Zero Knowledge Proofs Based Authenticated Key Agreement Protocol for Sustainable Healthcare

Gurjot Singh Gaba, Mustapha Hedabou, Pardeep Kumar, An Braeken, Madhusanka Liyanage, Mamoun Alazab

Abstract

Upgradation of technologies for sustainable smart cities has led to rapid growth in Internet of Things (IoT) applications, including e-healthcare services wherein smart devices collect patient data and deliver it remotely to the servers in real-time. Despite its enormous benefits, IoT in healthcare has not received much attention primarily due to the risk of unauthorized access to confidential medical information enabled by the vulnerable wireless channel for communication. Besides, tiny IoT devices have limited computing power and storage capabilities that prevent administrators from using complex and resource-hungry security protocols. The cyber attacks on the Internet of Healthcare applications (IoHA) could result in fatalities, decreased revenue, and reputation loss, hence endangering sustainability. The existing security protocols are unsuitable due to the cost complexities that necessitate developing new security protocols for resource-constrained and heterogeneous IoT networks. We introduce a confidentiality and anonymity-preserving scheme for critical infrastructures of IoT to conquer cyber threats for sustainable healthcare. This paper proposes Zero-Knowledge Proofs (ZKP) based Authenticated Key Agreement (AKA) protocol for IoHA. ZKP-AKA uses zero-knowledge proofs, physically unclonable function, biometrics, symmetric cryptography, message digest, etc., for accomplishing the protocol's objective at minimal computation, storage, and communication expenses. ZKP-AKA retains data integrity, confidentiality, anonymity, and safety from significant cyber threats.

Index Terms

Sustainable healthcare, Internet of Things, Mutual Authentication, Physically Unclonable Function, Security, Zero Knowledge Proofs.

I. Introduction

The growth of IoT in the recent years has enabled the task force of healthcare organizations to perform their work with better optimization and precision [1]. IoT has enabled the healthcare institutions to share the pathology lab reports and doctor's prescription with the user in phygital form [2]. Digitalization is imperative for sustainable cities as it promotes social and economic intercommunication and contributes to environmentally safe urban ecosystems and civilizations [3]. The digital transformation has enabled the medical staff and patients to exchange the information to far distant places without delay, thus ensuring sustainable healthcare [4]. Fig. 1 illustrates the infrastructural changes (H1.0 to H4.0) that took place over

Gurjot Singh Gaba and Mustapha Hedabou are with the School of Computer Science, Mohammed VI Polytechnic University, Ben Geurir 43150, Morocco, *email*: gurjot.singh@um6p.ma, mustapha.hedabou@um6p.ma

Pardeep Kumar is with the Department of Computer Science, Swansea University SA1 8EN, U.K., e-mail: pardeep.kumar@swansea.ac.uk

An Braeken is with the Faculty of Engineering, Vrije Universiteit, Brussel 1050, Belgium, e-mail: abraeken@gmail.com

Madhusanka Liyanage is with the School of Computer Science, University College Dublin, Ireland and Centre for Wireless Communications, University of Oulu, Finland, email: madhusanka@ucd.ie

Mamoun Alazab is with the College of Engineering, IT and Environment, Charles Darwin University, Casuarina, NT, Australia, e-mail: alazab.m@ieee.org

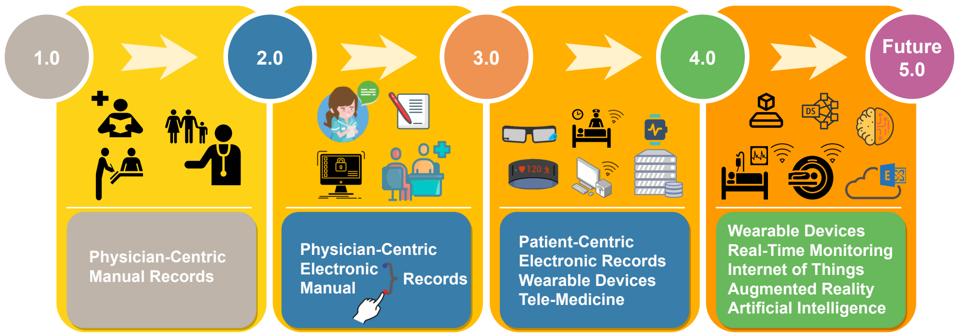

1.0
2.0
3.0
4.0
Future 5.0
Physician-Centric Manual Records
Physician-Centric
Electronic
Manual
Records
Patient-Centric Electronic Records Wearable Devices Tele-Medicine
Wearable Devices Real-Time Monitoring Internet of Things Augmented Reality Artificial Intelligence

Figure 1: Healthcare Evolution: A journey from *Past* (H1.0) to *Present* (H4.0)

time in healthcare institutions [5]. In Healthcare 1.0, the doctors maintained the records manually, which got replaced with electronic records in Healthcare 2.0. On the contrary, Healthcare 3.0 was patient-centric, wherein wearable devices were used to collect patient's health information, accessible remotely through the internet [6].

Healthcare 4.0 uses several wearable devices to monitor and analyze heart rate, blood pressure, breath analyzer, electrocardiograph etc., through a smartwatch, health tracker, pacemaker and so on. Healthcare 3.0 had storage problems which have been resolved in Healthcare 4.0. The Healthcare 4.0 infrastructure stores the data in cloud servers which is accessible to legitimate stakeholders only. However, keeping the integrity and privacy of the data intact is still troublesome in Healthcare 4.0. [7].

Securing IoT is challenging because of the involvement of heterogeneous resource-constrained nodes [8]. Limited resources available with IoT nodes do not permit the developer and administrator to deploy complex security protocols. In spite of the best efforts to develop adequate measures, the number of cyber attacks on healthcare institutions has risen exponentially. The cyber attack on University of Vermont Health Network in 2020 left the affected persons stranded for more than 40 days. More than 5000 computers were not functional due to which almost 300 employees were jobless for many days. Experts believed that the cyber attack led to a loss of 1.5 million per day in revenue and extra expenses. Universal Health Services, established in King of Prussia, also suffered a massive malware attack in 2020 that lasted for eight days [9].

Sustainable and smart healthcare institutions equip the stakeholders with state-of-the-art technologies required to diagnose, operate and communicate as shown in Fig. 2. The technology infusion is fruitful but dangerous as intelligent devices share information through the wireless networks which are prone to different attacks like man-in-the-middle (MITM), replay, impersonation and so on. These attacks may result in data exploitation, organization's reputation loss and loss of human lives. The prevention from

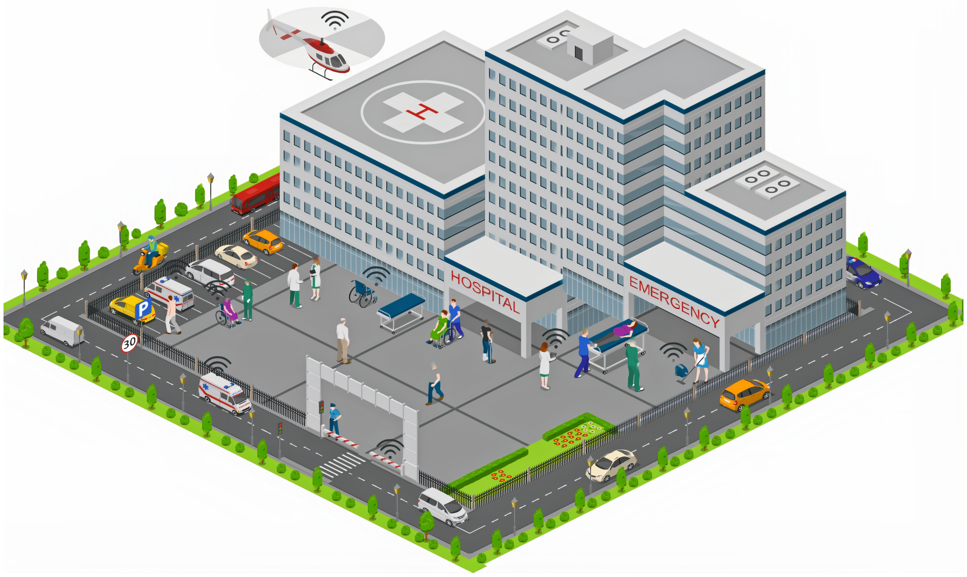


Figure 2: IoT-enabled Smart Healthcare Institution

these cyber threats is challenging in a resource-constrained environment [10]. A good solution to restrict breaching and prevent loss can be an application-oriented lightweight IoT security protocol that provides secure mutual authentication and safe key exchange between any two legitimate entities [11].

The remaining paper has been put together in this sequence: Section II has the literature review, and the preliminaries have been put in section III. Section IV demonstrates the proposed scheme, whereas section V contains the security analysis. The performance and comparative analysis are discussed in section VI. Finally, section VII provides a gist of the paper and throws some light on the future scope.

II. Literature Review

In-spite of a good in-depth research, the existing schemes lack in ensuring sustainability at healthcare institutions. This section provides an overview of existing authentication and key exchange schemes [12]–[33]. Deebak [12] proposed a mutual authentication scheme for heterogeneous Wireless Sensor Networks (WSN), but it is proven insecure in [13]. Chen et al. [14] extended the security to Deebak scheme [12], but Xu et al. [15] found the Chen's scheme susceptible to replay and impersonation attacks. The method used by Wang [16] to develop a mutual authentication scheme was based on the principle of the elliptic curve cryptography (ECC). Besides user anonymity, Wang [16] claimed the robustness of its approach against password guessing and verifier attacks. However, Odelu et al. [17] discovered that Wang's [16] method did not maintain user anonymity and was not safe from password attacks.

A lightweight mechanism for ad hoc WSN was brought in by Turkanovic et al. [18]. The scheme was focused on the user authentication and key agreement between a user and the sensor node, however

Farash et al. [19] found the scheme insecure against impersonation attacks. Chang et al. [21] presented two proposals to overcome the security issues of Turkanovic et al. scheme [18]. During analysis, the former protocol developed by Chang et al. [21] was found insecure, whereas the latter was expensive in terms of resources. Besides, Gope et al. [22] found the scheme [21] vulnerable to traceability.

A biometric and smart card-based approach for IoT-specific environment was introduced in [23]. It did not gain much attention due to the use of fuzzy extractor and vulnerability to the well-known attacks. A scheme with authentication based on user identity, biometric and password was proposed by Li et al. [24]. It was not only resource expensive, but the authors did not investigate the robustness of their protocol under compromised conditions. To lessen the computation expense, Esfahani et al. [25] came up with a very light protocol that attains the goal of authentication with the use of just the message digest and XOR operations. The key agreement was attained by authentication made by biometric and Elliptic Curve Cryptography (ECC) and simulated in the Network Simulator (NS3) [27]. Lack of message freshness and privacy motivated Paliwal [26] to devise a scheme that would overcome the issues of [27]. However, extensive use of cryptographic primitives and the exchange of enormous messages made the Paliwal scheme bulky and unfit for resource-constrained IoT networks.

Islam et al. [28] improved upon the scheme put forward by Lin et al. [29] that had a password-based authentication mechanism based on ECC. But H. Debitao along with fellow researchers [30] later discovered that the scheme was not safe from password guessing attacks, stolen verifier attacks as well as the insider attacks. Amin et al. [31] put forth a protocol that provided user privacy protection and lightweight computation for Telecare Medicine Information System (TMIS). Lung et al. [32] discovered that Amin's scheme did not safeguard the sensitive medical data. Zhang et al. [33] was successful in making a protocol based on dynamic authentication and three-factor key agreement that protected the e-health systems with respect to privacy of data. However, Lung and his team [32] found that Zhang's scheme [33] was not checking the authenticity of the user before sending the request to the server. As the scheme was built upon single-server architecture, it was easy for the attacker to trigger a DoS attack by sending repetitive login intercepted messages.

A. Problem Statement and Research Motivation

The advent of wearable IoT devices has revolutionized healthcare to a great extent. It saves time and money by connecting the patient to the physician remotely and reduces the burden on the healthcare institutions. The extensive range of benefits offered by IoMT triggered its growth at the compound annual growth rate of 26.2%. Although it has benefits, it could endanger the lives of the patients and healthcare professionals, as per cyber experts. The cyber hackers could breach the digitally stored medical records to reveal them publically, which can be embarrassing, or they might sell them on the dark web. The adversary can also modify the medical reports, leading to patients' inaccurate treatment, resulting in adverse health conditions. Apart from harming the confidentiality and integrity of healthcare systems, the attacker can also impact the availability of internet-enabled medical applications. Untimely and non-availability of these applications could result in fatalities. Additionally, a lack of reliable accountability and authentication mechanisms builds fear in potential stakeholders' minds.

The researchers provided various cyber security solutions to address these problems. These schemes have used fog, edge, cloud, blockchain, password, biometrics, hash, and elliptic curve cryptography, based frameworks. However, most of these schemes are susceptible to cyber-attacks and have high computational and communication costs. Despite the availability of existing schemes, the healthcare sector suffered greatly in 2021 as millions of records were breached, the ransom was paid, and unauthorized users obtained access [34]. This puts great responsibility on the security protocol developer and the network administrator to design secure and robust protocols that are more immune to cyber attacks [35]. The mutual authentication and secure key exchange procedures must be strong enough to provide prolonged and sustainable security to IoT networks from malicious threats.

B. Our Contribution

- We have formulated a mutual authentication and key agreement protocol to protect IoT healthcare networks from unauthorized abuses.
- We have implemented the protocol using Zero-Knowledge Proof (ZKP) and Physically Unclonable Function (PUF) to safeguard confidentiality and prevent physical attacks.
- We have investigated the protocol's robustness against diverse harmful cyber-attacks through formal analysis using AVISPA and informal analysis using logical rules.
- We have analyzed the performance of ZKP-AKA and compared it with existing security protocols.

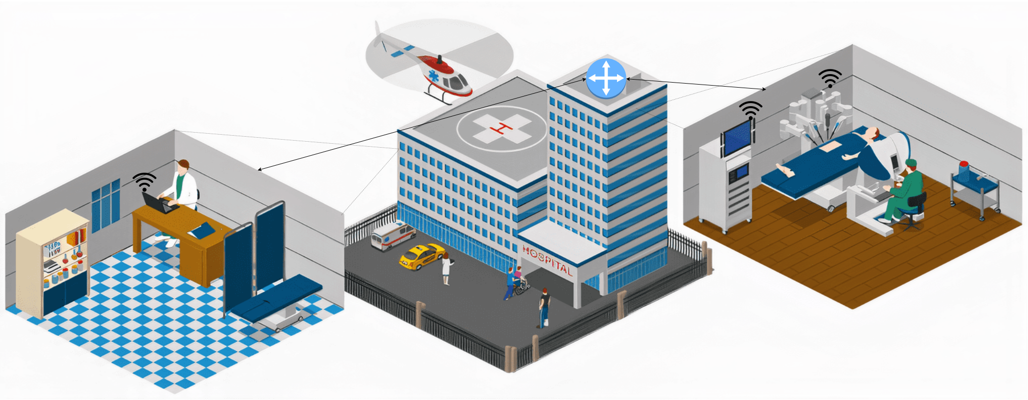


Figure 3: Security protocol deployment environment

III. Preliminaries

A. System Model

Fig. 3 illustrates the IoT-enabled healthcare infrastructure wherein the gateway acts as an interface to the user for receiving real-time information from the IoT sensor node.

1) User: A user can be a doctor or any authorized medical personnel who wishes to monitor and access real-time information of the patient from near or remote location. The doctor's device is assumed to be resource-constrained due to low storage, finite power, and less capability for computation.

2) Gateway: Gateway is the resource-abundant network device that acts as an interface between a user device and the IoT sensor node. It also helps in mutual authentication and secret key establishment.

3) IoT Sensor Node: The IoT node is wirelessly connected to the user's device through the gateway. This enables the user to keep an eye on operations and from anywhere as it receives data from various medical equipment used in healthcare [36]. Unlike gateway, the IoT sensor nodes are resource-constrained.

B. Adversary Model

Our scheme has considered the Dolev-Yao (DY) threat model [37] for determining its robustness. According to the DY model, the adversary is able to read, overhear, and edit the information shared between different entities. The intruder can intercept the messages to extract user identity, secret key, precious data, etc. which may compromise user's private data, causing severe physical or mental harm. These impacts also put human lives at risk. An intruder can capture the message and use it to launch replay to get unauthorized access to the healthcare system. The intruder can also modify timestamps to gain illegal access to the system and inject malware to disrupt critical healthcare operations.

C. Zero Knowledge Proof (ZKP)

Zero-Knowledge Proof is the one that helps the prover to convince the verifier about its legitimacy without disclosing any secret information and it was first introduced in 1985 by Goldwasser et al. [38], [39]. Fundamentally, the prover demonstrates the secret knowledge to the verifier through the number of interactive rounds, and no sensitive information is shared during the entire process.

ZKP should attain these three properties to work efficiently:

1) *Completeness*: Genuine statement of the prover should convince the honest verifier.
2) *Soundness*: False statement by a dishonest prover is not adequate to convince the honest verifier, except with a minimal probability.
3) *Zero-knowledge*: The verifier does not get to know anything else except the fact that the statement is true.

D. Physical Unclonable Function (PUF)

Physical Unclonable Function (PUF) is a process to provide hardware security with little computation complexities and it is favorable for tiny resource-constrained devices. The main reason for that is the easy integration process of PUF and the fact that they cannot be duplicated as they are dependent upon the device's physical attributes during manufacturing. PUF is also known as the physical one-way function and physical random function (PRF) [40], [41]. PUF embedded devices generate a unique response for every different input challenge. Due to its unique characteristics, PUF becomes the ideal solution for verifying the authenticity of network entities in resource-constrained networks. The response of PUF is only determined by its unique complex physical function integrated within every device. More commonly, Challenge-Response Pair (CRP) is referred to as PUF, where the set of CRP is treated as a biometric of its integrated device.

E. Security and other goals

- *Data privacy*: Healthcare institutions store precious information like patient records, hospital records, medical records etc. Therefore, data privacy is very crucial to keep the data safe from malignant minds.
- *Defense against various attacks*: The user device and the IoT sensor node can succumb to various attacks such as MITM, replay, etc., disrupting the network functioning [42]. Security protocols must protect the network from such attacks.

- *Mutual authentication and key agreement*: The IoT networks use an unguided medium to exchange information. The attackers also try to join the network to access the critical data. The security protocols must ensure the verification of the devices before permitting them to join the network [43]. The protocols must enable the legitimate parties to exchange security keys to secure the information to be exchanged between them.
- *Message integrity and freshness*: Adversaries are always on the lookout for an opportunity to hinder the smooth operations of networks. The attacker can replay the messages to get unauthorized access and modify the messages to execute malicious actions. Thus, the security protocols must preserve the integrity of information and verify the message freshness before processing the requests [44].
- *Lightweightness*: The user device and IoT sensor nodes are resource-constrained. The security schemes must be lightweight in computation and communication to ensure prolonged connectivity and access to the network.
- *Availability*: Healthcare professionals require round-the-clock connectivity with the IoT-enabled patient diagnosis and treatment devices. Non-accessibility of these devices could result in catastrophe, including fatalities. Therefore, the network administrator should ensure the timely availability of systems and resources to all the authorized users.

IV. Proposed Scheme

The user and the IoT sensor node are first registered at the gateway. Post-registration, the user device can communicate securely with the IoT sensor node via gateway but after proving the legitimacy. The entire process of registration and authenticated key agreement is disclosed in this section. Table I lists out the notations used through the entire paper.

A. Assumptions

The following assumptions have been made while implementing the protocol:

- User device and IoT sensor node have limited computational capability, battery reserve, and storage space (resource-constrained).
- Gateway is a tamper-less trusted entity with no resource restrictions.
- The network devices can execute cryptography operations.
- PUF is attached to the microcontroller of the user device and IoT sensor node. Any attempt to tamper with the PUF of the user device and IoT sensor node will render them useless [22].

Table I: Notations and Descriptions

Notation	Description	Notation	Description
G, H, F	Points on elliptic curve	Z, W, τ_1, τ_2, X, Q	Variables
r_1, r_2, r_3, k_1, k_2	Variables	U_{ID}, R_q	User identity, Registration request
B_1, B_2	Components of biometric	SK_U, SK_{SN}	Temporary secret key for user and IoT sensor node
E, D, h	Encryption, Decryption, and Hash	{||}, {-}, {+}	Concatenation, Subtraction, Addition
β, γ	Temporary identity of user and IoT sensor node	N_1 - N_7, K, S, I	Nonce(s), Key, Salt, Iterations
T-C / E-A	If true, then continue else abort	VG, VH	Points G and H added V times (E.C. Algebra)
C_U, C_{SN}	PUF challenges for user device and IoT sensor node	MF	Point F added M times (E.C. Algebra)
β_{new}, γ_{new}	New temporary identity of user and IoT sensor node	{M, V}, KDF	Random value, Key derivation function
T_{96}	Truncated to 96 bits	R^1_{SG}	Random secret by gateway for user
R_{SN}	Response to PUF challenge, C_{SN}	XF	Point F added M times (E.C. Algebra)
R_U	Response to PUF challenge, C_U	P_U, P_{SN}	PUF embedded in user device and IoT sensor node
R^2_{SG}	Random secret by gateway for IoT sensor node	CR_{PU}, CR_{PSN}	Challenge response pair for user and IoT sensor node

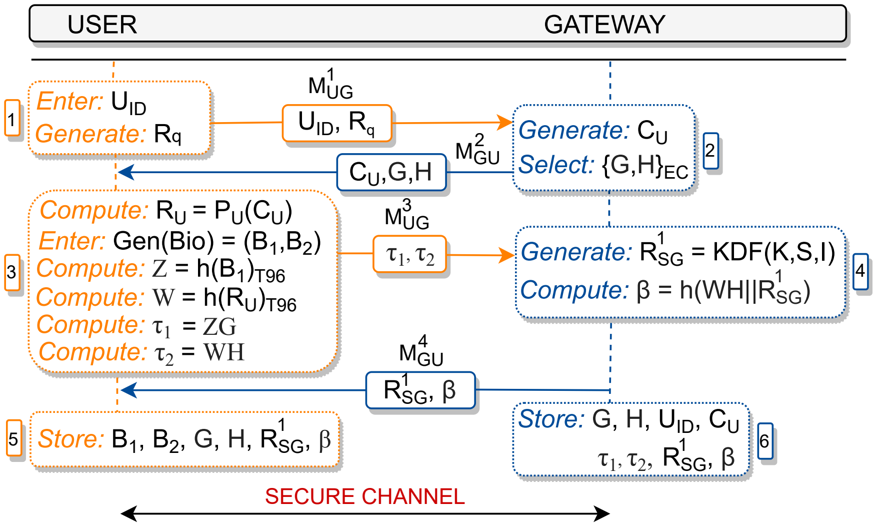

USER
GATEWAY
1
Enter: U_{ID}
Generate: Rq
M^1_{UG}
U_{ID}, R_q
Generate: C_U
Select: $\{G,H\}_{EC}$
2
M^2_{GU}
C_U,G,H
Compute: $R_U = P_U(C_U)$
Enter: Gen(Bio) = (B_1,B_2)
3
Compute: $Z = h(B_1)_{T96}$
Compute: $W = h(R_U)_{T96}$
Compute: τ_1 = ZG
Compute: τ_2 = WH
M^3_{UG}
τ_1, τ_2
Generate: R^1_{SG} = KDF(K,S,I)
Compute: $\beta = h(WH\|\|R^1_{SG})$
4
M^4_{GU}
R^1_{SG}, β
5
Store: B_1, B_2, G, H, R^1_{SG}, β
Store: G, H, U_{ID}, C_U
τ_1, τ_2, R^1_{SG}, β
6
SECURE CHANNEL

Figure 4: User and User Device Registration Phase

- Due to deployment and use at unfriendly locations, physical capturing of IoT sensor nodes and the user device is possible.

B. User and User Device Registration Phase

A user initially registers the device at the gateway. The whole process of user and its device registration is presented in Fig. 4.

Step 1: During the network setup at a smart healthcare institution, each user (healthcare professional) has to be registered with the trusted gateway of the network. During registration, the user needs to enter his/her unique user identity (U_{ID}) issued by the healthcare institution. The user then generates the registration request (R_q), prepares M^1_{UG} (U_{ID}, R_q), and forwards it to the gateway.

Step 2: Upon the reception of M^1_{UG} from the user, the gateway generates a challenge for user device, C_U. Apart from developing the challenge, the gateway also selects two random points on the elliptic curve $\{G, H\}_{EC}$. After that, the gateway prepares M^2_{GU} (C_U, G, H) and sends it to the user.

Step 3: When the user receives M^2_{GU} from the gateway, it prompts its embedded PUF to generate the response R_U = $P_U(C_U)$. Subsequently, the user enters the biometric impression, which is stored in the form of two components, secret string (B_1) and helper string (B_2). Further, the user device computes the message digest of B_1 and R_U and truncates the result to 96 bits for reducing storage space requirements. Now the user device computes τ_1 = ZG and τ_2 = WH. Finally, the user device prepares the message M^3_{UG} (τ_1, τ_2) and sends it to the gateway.

Step 4: The gateway collects the message M^3_{UG} and generates the first random secret, R^1_{SG} = KDF (K,S,I) through *key derivation function*. The temporary identity of user (β = $h(WH$ || $R^1_{SG})$ is also generated to keep the communication anonymous. Lastly, the gateway sends M^4_{GU} (R^1_{SG}, β) to the user.

Step 5: In this step, the user and gateway store the information on their devices. This information is essential for proving and verifying the authenticity of each other in future communications. User and gateway stores B_1, B_2, G, H, R^1_{SG}, β, and G, H, U_{ID}, C_U, τ_1, τ_2, R^1_{SG}, β, respectively.

C. IoT Sensor Node Registration Phase

IoT sensor node performs various tasks based on the deployment scenario. The IoT sensor node cannot relay any information unless it validates its identity at the gateway. Hence, the IoT sensor node undergoes a registration phase during deployment. The entire process is demonstrated through Fig. 5.

Step 1: Every IoT sensor node needs to be registered with the gateway at the smart healthcare institute during the network setup. The gateway produces a challenge for IoT sensor node (C_{SN}) and selects a random point F on the elliptic curve. Gateway then forms a message, M^1_{GI} = (C_{SN}, F) and sends it to IoT sensor node.

Step 2: When the sensor node obtains the message M^1_{GI} from gateway, it determines response R_{SN} = $P_{SN}(C_{SN})$. Further, IoT sensor node computes the message digest of PUF response, X = $h(R_{SN})_{T96}$

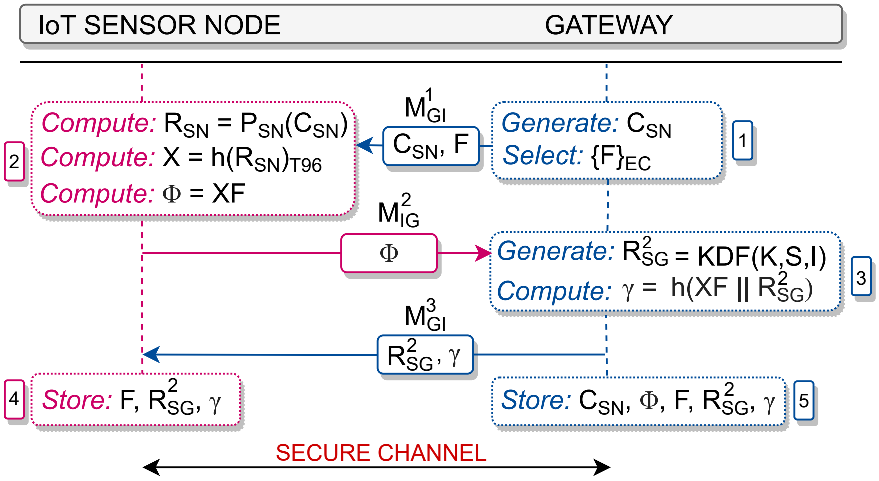

IoT SENSOR NODE
GATEWAY
1
Generate: C_{SN}
Select: $\{F\}_{EC}$
M_{GI}^1
C_{SN}, F
2
Compute: $R_{SN} = P_{SN}(C_{SN})$
Compute: $X = h(R_{SN})_{T96}$
Compute: Φ = XF
M_{IG}^2
Φ
3
Generate: R_{SG}^2 = KDF(K,S,I)
Compute: γ = h(XF || R_{SG}^2)
M_{GI}^3
R_{SG}^2, γ
4
Store: F, R_{SG}^2, γ
5
Store: C_{SN}, Φ, F, R_{SG}^2, γ
SECURE CHANNEL

Figure 5: IoT Sensor Node Registration Phase

and truncates the result to 96 bits for reducing storage space requirements. Next, the IoT sensor node computes Φ = XF (i.e., X times the point F on elliptic curve), composes a message M_{IG}^2= Φ which is forwarded to the gateway.

Step 3: Upon receiving M_{IG}^2, the gateway generates the second random secret R_{SG}^2 = KDF (K,S,I) through *key derivation function*. The gateway also generates the temporary identity of IoT sensor node γ = $h(XF$ || $R_{SG}^2)$ to keep the communication anonymous. Lastly, the gateway sends M_{GI}^3 (R_{SG}^2, γ) to the IoT sensor node.

Step 4: Atlast, the IoT sensor node and gateway stores the secret information on their devices. This information is essential for proving and verifying the authenticity of each other in future communications. IoT sensor node and gateway stores F, R_{SG}^2, γ and C_{SN}, Φ, F, R_{SG}^2, γ, respectively.

D. Mutual Authentication and Key Agreement Phase

This phase is initiated when the user needs to exchange information with the IoT sensor node. Before any secret key negotiation between the user and the IoT sensor node happens, the legitimacy of the user, user device, IoT sensor node, and the gateway is validated. Fig. 6 shows the complete process of the validation and it is discussed below:

Step 1: The user enters his biometric in the device and the fuzzy extractor retrieves $B_1^{'}$, $B_2^{'}$ components of the biometric. The user device evaluates the truthfulness of the entered biometric ($B_1^{'}$, $B_2^{'}$) by comparing it with the biometric value stored in the user device (B_1, B_2) during the registration phase. Unsuccessful results do not enable the current user to access the healthcare IoT network. Now the user device generates nonce (N_1), prepares M_{UG}^1 = (β, N_1) and sends it to the gateway.

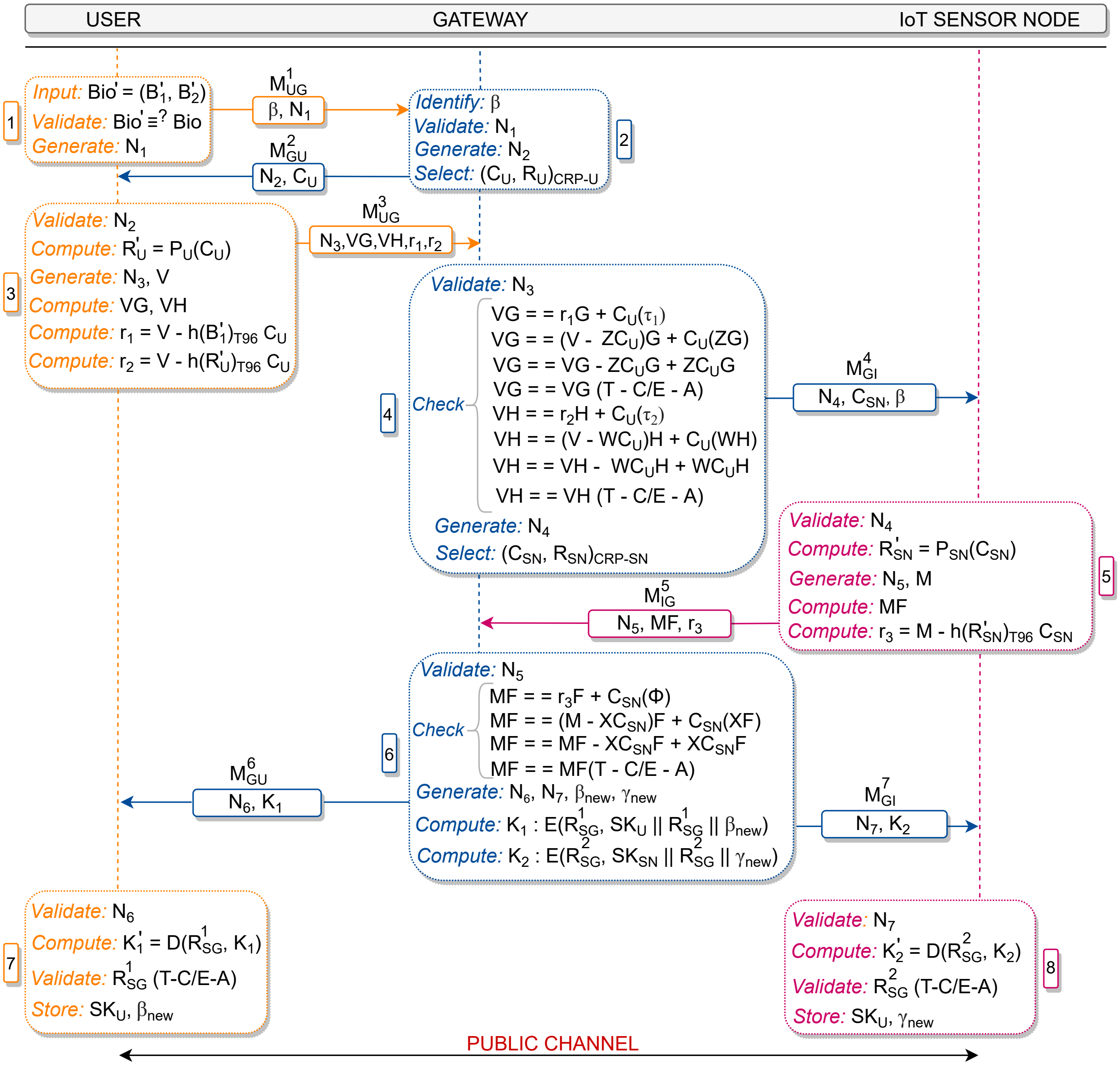


Figure 6: Mutual Authentication and Key Agreement Phase

Step 2: As soon as the gateway gets the M^1_{UG} from user device, it begins to look out for β in the database. Once verified, the gateway begins the validation of nonce N_1 and generates nonce N_2. Lastly, the gateway selects the challenge and response pair for the user device, $(C_U,\ R_U)_{CRP-U}$. The gateway drafts the message M^2_{GU} = $(N_2,\ C_U)$ and delivers it to user device.

Step 3: User device receives the M^2_{GU} from gateway, validates the nonce N_2, and computes the PUF response $R^{'}_U$ = $P_U(C_U)$. Further, user device generates a fresh nonce N_3 and random value V. The user device computes VG, which, as per elliptic curve algebra, is V times the addition of elliptic curve point G to itself; likewise, VH is calculated. In the end, the device computes r_1 = V - $h(B^{'}_1)_{T96}$ C_U and r_2 =

V - $h(R_U^{'})_{T96}$ C_U, forms the message M_{UG}^3 = (N_3, VG, VH, r_1, r_2) and transport it to the gateway.

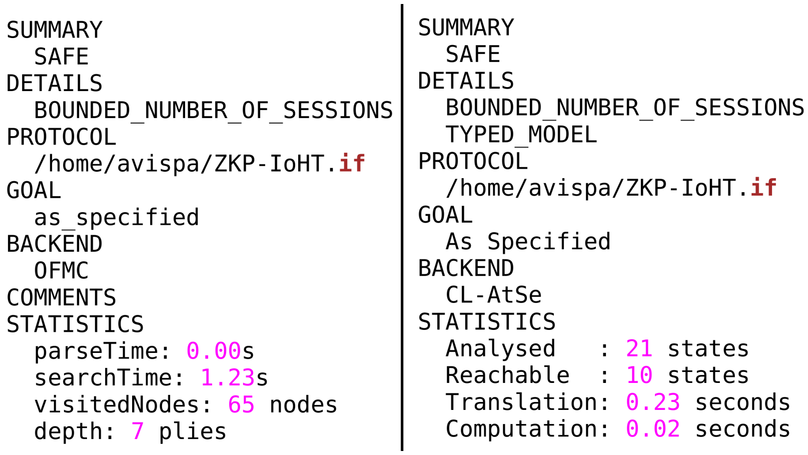
Step 4: When the gateway receives the message M_{UG}^3 from a user device, it validates the nonce N_3. The gateway evaluates the authenticity of the user by computing r_1G + $C_U(\tau_1)$ (wherein G, C_U, τ_1 are retrieved by gateway from its memory) and comparing it with the received VG. Further, the gateway investigates the authenticity of the user device by computing r_2H + $C_U(\tau_2)$ (wherein H, C_U, τ_2 are retrieved by the gateway from its memory) and comparing it with the received VH. The session terminates if either the user or user device fails to prove the authenticity at the gateway. Post-authenticity check, the gateway generates the nonce N_4 and selects the challenge-response pair for the IoT sensor node, (C_{SN}, $R_{SN})_{CRP-SN}$. At the end, gateway sends the M_{GI}^4 = (N_4, C_{SN}, β) to the IoT sensor node.

Step 5: After obtaining M_{GI}^4, the IoT sensor node evaluates the freshness of nonce, N_4. The IoT sensor node computes the PUF response $R_{SN}^{'}$ = $P_{SN}(C_{SN})$ based on the challenge C_{SN} sent by the gateway. Next, the nonce N_5 and random value M is generated by the gateway. The IoT sensor node computes MF (addition of elliptic curve point F to itself by M times; scalar multiplication). At last, IoT sensor node computes the random value, r_3 = M - $h(R_{SN}^{'})_{T96}$ C_{SN}, forms the message M_{IG}^5 = (N_5, MF, r_3), and delivers it to the gateway.

Step 6: Gateway examines the freshness of nonce N_5 after it receives the message M_{IG}^5 from the IoT sensor node. Subsequently, gateway evaluates the authenticity of IoT sensor node by computing the r_3F + $C_{SN}(\Phi)$ (wherein F, C_{SN}, Φ are retrieved by the gateway from its memory) and comparing it with the received MF. The session terminates if IoT sensor node fails to authenticate itself at gateway. The gateway produces nonce N_6 and N_7 apart from the temporary identities of the user (β_{new}) and the IoT sensor node (γ_{new}). The gateway prepares K_1 = $E(R_{SG}^1$, SK_U $||$ R_{SG}^1 $||$ $\beta_{new})$ and K_2 = $E(R_{SG}^2$, SK_{SN} $||$ R_{SG}^2 $||$ $\gamma_{new})$. At last, gateway forms two messages M_{GU}^6 = (N_6, K_1) and M_{GI}^7 = (N_7, K_2) which are sent to the user and the IoT sensor node, respectively.

Step 7: After receiving M_{GU}^6 from the gateway, the user device validates the nonce N_6. Post validation, user device decrypts $K_1^{'}$ = D(R_{SG}^1, K_1) and retrieves SK_U, R_{SG}^1 and β_{new}. The user device authenticates the gateway by comparing the received R_{SG}^1 with the pre-stored value in the user device. The session is terminated in case the stored value and the received value do not match. Lastly, the user device stores the values of single-use secret session key SK_U and temporary identity β_{new} in its database.

Step 8: The IoT sensor node validates the nonce N_7 soon after it receives the M_{GI}^7 message from the gateway. Post validation, IoT sensor node decrypts $K_2^{'}$ = D(R_{SG}^2, K_2) and retrieves the SK_{SN}, R_{SG}^2, and



```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/avispa/ZKP-IoHT.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 1.23s
  visitedNodes: 65 nodes
  depth: 7 plies
```

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/avispa/ZKP-IoHT.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed   : 21 states
  Reachable  : 10 states
  Translation: 0.23 seconds
  Computation: 0.02 seconds
```

Figure 7: Results from OFMC and CL-AtSe backend of AVISPA

γ_{new}. Further, the IoT sensor node tries to match the received value R_{SG}^2 with the pre-stored value in the IoT sensor node to validate the authenticity of the gateway. The session is terminated in case the stored value and the received value contradicts. In last step, the IoT sensor node stores the values of single-use secret session key SK_{SN} and temporary identity γ_{new} in its database.

Zero-Knowledge Proofs have enabled the *user device* (*Prover 1*) and *IoT sensor node* (*Prover 2*) to prove the authenticity at the *gateway* (*Verifier*) without revealing any secret information over the vulnerable wireless channel, thus assuring privacy and resistance to cyber-attacks.

V. Security Analysis

A. Formal

This section proves the robust nature of the presented scheme against various attacks (e.g., replay, impersonation, MITM, modification), verified through the "Automated Validation of Internet Security Protocols and Applications (AVISPA)" tool [45]. AVISPA is a security analyzer used by researchers working on security and authentication protocols to perform formal security analysis. AVISPA offers four backends, namely, on-the-fly mode-checker (OFMC), constraint-logic based attack searcher (CL-AtSe), SAT (Boolean satisfiability problem) based model checker (SATMC), and the tree automata-based on automatic approximations for the analysis of security protocols (TA4SP). AVISPA uses "High-Level Protocol Specification Language (HLPSL)" to convert high-level implementation to "Intermediate Format (IF)" using the HLPSL2IF translator.

We have defined three primary roles in AVISPA, (a) user device, (b) gateway, and (c) IoT sensor node. Besides, the composition of sessions is disclosed, followed by declaring global constants, intruder knowledge, and goals in the environment role. The simulation in the OFMC backend took less than one millisecond to visit 65 nodes at a depth of 7 plies. Likewise, the CL-AtSe backend took 0.23s of translation time and 0.02s of computation time to examine the protocol's robustness against cyber attacks. Fig. 7 demonstrates that AVISPA could not figure out any cyber threat or vulnerability even after many rounds of iterations in the compromised environment. Thus, it can be observed that the proposed protocol secures the IoT-based healthcare applications.

B. Informal

In this section, the security fundamentals and logical reasoning are used to evaluate the strength of the ZKP-AKA against malicious threats.

Theorem 1. *Resistant to replay attacks.*

Proof. Assuming that the attacker has captured a message, M_{GU}^{2} = N_2, C_U and later tries to replay it for gaining access to privileged authorized resources. Despite capturing, the attacker fails to get access as the replayed message contains an old nonce, N_2. Similarly, other messages M_{UG}^{1}, M_{UG}^{3}, M_{GI}^{4}, M_{IG}^{5}, M_{GU}^{6}, and M_{GI}^{7} are not prone to replay attacks. Thus, the proposed scheme withstands replay attacks. □

Theorem 2. *Prevention from MITM attacks.*

Proof. Let's say the adversary intercepts the message, M_{GI}^{4} = N_4, C_{SN}, β. One of the adversary's goals is to retrieve secret or personally identifiable information from intercepted messages to mimic a legitimate entity. If the adversary gets successful, then it would enable the adversary to conduct a MITM attack easily. In message M_{GI}^{4} = N_4, C_{SN}, β, neither the identity details nor any secret information is revealed. β is a temporary identity of the user which is just valid for one session. In contrast, modification to C_{SN} would generate false results at the gateway and IoT sensor node, hence giving no opportunity to the adversary for carrying out a successful MITM attack. Likewise, other messages M_{UG}^{1}, M_{GU}^{2},M_{UG}^{3}, M_{IG}^{5}, M_{GU}^{6}, and M_{GI}^{7} will not be affected by MITM attacks. □

Theorem 3. *Secure from impersonation attacks.*

Proof. In the case of an attacker eavesdropping on the message, M_{IG}^{5} = N_5, MF, r_3, it is possible for the attacker to extract the important information using which the attacker can imitate as a legitimate IoT sensor node. However, the attacker fails to derive any useful information because a scalar product MF is sent instead of M and F, ensuring complete privacy of information. Besides, r_3 = M - h($R_{SN}^{'}$)$_{T96}$ C_{SN}

is protected because of collision-resistant property of hash functions. The attacker is unable to prove its legitimacy without any secret information (e.g., identity or secret value). These characteristics make the proposed protocol secure from impersonation attacks. The other messages M_{UG}^{1}, M_{GU}^{2}, M_{UG}^{3}, M_{GI}^{4}, M_{GU}^{6} and M_{GI}^{7} are also secure from the impersonation attack. □

Theorem 4. *ZKP-AKA ensure data privacy.*

Proof. Suppose an attacker succeeds in stealing the message M_{GU}^{6} = N_6, K_1, where N_6 is nonce and K_1 carries encrypted information that is E(R_{SG}^{1}, SK_U || R_{SG}^{1} || β_{new}). The information is encrypted with the secret value available only with a trusted gateway and legitimate user, so the attacker cannot retrieve any information without the decryption key R_{SG}^{1}. Consequently, the proposed protocol ensures data privacy in M_{GU}^{6} and remaining messages M_{UG}^{1}, M_{GU}^{2}, M_{UG}^{3}, M_{GI}^{4}, M_{IG}^{5} and M_{GI}^{7}. □

Theorem 5. *Attainment of user and sensor node identity anonymity and untraceability.*

Proof. To prove this theorem, we shall consider that the attacker has obtained the message M_{GI}^{4} = N_4, C_{SN}, β where N_4 is nonce, C_{SN} is a challenge for IoT sensor node, and β is the temporary identity of user. Since the user makes use of temporary identity β while communicating with the gateway and IoT sensor node, the real identity U_{ID} is never disclosed; thus the communication remains anonymous. To some extent, the proposed protocol ensures untraceability by using a fresh temporary identity for every session. □

Theorem 6. *Prevention from modification attacks.*

Proof. Let us examine a scenario where the attacker tries to modify the message, M_{UG}^{3} = N_3, VG, VH, r_1, r_2, where N_3 is nonce, VG and VH are points on elliptic curve, r_1 and r_2 are calculated as V - h($B_1^{'}$)$_{T96}$ C_U and V - h(($R_U^{'}$))$_{T96}$ C_U, respectively. It is evident that the attacker is not aware of V, G, and H; moreover, the message contains a message digest. Hence, it is impossible to modify the information because of the hash function and non-availability of information (V, G, H). Any alterations carried out by an attacker can be easily identified at the gateway leading to session termination and attack prevention. The other messages M_{UG}^{1}, M_{GU}^{2}, M_{GI}^{4}, M_{IG}^{5}, M_{GU}^{6} and M_{GI}^{7} are also protected against modification attacks. □

Theorem 7. *Resilient to physical attacks.*

Proof. It may also happen that the adversary physically captures the user device or IoT sensor node for either tampering or cloning. In this case, the adversary will fail because the user device and IoT sensor node are equipped with PUF, and any tampering with the PUF will render it useless. The tampered user device and IoT sensor node will surely not produce the desired output of PUF $(C_U, R_U)_{CRP-U}$ and PUF $(C_{SN}, R_{SN})_{CRP-SN}$. In this way, the device fails to prove its legitimacy at the gateway. The suggested protocol is resilient to physical attacks as cloning is impossible because the PUF is embedded during manufacturing and cannot be imitated. □

Theorem 8. *Secure establishment of session keys.*

Proof. ZKP-AKA ensures the secrecy of the session key during the key agreement process between the parties. The temporary session keys, SK_U and SK_{SN} are encrypted before being sent to the user device and IoT sensor node in messages M^6_{GU} and M^7_{GI}, respectively. The attacker would not be able to decrypt it because it requires R^1_{SG} and R^2_{SG} to reveal the keys, which is not available with the attacker. Thus, the proposed scheme ensures a secure establishment of the session keys. □

Theorem 9. *ZKP-AKA guarantees perfect forward secrecy and unlinkability.*

Proof. Let us believe that the adversary has grabbed the message M^6_{GU} = N_6, K_1, and is trying to discover the secret key, SK_U. Although it is nearly impossible to retrieve the secret key (SK_U) as it is encrypted (E(R^1_{SG}, SK_U || R^1_{SG} || β_{new})), let us consider a hypothetical case where the antagonist successfully obtains it. This could enable the adversary to compromise the current session messages but not the preceding and succeeding because the keys in each session are unique and have no linkage between them. Moreover, the random secret used to secure the session key changes every session. Also, there is no relation between the prior and subsequent random secrets. The adversary could not compute random secrets as the required information (K,S,I) is only available with the gateway and never shared on the vulnerable public channel. Therefore, the adversary cannot predict future and past secret keys, even if the present key is compromised, which in turn guarantees perfect forward and backward secrecy. Besides, the entities use unique temporary identities (β, γ) per session instead of real identities; consequently, an adversary can't find any connection between messages exchanged in different sessions. Thus, ZKP-AKA ensures unlinkability in all its sessions. □

VI. Performance and Comparative Analysis

The performance of the ZKP-AKA protocol is evaluated on various parameters, including storage space requirements, security attributes, computation complexity, communication expenses, and energy cost. A

Table II: **Comparison of ZKP-AKA Protocol vs. Conventional Protocols**

$\mathcal{SG}$	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	$\mathcal{Z}$
$\mathcal{SG}_1$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{SG}_2$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{SG}_3$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{SG}_4$	✓	×	×	✓	×	×	✓	×	✓
$\mathcal{SG}_5$	✓	×	✓	✓	×	✓	✓	×	✓
$\mathcal{SG}_6$	✓	✓	✓	×	×	✓	✓	✓	✓
$\mathcal{SG}_7$	×	×	✓	×	×	×	×	×	✓
$\mathcal{SG}_8$	×	×	✓	×	×	×	×	×	✓
$\mathcal{SG}_9$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{SG}_{10}$	✓	×	×	✓	×	×	×	×	✓
$\mathcal{SG}_{11}$	✓	✓	✓	✓	×	×	✓	✓	✓
$\mathcal{SG}_{12}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{SG}_{13}$	✓	✓	✓	✓	✓	✓	✓	×	✓
$\mathcal{SG}_{14}$	−	✓	✓	✓	✓	−	✓	✓	✓
$\mathcal{SG}_{15}$	✓	×	✓	×	×	✓	×	×	✓
$\mathcal{SG}_{16}$	−	×	✓	✓	✓	−	✓	✓	✓
$\mathcal{SG}_{17}$	×	×	✓	×	×	×	×	×	✓

$\mathfrak{Acronyms}$: $\mathcal{SG}$: Security goals, $\mathcal{Z}$: ZKP-AKA protocol, $(\checkmark)$: Secure against attack/preserves a security attribute, $(\times)$: Vulnerable/non accomplishment of security attribute, $(-)$: Not applicable, $\mathcal{SG}_1$: Replay, $\mathcal{SG}_2$: Impersonation, $\mathcal{SG}_3$: Modification of messages, $\mathcal{SG}_4$: DoS, $\mathcal{SG}_5$: MITM, $\mathcal{SG}_6$: Known key, $\mathcal{SG}_7$: Cloning, $\mathcal{SG}_8$: Side-channel, $\mathcal{SG}_9$: Mutual authentication, $\mathcal{SG}_{10}$: Data privacy, $\mathcal{SG}_{11}$: Session key security, $\mathcal{SG}_{12}$: Message integrity, $\mathcal{SG}_{13}$: Message freshness, $\mathcal{SG}_{14}$: User identity anonymity, $\mathcal{SG}_{15}$: Sensor node identity anonymity, $\mathcal{SG}_{16}$: User untraceability, $\mathcal{SG}_{17}$: Sensor node untraceability, S_1: [20], S_2: [21], S_3: [22], S_4: [23], S_5: [24], S_6: [25], S_7: [26], S_8: [27].

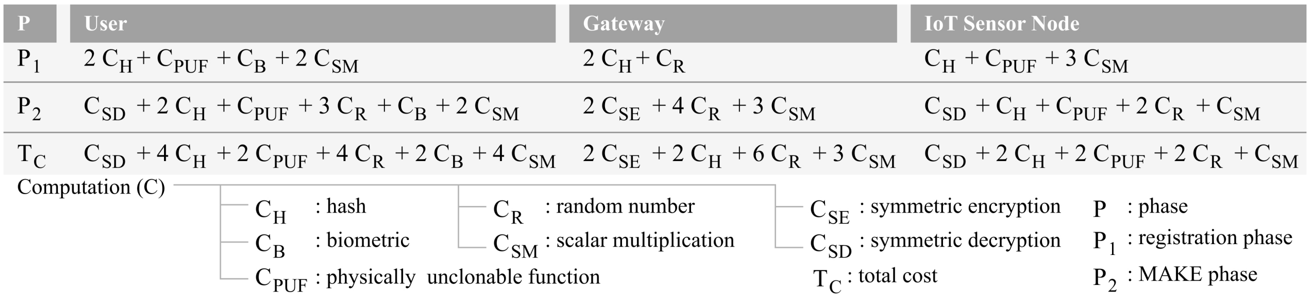
comprehensive analysis of the performance of the ZKP-AKA protocol is performed and furnished in this section as follows:

A. Storage Space Requirements

The ZKP-AKA protocol has been tested using the CM5000 TelosB mote with the following specifications - TI MSP430F1611 micro-controller, CC2420 RF chip, memory 1MB and power source of 3V (2xAA battery) [46]–[48]. Out of the total memory space available, only 0.0048% is used by the ZKP-AKA protocol to execute its operations. Similarly, an intelligent user device [49], [50] uses very little amount (0.0000000029%) of the total memory space available. Clearly, the scheme proposed achieves storage space efficiency, which is an utmost requirement for sustainable healthcare applications in a resource-constrained environment.

B. Security Attributes and Computation Cost Analysis

Table II shows that the traditional schemes are not secure from attacks such as confidentiality, integrity, replay, etc. In contrast, the proposed scheme is found much stronger when compared to the existing



P	User	Gateway	IoT Sensor Node
P_1	$2\,C_H + C_{PUF} + C_B + 2\,C_{SM}$	$2\,C_H + C_R$	$C_H + C_{PUF} + 3\,C_{SM}$
P_2	$C_{SD} + 2\,C_H + C_{PUF} + 3\,C_R + C_B + 2\,C_{SM}$	$2\,C_{SE} + 4\,C_R + 3\,C_{SM}$	$C_{SD} + C_H + C_{PUF} + 2\,C_R + C_{SM}$
T_C	$C_{SD} + 4\,C_H + 2\,C_{PUF} + 4\,C_R + 2\,C_B + 4\,C_{SM}$	$2\,C_{SE} + 2\,C_H + 6\,C_R + 3\,C_{SM}$	$C_{SD} + 2\,C_H + 2\,C_{PUF} + 2\,C_R + C_{SM}$

Computation (C)

C_H	: hash	C_R	: random number	C_{SE}	: symmetric encryption	P	: phase
C_B	: biometric	C_{SM}	: scalar multiplication	C_{SD}	: symmetric decryption	P_1	: registration phase
C_{PUF}	: physically unclonable function			T_C	: total cost	P_2	: MAKE phase

Figure 8: Computation Cost of ZKP-AKA protocol

schemes. Further, Fig. 8 provides the computation cost spent by different network devices in the ZKP-AKA protocol. ZKP-AKA uses only lightweight cryptography functions such as message digest, ZKP, PUF, etc. rather than bulky cryptography operations. The use of less complex cryptographic operations in the ZKP-AKA protocol preserves the network devices' computation power, storage space, and energy reserves. Fig. 9 presents the computational cost of conventional protocols versus the computation cost of ZKP-AKA protocol for the mutual authentication and key agreement phase. It is evident that the ZKP-AKA protocol uses fewer cryptography primitives than traditional protocols [20]–[27]; hence, the proposed scheme is more computation efficient.

Fig. 10 illustrates the computation cost spent by the user device, gateway, and IoT sensor node in ZKP-AKA and conventional protocols. The schemes [20] and [25] have low and moderate computation complexities; but, these schemes do not support user-based IoT-Healthcare applications. Whereas [21] and [27] have reasonable computation expenditures, they are likely to be exploited by attackers, as proven in Table II. It is apparent from Fig. 10 that other protocols [22], [23], [24], and [26] have high computation expenses compared to the ZKP-AKA protocol. ZKP-AKA is proven to be the most computation-efficient protocol that satisfies the security requirements of sustainable healthcare applications.

C. Communication and Energy Cost Analysis

Fig. 11(a) shows the number of bits exchanged between entities in ZKP-AKA and traditional protocols. It is perceptible from Fig. 11(a) that ZKP-AKA incurs minimum communication cost, whereas [22] has the highest cost. The schemes [21] and [23]–[27], in contrast to scheme [22], are relatively reasonable but far costlier than ZKP-AKA. The quantity of bits exchanged in the protocol [20] is closer to ZKA-AKA but is susceptible to cloning and side-channel attacks and does not ensure untraceability. The exchange of enormous bits reduce the lifetime of IoT and other network devices because the energy drain is proportional to the number of bits exchanged during protocol execution. As per the datasheet [46], TelosB

Scheme	Computation Cost
S_1	$C_{AE} + 3\,C_{AD} + 2\,C_H + 2\,C_M + 2\,C_{XOR}$
S_2	$18\,C_H + 9\,C_{XOR} + 2\,C_H$
S_3	$22\,C_H + 5\,C_{PUF} + 16\,C_{XOR} + 3\,C_R + C_B$
S_4	$37\,C_H + 16\,C_{XOR} + 2\,C_R + C_B$
S_5	$4\,C_{SE} + 4\,C_{SD} + 19\,C_H + 14\,C_{XOR} + 4\,C_R + C_B + 3\,C_{SM}$
S_6	$15\,C_H + 10\,C_{XOR} + 2\,C_R$
S_7	$25\,C_H + 20\,C_{XOR} + 3\,C_R + 9\,C_{MOD}$
S_8	$18\,C_H + 9\,C_{XOR} + 3\,C_R + C_B + 6\,C_{SM}$
ZKP-AKA	$2\,C_{SE} + 2\,C_{SD} + 3\,C_H + 2\,C_{PUF} + 9\,C_R + C_B + 6\,C_{SM}$

Computation (C)

C_{AE}	: asymmetric encryption	C_R	: random number
C_{AD}	: asymmetric decryption	C_B	: biometric
C_H	: hash (message digest)	C_{MOD}	: modulus
C_{SE}	: symmetric encryption	C_{XOR}	: bit-wise XOR
C_{SD}	: symmetric decryption	C_{SM}	: scalar multiplication
C_M	: hash based MAC		
C_{PUF}	: physically unclonable function		

Figure 9: Computation Cost Comparison of ZKP-AKA Protocol vs. Conventional Protocols; S_1: [20], S_2: [21], S_3: [22], S_4: [23], S_5: [24], S_6: [25], S_7: [26], S_8: [27].

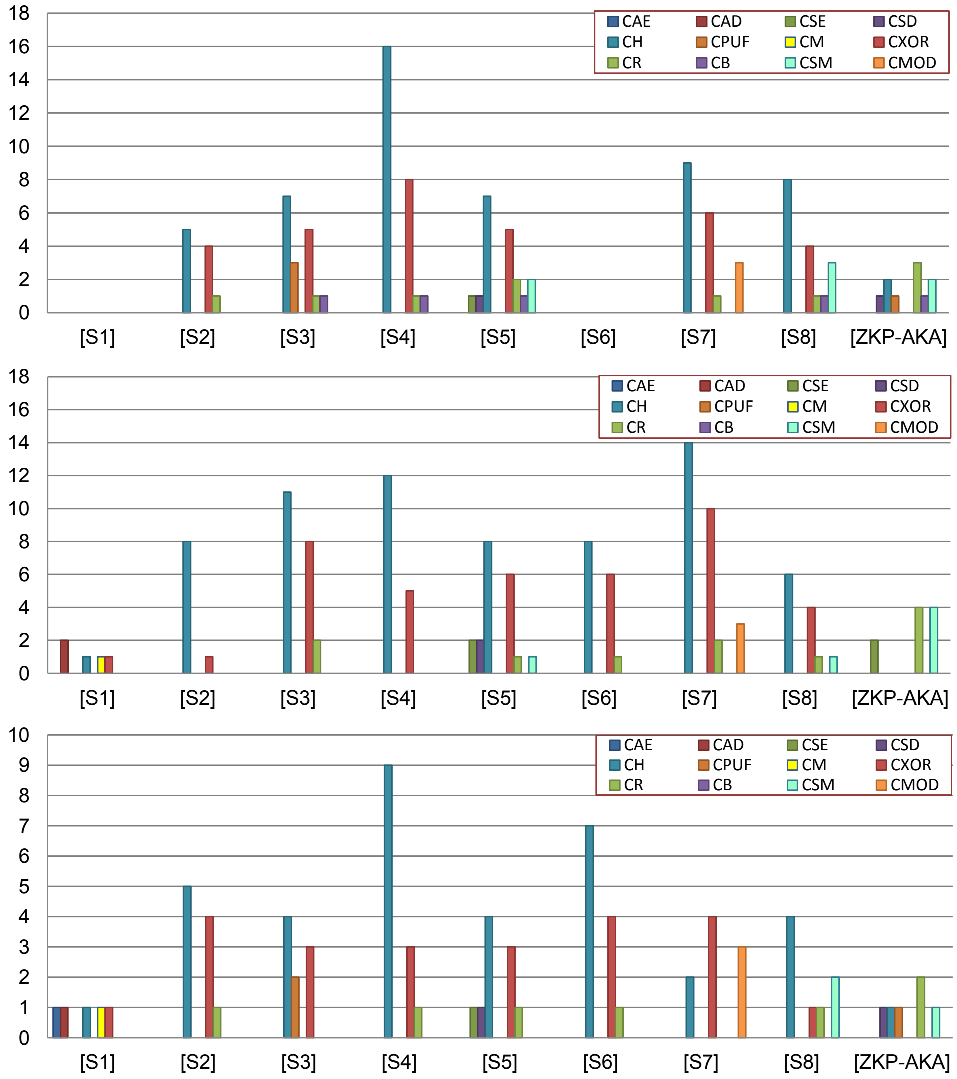
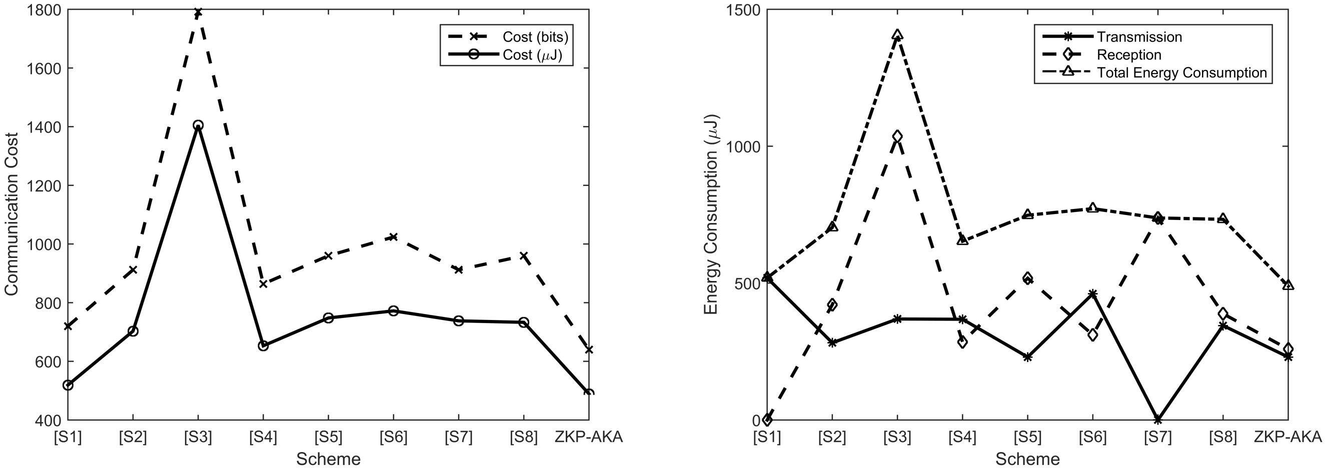


Figure 10: Computation Cost of User (Atop), Gateway (Middle), and IoT Sensor Node (Last) of ZKP-AKA Protocol vs. Conventional Protocols; S_1: [20], S_2: [21], S_3: [22], S_4: [23], S_5: [24], S_6: [25], S_7: [26], S_8: [27]



(a) (b)

Figure 11: (a) Comparison of communication cost incurred by IoT Sensor Node (b) Energy Cost Comparison of ZKP-AKA vs. Conventional Protocols $\{S_1$: [20], S_2: [21], S_3: [22], S_4: [23], S_5: [24], S_6: [25], S_7: [26], S_8: [27]$\}$.

mote consumes 0.72 μJ and 0.81 μJ of energy while sending and receiving a bit, respectively. Fig. 11(b) provides insights on the energy consumed by an IoT sensor node in different protocols to exchange messages in the mutual authentication and key agreement phase. It is observed from the calculations that protocol in [22] drains a lot of energy during implementation, whereas protocols in [21], [23]–[27] exhaust less energy compared to [22], but enough to affect the life cycle of the IoT nodes. Although the energy consumption of the protocol in [20] and ZKP-AKA are proximal to each other, [20] is prone to cyber attacks, as discussed lately. Consequently, the ZKP-AKA protocol is superior to existing protocols in terms of communication and energy costs.

VII. Conclusions and Future Directions

The paper proposes a Zero-Knowledge Proofs-based novel mutual authentication and key agreement protocol to secure the IoT-based critical healthcare applications. The essential security features are attained using asymmetric key cryptography, message digest, PUF, etc. The presented protocol withstands major security threats such as MITM, replay, impersonation, and physical attacks to ensure sustainable healthcare services. Other benefits of the protocol include anonymous and untraceable communication in the public channel. The formal and informal security analysis show that the scheme is non-vulnerable and robust. Additionally, it incurs low computational and communication costs when compared with the conventional protocols in the IoT-Healthcare. The future research aspects may include homomorphic encryption to escalate privacy, and blockchain to decentralize the environment for enhancing sustainability.

Declaration of competing interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] H. Zahmatkesh and F. Al-Turjman, “Fog computing for sustainable smart cities in the iot era: Caching techniques and enabling technologies-an overview,” *Sustainable Cities and Society*, vol. 59, p. 102139, 2020.

[2] S. K. Singh, Y.-S. Jeong, and J. H. Park, “A deep learning-based iot-oriented infrastructure for secure smart city,” *Sustainable Cities and Society*, vol. 60, p. 102252, 2020.

[3] D. A. da Silva, R. T. de Sousa Jr, R. de Oliveira Albuquerque, A. L. S. Orozco, and L. J. G. Villalba, “Iot-based security service for the documentary chain of custody,” *Sustainable Cities and Society*, vol. 71, p. 102940, 2021.

[4] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, “Security and privacy-preserving challenges of e-health solutions in cloud computing,” *IEEE access*, vol. 7, pp. 74 361–74 382, 2019.

[5] P. J. Choi, R. J. Oskouian, and R. S. Tubbs, “Telesurgery: past, present, and future,” *Cureus*, vol. 10, no. 5, 2018.

[6] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, “Fog computing for healthcare 4.0 environment: Opportunities and challenges,” *Computers & Electrical Engineering*, vol. 72, pp. 1–13, 2018.

[7] J. Vora, P. Italiya, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and K.-F. Hsiao, “Ensuring privacy and security in e-health records,” in *2018 International conference on computer, information and telecommunication systems (CITS)*. IEEE, 2018, pp. 1–5.

[8] B. Deebak, “Lightweight authentication and key management in mobile-sink for smart iot-assisted systems,” *Sustainable Cities and Society*, vol. 63, p. 102416, 2020.

[9] M. Pandey, R. Agarwal, S. K. Shukla, and N. K. Verma, “Security of healthcare data using blockchains: A survey,” *arXiv preprint arXiv:2103.12326*, 2021.

[10] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K.-K. R. Choo, and Y. Park, “Design of secure and lightweight authentication protocol for wearable devices environment,” *IEEE journal of biomedical and health informatics*, vol. 22, no. 4, pp. 1310–1322, 2017.

[11] Y.-M. Huang, M.-Y. Hsieh, H.-C. Chao, S.-H. Hung, and J. H. Park, “Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks,” *IEEE journal on selected areas in communications*, vol. 27, no. 4, pp. 400–411, 2009.

[12] B. D. Deebak, “Secure and efficient mutual adaptive user authentication scheme for heterogeneous wireless sensor networks using multimedia client–server systems,” *Wireless Personal Communications*, vol. 87, no. 3, pp. 1013–1035, 2016.

[13] Y. K. Ever, “Secure-anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks,” *IEEE systems journal*, vol. 13, no. 1, pp. 456–467, 2018.

[14] T.-H. Chen and W.-K. Shih, “A robust mutual authentication protocol for wireless sensor networks,” *ETRI journal*, vol. 32, no. 5, pp. 704–712, 2010.

[15] L. Xu and F. Wu, “Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care,” *Journal of medical systems*, vol. 39, no. 2, pp. 1–9, 2015.

[16] L. Wang, “Analysis and enhancement of a password authentication and update scheme based on elliptic curve cryptography,” *Journal of Applied Mathematics*, vol. 2014, 2014.

[17] V. Odelu, A. K. Das, and A. Goswami, “An efficient ecc-based privacy-preserving client authentication protocol with key agreement using smart card,” *Journal of Information Security and Applications*, vol. 21, pp. 1–19, 2015.

[18] M. Turkanović, B. Brumen, and M. Hölbl, “A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion,” *Ad Hoc Networks*, vol. 20, pp. 96–112, 2014.

[19] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, “An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment,” *Ad Hoc Networks*, vol. 36, pp. 152–176, 2016.

[20] G. Singh, G. Kumar, H. Monga, T.-H. Kim, M. Liyanage, and P. Kumar, “Robust and lightweight key exchange (lke) protocol for industry 4.0,” *IEEE Access*, vol. 8, pp. 132 808–132 824, 2020.

[21] C.-C. Chang and H.-D. Le, “A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks,” *IEEE Transactions on wireless communications*, vol. 15, no. 1, pp. 357–366, 2015.

[22] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, “Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks,” *IEEE transactions on industrial informatics*, vol. 15, no. 9, pp. 4957–4968, 2019.

[23] 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*, vol. 5, no. 6, pp. 4900–4913, 2018.

[24] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, and K.-K. R. Choo, “A robust and energy efficient authentication protocol for industrial internet of things,” *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1606–1615, 2018.

[25] A. Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Rodriguez, A. Bicaku, S. Maksuti, M. G. Tauber, C. Schmittner, and J. Bastos, “A lightweight authentication mechanism for m2m communications in industrial iot environment,” *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 288–296, 2017.

[26] S. Paliwal, “Hash-based conditional privacy preserving authentication and key exchange protocol suitable for industrial internet of things,” *IEEE Access*, vol. 7, pp. 136 073–136 093, 2019.

[27] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, “A robust ecc-based provable secure authentication protocol with privacy preserving for industrial internet of things,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3599–3609, 2018.

[28] S. H. Islam and G. Biswas, “Design of improved password authentication and update scheme based on elliptic curve cryptography,” *Mathematical and Computer Modelling*, vol. 57, no. 11-12, pp. 2703–2717, 2013.

[29] C.-L. Lin and T. Hwang, “A password authentication scheme with secure password updating,” *Computers & Security*, vol. 22, no. 1, pp. 68–72, 2003.

[30] H. Debiao, C. Jianhua, and H. Jin, “An id-based client authentication with key agreement protocol for mobile client–server environment on ecc with provable security,” *Information Fusion*, vol. 13, no. 3, pp. 223–230, 2012.

[31] R. Amin, S. H. Islam, P. Gope, K.-K. R. Choo, and N. Tapas, “Anonymity preserving and lightweight multimedical server authentication protocol for telecare medical information system,” *IEEE journal of biomedical and health informatics*, vol. 23, no. 4, pp. 1749–1759, 2018.

[32] C.-L. Hsu, T.-V. Le, M.-C. Hsieh, K.-Y. Tsai, C.-F. Lu, and T.-W. Lin, “Three-factor ucsso scheme with fast authentication and privacy protection for telecare medicine information systems,” *IEEE Access*, vol. 8, pp. 196 553–196 566, 2020.

[33] L. Zhang, Y. Zhang, S. Tang, and H. Luo, “Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement,” *IEEE Transactions on Industrial Electronics*, vol. 65, no. 3, pp. 2795–2805, 2017.

[34] “Healthcare data breach report.”

[35] M. A. Rahman, M. S. Hossain, A. J. Showail, N. A. Alrajeh, and M. F. Alhamid, “A secure, private, and explainable ioht framework to support sustainable health monitoring in a smart city,” *Sustainable Cities and Society*, p. 103083, 2021.

[36] J. Al-Muhtadi, K. Saleem, S. Al-Rabiaah, M. Imran, A. Gawanmeh, and J. J. Rodrigues, “A lightweight cyber security framework with context-awareness for pervasive computing environments,” *Sustainable Cities and Society*, vol. 66, p. 102610, 2021.

[37] D. Dolev and A. Yao, “On the security of public key protocols,” *IEEE Transactions on information theory*, vol. 29, no. 2, pp. 198–208, 1983.

[38] S. Goldwasser, S. Micali, and C. Rackoff, “The knowledge complexity of interactive proof systems,” *SIAM Journal on computing*, vol. 18, no. 1, pp. 186–208, 1989.

[39] C. Hazay and Y. Lindell, “A note on zero-knowledge proofs of knowledge and the zkpok ideal functionality.” *IACR Cryptol. ePrint Arch.*, vol. 2010, p. 552, 2010.

[40] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, “Physical one-way functions,” *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[41] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, “Silicon physical random functions,” in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 2002, pp. 148–160.

[42] S. Singh, P. K. Sharma, B. Yoon, M. Shojafar, G. H. Cho, and I.-H. Ra, “Convergence of blockchain and artificial intelligence in iot network for the sustainable smart city,” *Sustainable Cities and Society*, vol. 63, p. 102364, 2020.

[43] S. Jegadeesan, M. Azees, P. M. Kumar, G. Manogaran, N. Chilamkurti, R. Varatharajan, and C.-H. Hsu, “An efficient anonymous mutual authentication technique for providing secure communication in mobile cloud computing for smart city applications,” *Sustainable Cities and Society*, vol. 49, p. 101522, 2019.

[44] 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*, vol. 41, pp. 878–885, 2018.

[45] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P. H. Drielsma, P.-C. Héam, O. Kouchnarenko, J. Mantovani *et al.*, “The avispa tool for the automated validation of internet security protocols and applications,” in *International conference on computer aided verification*. Springer, 2005, pp. 281–285.

[46] S. Fajarado, “CM5000 Datasheet,” http://www.epssilon.cl/files/EPS5000.pdf, 2010, online; accessed February 15, 2020.

[47] S. H. Ebenuwa, M. S. Sharif, M. A., and A. Al-Nemrat, “Variance ranking attributes selection techniques for binary classification problem in imbalance data,” *IEEE Access*, vol. 7, pp. 24 649–24 666, 2019.

[48] M. A., S. Khan, S. S. R. Krishnan, Q.-V. Pham, M. P. K. Reddy, and T. R. Gadekallu, “A multidirectional lstm model for predicting the stability of a smart grid,” *IEEE Access*, vol. 8, pp. 85 454–85 463, 2020.

[49] B. Bera, S. Saha, A. K. Das, N. Kumar, P. Lorenz, and M. A., “Blockchain-envisioned secure data delivery and collection scheme for 5g-based iot-enabled internet of drones environment,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 9097–9111, 2020.

[50] M. A. and R. Broadhurst, “Spam and criminal activity,” *Trends and issues in crime and criminal justice*, no. 526, pp. 1–20, 2016.