proposed scheme provides resilience against the physical capture of IoMT devices.

6. Ephemeral Secret Leakage Attack: The session key in the proposed scheme consists of the temporary session specific parameters (r_x, r_y) and permanent long term private key (k_{sdx}, k_{sdy}). These temporary and permanent parameters are contributed equally by both sides- the initiator and the responder. So, the leakage of temporary (r_x, r_y) or permanent (k_{sdx}, k_{sdy}) parameters alone is not sufficient to expose session key. $\mathcal{A}$ must know both ephemeral credentials (temporary and permanent). Therefore, the proposed scheme provides resistance against the ephemeral secret leakage attack.

7. Anonymity and Untraceability: In the proposed scheme, both the request and response messages contain all dynamic parameters based on a randomly selected number (r_x or r_y). Moreover, the signatures (from both sides) contain the current timestamp. The identity of IoMT devices is also concealed in one way hash functions. The devices' public key is also hidden in a dynamic parameter containing randomly generated session specific numbers. Therefore, the proposed scheme provides identity hiding and provides untraceabilty due to all dynamic parameters.

6. Formal Security Analysis

We scrutinize the formal security of the proposed scheme in this section. The cryptographic hash operation and elliptic curve decisional Diffie-Hellman problem (ECDDHP) is defined as follows.

Definition D1 (Cryptographic hash operation). A cryptographic one way hash operation for collision resistant $h : \{0,1\}^* \rightarrow \{0,1\}^n$ is used as a deterministic operation in which n bits output string of fixed length is generated by input length of dynamic length. For finding the collision of hash in $h(...)$, the advantage of adversary $(\mathcal{A})$ is supposed as $Adv_{(\mathcal{A})}^{HASH}(rt)$. Then, $Adv_{(\mathcal{A})}^{HASH}(rt) = Prob[(x_1, x_2) \in_R \mathcal{A} : x_1 \neq x_2, h(x_1) = h(x_2)]$, where $Prob[N]$ is the probability of an arbitrary event N and the input pair $(x_1, x_2) \in_R \mathcal{A}$ means that the strings of input x_1 and x_2 will be chosen by adversary randomly. We say "the collision resistance of $h(.)$ can be attacked by an $(\zeta.rt) - adversary\ \mathcal{A}$", such that rt is at the most run time of $\mathcal{A}$ and that $Adv_{(\mathcal{A})}^{HASH}(rt) \leq \zeta$.

Definition D2 (Elliptic curve decisional Diffie-Hellman problem (ECDDHP)).

Let $E_\alpha(i,j)$ be an elliptic curve over a prime $\alpha : y^2 = x^3 + ix + j\ (mod\ \alpha)$ and $G \in E_\alpha(i,j)$ be a point. The $ECDDHP$ is that with a quadruple $(G, x.G, y.G, z.G)$, computes if $z = xy$ or a uniform arbitrary value, where $x, y, z \in Z_\alpha^*$ and $Z_\alpha^* = \{1, 2, ..., \alpha - 1\}$.

If α is selected large then the $ECDDHP$ is infeasible for computation. So, α should be chosen 160-bits at least for the intractability of $ECDDHP$.

6.1. Random Oracle Model

We prove the security of the secret key of D2DAC-IoMT (Device Access Scheme with Secure Certificate) in this section. We use the Random Oracle Model (ROM) (Abdalla et al., 2005) in order to prove and analyze the security of our scheme (D2DAC-IoMT). Under ROM's model, an attacker $\mathcal{A}$ is associated with the $u_t h$ instance of an executing participant ($\mathcal{P}A^u$).In D2DAC-IoMT, the smart devices of IoMT SD_x or SD_y can be recognized as $\mathcal{P}A^u$. The $u_t h$ and $y_t h$ instances of SD_x or SD_y is supposed as $\mathcal{P}A^u_{SD_x}$ and $\mathcal{P}A^v_{SD_y}$, respectively. A real attack simulated by a few queries such as Reveal, Execute, and Test is discussed below. Furthermore, it is considered that one-way hash operation $h(.)$ can be designed as a random oracle, i.e., $Hash$, that can be accessed by all the users who participate, including $\mathcal{A}$. To explain the presented protocol's security model, a set of games have been designed between SD_x and an adversary $\mathcal{A}$. The attacker $\mathcal{A}$ can ask various queries in the defined set of games, while $\mathcal{SD}_y$ will act as follow:

- *Reveal Query* ($\mathcal{P}^u$): The attacker can reveal the current session key SK_{xy} between $\mathcal{P}^u$ and the second participant with the execution of this query.
- *Execute Query* ($\mathcal{P}^u_{SD_x}$,$\mathcal{P}^v_{SD_y}$): The information exchanged between SD_x and SD_y can be intercepted by attacker with the execution of this query.
- *Test Query* ($\mathcal{P}^u$): An adversary $\mathcal{A}$ will achieve the session key SK that is involved in $\mathcal{P}^v_{SD_y}$. Else, a randomly generated number with the same

length as the already generated number is selected by SD_x and send it to $\mathcal{A}$.

6.2. Provable Security

Furthermore, in Theorem TH1, we now prove that the presented scheme achieves session key security.

Theorem TH1: Suppose an attacker $\mathcal{A}$ runs in a polynomial time T against our scheme D2DAC-IoMT. If the range space of has the operation, number of queries for hash and advantage of $\mathcal{A}$ for breaking $ECDDHP$ are $|Hash|$, q_{hash} and $Adv_{\mathcal{A}}^{ECDDHP}(t)$, respectively. Then the advantage of attacker $\mathcal{A}$ for breaking the semantic security of $D2DAC-IoMT$ to extract the session key SK_{xy} exchanged between any two participants of IoMT smart devices SD_x and SD_y during the key agreement and access control phase can be supposed as $Adv_{\mathcal{A}}^{D2DAC-IoMT}(t) \leq \frac{q_{hash}^2}{|Hash|} + 2Adv_{\mathcal{A}}^{ECDDHP}(t)$.

Proof: We consider the following games i.e. GA_i, $i \in [0,2]$ for proving this theorem, where "an event wherein the arbitrary bit b can be guessed by $\mathcal{A}$ in GA_i correctly". The advantage of $\mathcal{A}$ for winning the game GA_i is denoted as $Adv_{\mathcal{A},G_i}^{D2DAC-IoMT} = Pr[Succ_{\mathcal{A}}^{G_i}]$. These games G_i, $i \in [0,2]$ are described as follows:

Game LG 0: The actual attack launched by $\mathcal{A}$ at our $D2DAC-IoMT$ is for the game LG 0, using the random oracle model (ROM). Since the bit b is chosen arbitrarily before starting the game LG 0, it pursues from the semantic security that

$$Adv_{\mathcal{A}}^{D2DAC-IoMT}(t) = |2.Adv_{\mathcal{A},LG0}^{D2DAC-IoMT} - 1| \tag{1}$$

Game LG 1: This game is designed as 'an intercepting attack', where $\mathcal{A}$ can forge all messages communicating over public channel $m_x = \{cerm_{sdx}, sig_{sdx}, T_{sdx}, PA_{sdx}, PK_{sdx}, P_x\}$ and $m_y = \{cerm_{sdy}, sig_{sdy}, T_{sdy}, PA_{sdy}, PK_{sdy}, P_y, SKV_{xy}\}$ during the key agreement and control access stage using the query of *Execute* which is described above. At the end of game, the queries of *Test* and *Reveal* can be executed by A in order to validate that the determined session key SK_{xy} between SD_x and SD_y is real or different key. SK_{xy} among SD_x and SD_y is determined as $SK_{xy} = h(R_x||R_y||cerm_{sdx}||cerm_{sdy}||ID_{gwd}) = SK'_{xy}$. The session key security SK_{xy} is relied on temporary secrets (r_x, r_y) and the long term private values (k_{sdx}, k_{gwd}) which are not known by $\mathcal{A}$. Thus, in this game LG 1, the winning probability of $\mathcal{A}$ will not be increased by only intercepting the transmitting messages m_x and m_y. The is described below, as the games LG 0 and LG 1 are identical.

$$Adv_{\mathcal{A},LG1}^{D2DAC-IoMT} = Adv_{\mathcal{A},LG0}^{D2DAC-IoMT} \tag{2}$$

Game LG 2: This game includes the execution of the Hash query. An active attack is designed for this game. In the message m_x, the values $r_x, ID_{sdx}, ID_{gwd} and k_{sdx}$ are secured by the one-way hash operation $h(.)$ of collision resistant (see definition D1). The values in the message m_y i.e. $r_y, ID_{sdy}, ID_{gwd}, and k_{sdy}$ are also protected by $h(.)$. After that, again from the forged $R_x = r_x.G$ and $R_y = r_y.G$, it is infeasible task for $\mathcal{A}$ to calculate r_x or r_y and hence, the session key SK_{xy} $(= SK'_{xy})$ as the $ECDDHP$ is intractable (see definition D2). Furthermore, due to collision resistant feature of hash operation $h(.)$, the derivation of $r_x, ID_{sdx}, ID_{gwd}, k_{sdx}, r_y, ID_{sdy}$ and k_{sdy} from the forged messages m_x and m_y is also infeasible. Since the information m_x

and m_y use identities, present timestamps, confidential credentials and all arbitrary numbers, we have no collision, if the query of *Hash* is launched by $\mathcal{A}$. As both of the games are almost identical except the involvement of the execution of Hash query in game LG 2, the $ECDDHP$ intractability will conclude the following result:

$$\begin{aligned} Adv_{\mathcal{A},LG1}^{D2DAC-IoMT} - Adv_{\mathcal{A},LG2}^{D2DAC-IoMT} \leq \\ \frac{q_{hash}^2}{|2Hash|} + Adv_{\mathcal{A}}^{ECDDHP}(t) \end{aligned} \tag{3}$$

As the $\mathcal{A}$ executes all the queries, and only b bit is left to guess for winning the game, once the query of *Test* and *Reveal* are simulated. So, we have

$$Adv_{\mathcal{A},LG2}^{D2DAC-IoMT} = \frac{1}{2} \tag{4}$$

The following result is given by equations (7)-(10):

$$\begin{aligned} \frac{1}{2}.Adv_{\mathcal{A}}^{D2DAC-IoMT}(t) &= |Adv_{\mathcal{A},LG0}^{D2DAC-IoMT} - \frac{1}{2}| \\ &= |Adv_{\mathcal{A},LG1}^{D2DAC-IoMT} - Adv_{\mathcal{A},LG2}^{D2DAC-IoMT}| \\ &\leq \frac{q_{hash}^2}{|2Hash|} + Adv_{\mathcal{A}}^{ECDDHP}(t) \end{aligned} \tag{5}$$

Finally, Eq.(11) is simplified by multiplication with the factor of 2, we conclude the desired result:

$$Adv_{\mathcal{A}}^{D2DAC-IoMT}(t) \leq \frac{q_{hash}^2}{|Hash|} + 2Adv_{\mathcal{A}}^{ECDDHP}(t). \tag{6}$$

7. Comparative Security and Performance Analysis

This section presents the security and performance comparisons between the proposed and related schemes (Zhou et al., 2007; Kim and Lee, 2009; Huang, 2009; Li et al., 2016; Luo et al., 2018; Malani et al., 2019; Li et al., 2019; Wu et al., 2021).

7.1. Security Comparisons

Table 2 depicts the security features comparison under the realistic adversarial model, as mentioned in subsection 3.2 of proposed and related schemes. Referring, Table 2, the proposed scheme provides all related security features, including secure certificate and anonymity, and the proposed scheme resists all known attacks. Contrary to the respective articles' claims, except for the proposed scheme, all other schemes are not providing anonymity and untraceability. In addition, schemes (Kim and Lee, 2009; Huang, 2009; Malani et al., 2019) could not resist malicious device deployment, schemes (Kim and Lee, 2009; Malani et al., 2019) are insecure against device impersonation, the scheme (Huang, 2009) is vulnerable to replay attacks. In contrast, the schemes (Kim and Lee, 2009; Li et al., 2016; Luo et al., 2018) do not provide direct communication between two sensing IoMT devices and need the intervention of GWD for creating a secure channel. The schemes (Li et al., 2016; Luo et al., 2018) lacks mutual authentication between the two communication IoMT devices. (Malani et al., 2019) scheme is also insecure against physical device capture attacks. The scheme of (Li et al., 2019) is insecure against man in middle and device impersonation attacks. Only proposed D2DAC-IoMT and (Wu et al., 2021) provide all security features. However, as shown in performance comparisons, D2DAC-IoMT out-performs Wu et al.'s scheme (Wu et al., 2021). Therefore, only the proposed scheme provides a good tradeoff between security and performance and can be considered a viable solution to secure the device to device communication in an IoMT environment.

Table 2: Security Comparisons

	Zhou et al. (2007)	Kim and Lee (2009)	Huang (2009)	Li et al. (2016)	Luo et al. (2018)	Malani et al. (2019)	Li et al. (2019)	Wu et al. (2021)	Our
RRA	✓	✓	✗	✓	✓	✓	✓	✓	✓
RMM	✓	✓	✓	✓	✓	✓	✗	✓	✓
PMA	✓	✓	✓	✗	✗	✓	✓	✓	✓
PKA	✓	✓	✓	✓	✓	✓	✓	✓	✓
RDI	✓	✗	✓	✓	✓	✗	✗	✓	✓
RMD	✓	✗	✗	✓	✓	✗	✓	✓	✓
RPC	✓	✓	✓	✓	✓	✗	✓	✓	✓
D2D	✓	✗	✓	✗	✗	✓	✓	✓	✓
PAU	✗	✗	✗	✗	✗	✗	✓	✓	✓

Note: RRA: Resists Replay Attack; RMM: Resists man in middle; PMA:Provides Mutual Authentication; PKA: Provides key Agreement; RDI:Resists Device Impersonation ; RMD: Resists Malicious Device Deployment ; RPC: Resists Physical Device Capture; D2D: Direct device to device communication; PAU: Provides Anonymity and Untraceability; ✓: Yes; ✗:No

Table 3: Computational Cost Analysis

	IoMT device/s	Total	RT(ms)
Zhou et al. (2007)	$6T_{epm} + 4T_{epa} + 2T_h$	$6T_{epm} + 4T_{epa} + 2T_h$	≈ 24.726
Kim and Lee (2009)	$4T_{epm} + 18T_h$	$4T_{epm} + 18T_h$	≈ 16.536
Huang (2009)	$4T_{epm} + 8T_h$	$4T_{epm} + 8T_h$	≈ 16.476
Li et al. (2016)	$2T_{pb} + 2T_h$	$6T_{pb} + 3T_{epm} + 1T_{ex} + 2T_h$	≈ 95.696
Luo et al. (2018)	$2T_{pb} + 2T_h$	$4T_{pb} + 3T_{epm} + 2T_{epa} + 2T_h$	≈ 62.449
Malani et al. (2019)	$12T_{epm} + 4T_{epa} + 15T_h$	$12T_{epm} + 4T_{epa} + 15T_h$	≈ 49.446
Li et al. (2019)	$8T_{ex} + 2T_{ecm} + 8T_h$	$8T_{ex} + 2T_{ecm} + 8T_h$	≈ 74.206
Wu et al. (2021)	$11T_{epm} + 2T_{epa} + 2T_{pb} + 8T_h$	$13T_{epm} + 3T_{epa} + 2T_{pb} + 8T_h$	≈ 70.301
Our	$14T_{epm} + 6T_{epa} + 10T_h$	$14T_{epm} + 6T_{epa} + 10T_h$	≈ 57.666

7.2. Computation Cost analysis

For accumulating the computation cost, the notations used are as follows: T_{epm} and T_{epa} represent the cost of point multiplication and point addition over $E_\alpha(i, j)$, respectively, while T_h, T_{pb}, T_{ex} and T_{en} depict the cost of hash function, bilinear pairing operation, modular exponentiation and symmetric encryption operations, respectively.

Using the authors' experiment conducted in (Hussain et al., 2021), on a Pi3-B+ with ARMv8-Cortex-A53 64bits-SoC and processing speed of 1.4 GHz and the Pi3-B+ encompasses 1 GB LPDDR2-SDRAM RAM, the time to complete different operations are as follows: $T_{bp} = 12.52$ ms, $T_{epm} = 4.107$ ms, $T_{epa} = 0.018$ ms, $T_{ex} = 8.243$ ms, and $T_h = 0.006$, where, Pi3-B+ acts both as an IoMT device and the mediating party used in some of the schemes (Li et al., 2016; Luo et al., 2018).

Computation cost of the proposed D2DAC-IoMT along with proposed schemes in (Zhou et al., 2007; Kim and Lee, 2009; Huang, 2009; Li et al., 2016; Luo et al., 2018; Malani et al., 2019; Li et al., 2019; Wu et al., 2021) are depicted in Table 3. While providing all security features and resistance to all known attacks, the proposed scheme incurs some extra computation cost as compared with some of the related schemes except (Li et al., 2016; Luo et al., 2018; Li et al., 2019; Wu et al., 2021). The proposed scheme completes the device access control phase with a key agreement in approximately 57.666 ms. The Fig. 3 also summarizes the computation cost comparisons.

7.3. Communication Cost

Table 4 shows the communication cost comparison of proposed and related schemes (Zhou et al., 2007; Kim and Lee, 2009; Huang, 2009; Li et al., 2016;

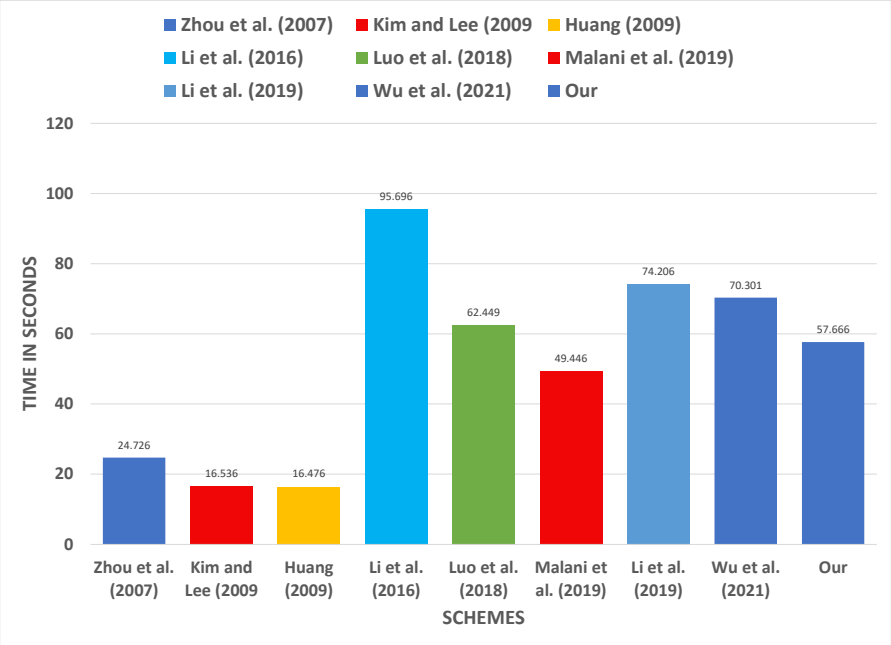

Figure 3: Computation Cost Comparisons

Luo et al., 2018; Malani et al., 2019; Li et al., 2019; Wu et al., 2021) and for this purpose, $SHA-1$ with 160 bit output is selected. For simplicity the size of identity is also considered as 160 bit, the size of random number is taken as 160 bit long; whereas, the timestamps are of 32 bit length and the size of a point over $E_\alpha(i,j)$ is fixed at 320 bit. The proposed scheme accomplishes the the device access control phase in two messages: 1) The request message $m_x = \{cerm_{sdx}, sig_{sdx}, T_{sdx}, PA_{sdx}, PK_{sdx}, P_x\}$ and 2) The response message $m_y = \{cerm_{sdy}, sig_{sdy}, T_{sdy}, PA_{sdy}, PK_{sdy}, P_y, SKV_{xy}\}$. The communication cost of m_x is $\{160+160+32+320+320+320\} = 1312$ bits; whereas, m_y

Table 4: Communication Cost Analysis

Trans.↓	Zhou et al. (2007)	Kim and Lee (2009)	Huang (2009)	Li et al. (2016)	Luo et al. (2018)	Malani et al. (2019)	Li et al. (2019)	Wu et al. (2021)	Our
Bits	4608	1920	1920	3488	3040	2144	2752	2944	2464
Msgs.	5	4	4	2	2	2	2	2	2

takes $\{160+160+32+320+320+320+160\} = 1472$ bits over communication channel. Hence, the total communication cost of the proposed scheme is 2784 bits. Although, the proposed D2DAC-IoMT has more communication cost as compared with some of the related schemes (Malani et al., 2019; Huang, 2009; Kim and Lee, 2009). However, this extra communication cost ensures anonymity and untraceability in the proposed scheme. Therefore, the proposed scheme is a viable solution in access control scenarios. The Fig. 4 also summarizes communication cost comparisons.

8. Conclusion

A novel certificate-based access control scheme for IoMT systems (D2DAC-IoMT) is proposed using elliptic curve cryptography (ECC). The proposed D2DAC-IoMT is designed carefully to mitigate IoMT specific security threats, including malicious device deployment, the man in the middle, stolen verifier, and device physical capture attacks, etc. The ECC based device specific certificate is based on GWN's private key and related secret parameters, which protects the security of all other non-compromised devices even if one or more devices are compromised. The security of the D2DAC-IoMT scheme is tested under the formal model. Moreover, the security provision of the D2DAC-IoMT scheme is explained through a discussion on functional security. The proposed D2DAC-IoMT scheme, while incurring some extra computation

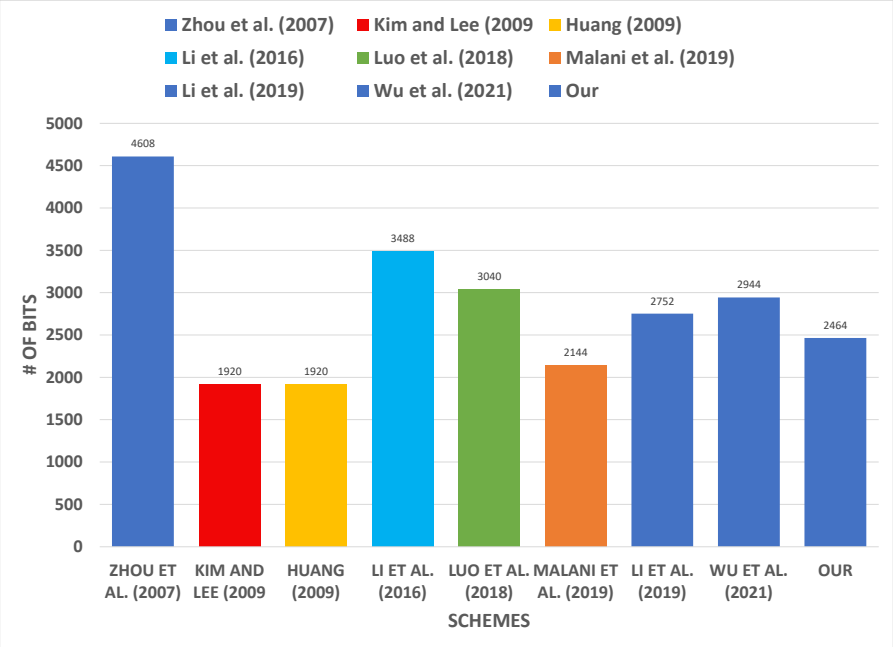

Figure 4: Communication Cost Comparisons

and communication costs, resists all known attacks.

References

M. Abdalla, P. Fouque, and D. Pointcheval. Password-based authenticated key exchange in the three-party setting. In *in Public Key Cryptographyv(PKC-05), Lecture Notes in Computer Science*, pages 65–84. Springer, Berlin, 2005. vol. 3386.

Z. Ali, S. A. Chaudhry, K. Mahmood, S. Garg, Z. Lv, and Y. B. Zikria. A clogging resistant secure authentication scheme for fog

computing services. *Computer Networks*, 185:107731, 2021. ISSN 1389-1286. doi: https://doi.org/10.1016/j.comnet.2020.107731. URL https://www.sciencedirect.com/science/article/pii/S1389128620313219.

R. Arul, G. Raja, A. O. Almagrabi, M. S. Alkatheiri, S. H. Chauhdary, and A. K. Bashir. A quantum-safe key hierarchy and dynamic security association for lte/sae in 5g scenario. *IEEE Transactions on Industrial Informatics*, 16(1):681–690, 2019.

K. A. Bhavsar, J. Singla, Y. D. Al-Otaibi, O.-Y. Song, Y. B. Zikria, and A. K. Bashir. Medical diagnosis using machine learning: A statistical review. *CMC-COMPUTERS MATERIALS & CONTINUA*, 67(1):107–125, 2021.

A. Braeken, P. Porambage, M. Stojmenovic, and L. Lambrinos. edaaas: Efficient distributed anonymous authentication and access in smart homes. *International Journal of Distributed Sensor Networks*, 12(12):1–11, 2016.

S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E.-J. Yoon, and K.-Y. Yoo. Secure signature-based authenticated key establishment scheme for future iot applications. *IEEE Access*, 5:3028–3043, 2017.

S. Challa, A. K. Das, P. Gope, N. Kumar, F. Wu, and A. V. Vasilakos. Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems. *Future Generation Computer Systems*, 108:1267–1286, 2020.

S. Chatterjee, A. K. Das, and J. K. Sing. An enhanced access control scheme in wireless sensor networks. *Ad Hoc & Sensor Wireless Networks*, 21(1-2): 121–149, 2014.

S. A. Chaudhry. Correcting "palk: Password-based anonymous lightweight key agreement framework for smart grid". *International Journal of Electrical Power & Energy Systems*, 125:106529, 2021. ISSN 0142-0615. doi: 10.1016/j.ijepes.2020.106529.

S. A. Chaudhry, M. S. Farash, N. Kumar, and M. H. Alsharif. Pflua-diot: A pairing free lightweight and unlinkable user access control scheme for distributed iot environments. *IEEE Systems Journal*, pages 1–8, 2020. doi: 10.1109/JSYST.2020.3036425.

S. A. Chaudhry, T. Shon, F. Al-Turjman, and M. H. Alsharif. Correcting design flaws: An improved and cloud assisted key agreement scheme in cyber physical systems. *Computer Communications*, 153:527–537, 2020a.

S. A. Chaudhry, K. Yahya, F. Al-Turjman, and M.-H. Yang. A secure and reliable device access control scheme for iot based sensor cloud systems. *IEEE Access*, 8:139244–139254, 2020b.

S. A. Chaudhry, A. Irshad, K. Yahya, N. Kumar, M. Alazab, and Y. B. Zikria. Rotating behind privacy: An improved lightweight authentication scheme for cloud-based iot environment. *ACM Trans. Internet Technol.*, 21(3), June 2021. ISSN 1533-5399. doi: 10.1145/3425707.

A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. Rodrigues. Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment. *IEEE Internet of Things Journal*, 5(6):4900–4913, 2018.

A. K. Das, M. Wazid, A. R. Yannam, J. J. Rodrigues, and Y. Park. Provably secure ecc-based device access control and key agreement protocol for iot environment. *IEEE Access*, 7:55382–55397, 2019.

B. Deebak. Lightweight authentication and key management in mobile-sink for smart iot-assisted systems. *Sustainable Cities and Society*, 63:102416, 2020.

B. D. Deebak and F. Al-Turjman. Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things. *IEEE Journal on Selected Areas in Communications*, 39(2):346–360, 2021. doi: 10.1109/JSAC.2020.3020599.

D. Dolev and A. C. Yao. On the security of public key protocols,. *Information Theory, IEEE Transactions on, vol. 29, no. 2*, 29(2):198–208, 1983.

D. Evans. *The Internet of Things: How the next evolution of the Internet is changing everything*. Cisco, San Jose, CA, USA, White Paper, 2011.

H. F. Huang. A novel access control protocol for secure sensor networks. *Computer Standards & Interfaces*, 31:272–276, 2009.

H. F. Huang. A new design of access control in wireless sensor networks, international journal of distributed sensor networks. *vol.*, 2146:7, 2011. doi: 10.1155/2011/412146. article ID 412146.

H. F. Huang and A. K. C. Liu. New dynamic access control in wireless sensor networks. In T. Yilan, editor, *IEEE Asia-Pacific Services Computing Conference (APSCC-08)*, pages 901–906, 2008.

S. Hussain and S. A. Chaudhry. Comments on "biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment". *IEEE Internet of Things Journal*, 6(6):10936–10940, 2019.

S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan, and N. Kumar. Amassing the security: An ecc-based authentication scheme for internet of drones. *IEEE Systems Journal*, pages 1–8, 2021. doi: 10.1109/JSYST.2021.3057047.

M. A. Khan and K. Salah. 'iot security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82:395–411, 2018. doi: 10.1016/j.future.2017.11.022.

H. S. Kim and S. W. Lee. Enhanced novel access control protocol over wireless sensor networks, ieee transactions on consumer electronics, vol. 55, no. 2. *p*, pages 492–498, 2009.

P. Kocher, J. Jaffe, and B. Jun. *Differential power analysis.* in Advances in Cryptology CRYPTO 99. Springer, 1999. pp. 388-397.

J. Laufs, H. Borrion, and B. Bradford. Security and the smart city: A systematic review. *Sustainable cities and society*, 55:102023, 2020.

F. Li, Y. Han, and C. Jin. Practical access control for sensor networks in the context of the internet of things. *Computer Communications*, 89-90: 154–164, 2016.

X. Li, F. Wu, S. Kumari, L. Xu, A. K. Sangaiah, and K.-K. R. Choo. A

provably secure and anonymous message authentication scheme for smart grids. *Journal of Parallel and Distributed Computing*, 132:242–249, 2019.

M. Luo, Y. Luo, Y. Wan, and Z. Wang. Secure and efficient access control scheme for wireless sensor networks in the cross-domain context of the iot. *Security and Communication Networks*, pages 1–10, 2018. URL `https://doi.org/10.1155/2018/6140978`.

S. Malani, J. Srinivas, A. K. Das, K. Srinathan, and M. Jo. Certificate-based anonymous device access control scheme for iot environment. *IEEE Internet of Things Journal*, 6(6):9762–9773, 2019.

J. Ni, K. Zhang, X. Lin, and X. S. Shen. Securing fog computing for internet of things applications: Challenges and solutions, ieee communications surveys tutorials, vol. 20, no. 1. *p*, 601-628, 2018.

K. Park, S. Noh, H. Lee, A. K. Das, M. Kim, Y. Park, and M. Wazid. Laks-nvt: Provably secure and lightweight authentication and key agreement scheme without verification table in medical internet of things. *IEEE Access*, 8: 119387–119404, 2020. doi: 10.1109/ACCESS.2020.3005592.

C. Peng, M. Luo, L. Li, K.-K. R. Choo, and D. He. Efficient certificateless online/offline signature scheme for wireless body area networks. *IEEE Internet of Things Journal*, pages 1–1, 2021. doi: 10.1109/JIOT.2021.3068364.

A. G. Reddy, D. Suresh, K. Phaneendra, J. S. Shin, and V. Odelu. Provably secure pseudo-identity based device authentication for smart cities environment. *Sustainable cities and society*, 41:878–885, 2018.

C. P. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4(3):161–174, 1991.

M. Shafiq, Z. Tian, A. K. Bashir, A. Jolfaei, and X. Yu. Data mining and machine learning methods for sustainable smart cities traffic classification: A survey. *Sustainable Cities and Society*, 60:102177, 2020.

T.-Y. Wu, Y.-Q. Lee, C.-M. Chen, Y. Tian, and N. A. Al-Nabhan. An enhanced pairing-based authentication scheme for smart grid communications. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–13, 2021.

Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao. A survey on security and privacy issues in internet-of-things. *in IEEE Internet of Things Journal*, 4 (5):1250–1258, October 2017. doi: 10.1109/JIOT.2017.2694844.

P. Zeng, K.-K. Choo, and D.-Z. Sun. On the security of an enhanced novel access control protocol for wireless sensor networks. *IEEE Transactions on Consumer Electronics*, 56(2):566–569, 2010.

Y. Zhou, Y. Zhang, and Y. Fang. Access control in wireless sensor networks„ vol. *Ad Hoc Networks*, 5:3–13, 2007.

Y. Zhou, T. Liu, F. Tang, and M. Tinashe. An unlinkable authentication scheme for distributed iot application. *IEEE Access*, 7:14757–14766, 2019.