Privacy-Preserving Authentication with Service Analytics for Forensic-Aware Cyber-Physical Systems

B D Deebak, *Member, IEEE,* Seong Oun Hwang, *Senior Member, IEEE,*

***Abstract*—Forensic Aware Cyber-Physical System (FA-CPS) is an evolving core of digital forensic systems that discovers the integrity of biometric service platforms. Most forensic agencies use emerging technologies such as IoT, Cloud, etc., to integrate a few core elements (networking, communication, and distributed computing) to achieve sustainable memory forensics. This systematic process brings additional capabilities to the physical systems that capture device memories to discover the evidence of malicious tools. Therefore, this paper deals with the Internet of Things (IoT) to form an effective and economical interaction with evolving technologies, including B5G/6G, edge, and cloud computing, to uncover the context of security implications. Most precisely, to sense, collect, share, and analyze numerical data from information systems, the application domain, like healthcare, utilizes computing methods and communications technologies to collect and analyze physiological data from patients in a haphazard way. Since an insecure network has security issues such as information leakage, secret key loss, and fraudulent authentication in Telehealth and remote monitoring, this work applies elliptic curve cryptography (ECC) and a physical unclonable function (PUF) to construct an AI-driven privacy-preserving key authentication framework (AID-PPKAF). In the proposed AID-PPKAF, the PUF generates key information, and ECC encrypts the parameters generated by the system to establish session key agreement and proper mutual authentication. The security analyses (both formal and informal) prove that AID-PPKAF has greater security efficiency than other state-of-the-art approaches. Lastly, a performance analysis using NS3 and a pragmatic study using SVM demonstrate the significance of identity protection in designing a more reliable authentication model.**

***Index Terms*—Internet of Things; Elliptic curve cryptography; Physical unclonable function; Privacy-preserving; Authentication; Artificial intelligence**

I. Introduction

In FA-CPS, interconnected devices (autonomous cars, the military Internet, assistive technologies) generate voluminous real-time data that may even be exchanged among components or systems in order to provide seamless connectivity [1]. Since data transfer is openly accessible, a malicious user can compromise the system to exfiltrate sensitive data for financial gain. As a consequence, an in-depth analysis is necessary to analyze the legal context of digital devices, including civil inquiry and criminal investigation [2]. A strategy of time-series analysis examines device connectivity and data storage based on digital forensics to inspect the volumes of data generated by real-time devices. Most devices use approved information to circumvent the examination of data prone to a distributed denial of service (DDoS) attack in order to examine cloud-based data sources.

Akbal et al. [3] explained the location features needed to investigate web user activities, including online banking, blogging, social interactions, and searching for malicious activities. Fletcher [4] analyzed timeline data with a network analyzer that uses a forensic tool known as log2timeline to support the data capture format. Shafqat [5] investigated Google Chrome's three modes (private, portable, and regular), logging different information sets to infer the nature of web sources such as bookmarks, downloads, search keywords, and websites visited. As an instance, in forensic medicine, Healthy human bodies have a few basic needs, such as safety, self-actualization, and physiological survival, in order to have a calm existence with stimulating mental activity. Conversely, an unhealthy body requires proper diagnosis and treatment to prevent illness and disease by using a healthcare system.

Healthcare systems manage all nursing processes to avoid the slightest problem (including recurrent power supply issues) during remote patient monitoring. Otherwise, patients' lives may worsen from not addressing serious risks like heart failure and mental illness. To assist medical professionals and avoid human error, a scalable self-organizing wireless mesh network guarantees trust in the security of network-oriented devices such as wireless medical sensor networks (WMSNs) and the Internet of Medical Things (IoMT). Also, this service facilitates more critical requirements of applications, such as exchanging and interpreting data to achieve better decision-making without human intervention. Just a statement of fact, emerging technology has developed a reliable authentication system that offers novel computing services to minimize treatment costs and shorten diagnostic periods to gain benefits from remote monitoring.

In recent times, healthcare industries have been growing faster, instituting around 20.4 billion network-enabled devices and interconnected technologies. Most technologies rely on three significant models of communication (transmission, interaction, and transaction) to remotely examine patient-treatment procedures. Familiar concepts such as big data and deep learning organize a large amount of real-time data to perform advanced data analytics. Most real-time applications use statistical learning paradigms as a branch of data science, reviewing the challenges of industries such as finance, marketing, advertising, remote sensing, and transportation [6]. Industrial applications tap into big data to define three theoretical descriptions in terms of high volume, high velocity, and extensive variety.

Innovative forms extract features such as trends, behaviors, and patterns that enhance situational perceptions, but are still vulnerable when addressing the processes of data management. The operative procedures of a WMSN exploit segments of the IoMT to connect network components and application devices. A WMSN can enhance the coverage areas of the computing devices to provide better medical treatment, including consultation and diagnostics. However, each participant demands a proper key agreement protocol (KAP) to link or transfer his/her sensitive information over insecure network channels [7]. To examine security efficiencies such as mutual authentication and session key agreement, participants (including patients and medical professionals) assess innovative frameworks using formal analysis.

Of late, the potential applications of the IoMT, such as remote surgery, medical emergency treatments, and patient information management, have addressed various security and privacy issues that pose severe threats to the storage of sensitive healthcare data

*Corresponding Authors (Seong Oun Hwang)

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (Ministry of Science and ICT) (RS-2024-00340882).

B D Deebak and Seong Oun Hwang are with the Department of Computer Engineering, Gachon Univesity, Gachon University, Seongnam 13120, South Korea e-mail: (deebak@gachon.ac.kr and sohwang@gachon.ac.kr).

[8]. Therefore, a few of these key properties are highlighted below.

- *Secrecy of sensitive data* guarantees that sensitive information of patients or professionals is diligently encrypted while exchanging data over the IoMT [9].
- *The integrity of sensitive data* guarantees that sensitive information of patients and professionals cannot be altered or modified by unauthorized agents to avoid incorrect predictions of disease or medical treatments [10].
- *The availability of sensitive data* guarantees they will be accessible to legitimate entities, including patients and professionals, in order to take appropriate action within deadlines [11].
- *Proper mutual authentication among users of the IoMT* guarantees that only legal participants successfully execute the authentication phase before sharing or exchanging sensitive data. Otherwise, participants cannot confidently recognize each other [12].
- *Secret key freshness* ensures the transmitted sensitive data is encrypted with a newly generated key to resist replay attacks and ensure secrecy going forward [13].

The next subsections discuss the motivation to address the challenges of device management and the research contributions that deal with attacks pertinent to the IoMT.

A. Motivation

In communication models around the globe, information analysis plays a crucial role in perceiving the nature of information sources, such as social media and the web, plus online courses, videos, and news. It also plays a key role in data exploration in order to understand the actual impacts on business, enterprise, and management environments. Information analysis applies machine learning (ML), data mining, and multivariate statistics to merge knowledge areas (theoretical, analytical, and technological) that orient extensive information in building a decision support system [14]. At present, industrial applications are associated with interconnected devices, and system software regulates the competencies of practical devices in terms of data acquisition and processing.

Most healthcare devices use sensing units to activate data flow over a self-organizing network to monitor the physical conditions of patients. Communication networks prefer WMSNs to transport medical data among the participants [15]. As a result, we believe that Artificial Intelligence in the IoMT (AI-IoMT) empowers the computing performance of healthcare systems to monitor and diagnose patient conditions remotely. Moreover, AI-IoMT engages and gratifies device interactions between patients and professionals to achieve early intervention and more accurate diagnoses. However, the key benefits of AI-IoMT are still not recognized across healthcare applications because it is prone to severe threats. In addition, IoMT applications are at risk from cyber-attacks when using an insecure wireless medium without robust security mechanisms [16].

Medical technologies (namely, wearable devices, electronic health records, and portable monitors) support healthcare automation, and thus, malignant activity may result in uncertain outcomes. Therefore, cybersecurity specialists are designing strategies like encryption schemes, including lattice-based and digital signatures, across system hardware and application software to prevent data breaches and vulnerabilities. In reality, medical institutes and stakeholders cannot prevent security breaches because the conventional approaches have already been affected severely (e.g., 41.2 Million records in 2019 [17]). Moreover, the deployment of the IoMT and AI is crucial for analyzing threat factors associated with healthcare systems using authentication techniques.

Most techniques utilized in edge computing explore adequate computing resources to authorize connectivity with intermediate nodes. Excessive computation often involves complex processes to create a scalable network and also utilize secret network data to prevent internal and external threats. Shariq et al. [18] designed a provably secure lightweight privacy-preserving authentication (PSL-PPA) to achieve high-level security features (i.e., anonymity and known-key secrecy). Pu et al. [19] developed a secure privacy-preserving authentication (SPPA) to offer high-level security protection against password-guessing and key impersonation attacks. Moreover, the SPPA exhibits conditional privacy-preserving features to ensure data confidentiality. To address key factors, this paper extensively studies a few security vulnerabilities, such as impersonation, man-in-the-middle attacks, illegal session key computation, and credential leakage [20]. Also, to protect healthcare IT systems, this paper constructs a robust security framework using AI. It specifically applies a support vector machine (SVM) through the service-ware analytic phase to analyze user behaviors based on their unique pattern (keystroke) to classify the input as 'authorized or unauthorized'. Please note that the other classifiers (logistic regression and random forest) cannot achieve better decisions due to slower prediction time.

B. Contributions

An IoT ecosystem comprises a few basic components of interconnected technologies (namely, remote connectivity, an application dashboard, network access, a device gateway, data storage, and system analytics) to accelerate the process of developing security strategies via integrated AI. In healthcare systems, the core functionalities of the IoT ecosystem (sensory components, wearable devices, and clinical strategies) can be exploited to minimize overall development costs and achieve better quality of care. Because medical devices are so ubiquitous and they offer seamless connections (including processing of critical medical data), severe security and privacy concerns arise, namely, data modification and disclosure. Sometimes, online attackers may target healthcare systems or their computing devices to obtain sensitive patient data [21]. Therefore, deployment of the IoMT requires AI security (AISec) to meet the essential requirements of healthcare applications. The major contributions of this paper are as follows.

1) We present an AI-driven privacy-preserving key authentication framework (AID-PPKAF) based on elliptic curve cryptography (ECC) and a physical unclonable function (PUF) to utilize lightweight operations such as a one-way hash function and bitwise XOR [22].
2) We construct a network with a threat model using the Dolev-Yao (DY) and Canetti-Krawczyk (CK) adversarial models [23] to analyze the core features of application devices, such as session states and private keys, that are vulnerable to session-hijacking attacks.
3) We conduct both formal and informal analyses using the properties of the DY and CK models to demonstrate key resiliencies against potential attacks such as ephemeral secret leakage and privileged insiders.
4) We analyze system computation and communication costs using two significant cases to exhibit the salient features of the proposed AID-PPKAF compared to other state-of-the-art approaches.
5) We conduct a quantitative analysis of chain-based IoMT using NS3 to analyze the functional attributes of the proposed AID-PPKAF and other relevant schemes.
6) Finally, we show a pragmatic study using SVM to validate the behavior of the proposed AISec with PPKAF and other relevant schemes in a real-world scenario. Moreover, the proposed AISec

is aimed at optimizing identity verification using a more reliable privacy-preserving system.

C. Structure of the Paper

The paper's sections are organized as follows. Section II considers forensic medicine and various key agreement techniques in order to discuss security weaknesses and key challenges. Section III deliberates the key primitives of the proposed mechanism to signify its relevance to state-of-the-art approaches. Section IV presents the phases of AID-PPKAF using elliptic curve cryptography and the physically unclonable function. Section V discusses the security analysis (both formal and informal), demonstrating proof of resiliency against potential attacks. Section VI presents a performance analysis of comparative features, such as computations and communications by AID-PPKAF and other schemes. Additionally, it covers a pragmatic study expressing the importance of an AI-driven approach, testing the robustness of the authentication mechanism in real-time. Section VII concludes the research, proposing future directions for the study.

II. Related Work

The applications of the IoMT demand a few general requirements from WMSNs, such as data integrity, availability, nonrepudiation, mutual authentication, security, and privacy, to preserve the sensitive information of patients. Of late, the cloud healthcare infrastructure (CHI) has operated various service paradigms (artificial intelligence, cyber-physical systems, multi-access edge computing) to drive the technical features of extensive information processing systems, such as mobility support and device heterogeneity. A CHI can even exploit key features of the IoMT to interoperate healthcare domains and transmit quality data. However, network interconnectivity is susceptible to severe DDoS attacks. Therefore, this section discusses various key agreement techniques of the IoMT, including multi-factor, lightweight, biometric, and anonymous-based authentication relating to FA-CPS to address their associated drawback.

Wazid et al. [30] designed a blockchain model to secure communications in a drone-aided healthcare environment. They utilized an effective key management technique to analyze a system parameter and demonstrate its performance efficiency. Camara et al. [31] reviewed privacy and security issues in networking environments to discuss the risks associated with implantable medical devices. Challa et al. [32] studied various authentication protocols to conduct a rigorous analysis of functional features, computations, storage, and communication costs. Also, they discovered a taxonomy to highlight the significance of various biometric-based, knowledge-based, and possession-based authentication mechanisms. Wang et al. [24] introduced fog-based access control to achieve high-level security in the IoMT environment. They used fine-grained data access to stimulate a control framework with fog computing.

However, in that framework, important security properties such as mutual authentication, secret key agreement, and perfect secrecy are not provided to determine the level of system security. Garg et al. [33] presented a blockchain-enabled authentication (B-EA) protocol to protect transmissions by a patient-centric system. This protocol utilizes a distributed ledger of transactions to store and access the data from a cloud server. Moreover, it can prevent unauthorized data access, withstanding various attacks such as device impersonation, privileged insider, and password guessing. Merabet et al. [23] employed machine-to-machine and machine-to-cloud authentication strategies to fulfill the essential requirements of healthcare applications. Unfortunately, their strategies did not use a dynamic addition phase for mobile devices and gateway controllers to provide device connectivity and data processing.

Kim et al. [25] employed a multi-level authentication technique (M-LAT) to resist keystroke-logging attacks. The technique applies biometric technologies to convert the behavioral characteristics of any individual into digital form, which enables the authentication system to strengthen device security. Kang et al. [26] developed low-cost batch authentication (LC-BAuth) that handles bulk tags, with a dedicated tag manager to identify illegal tags and minimize transmission overhead. They preferred batch certification with high-level security to improve system efficiency in the IoMT. Kumar et al. [22] structured a lightweight authentication (LAuth) scheme to deal with the significant features of healthcare infrastructure, including content authentication and key agreement. This scheme did not keep system parameters in a cloud database to resist potential threats such as stolen verifiers, parallel sessions, and replay attacks.

Deebak and Al-Turjman [27] designed seamless authentication (SAuth) for healthcare applications using the IoMT. However, their scheme incurs more computation and communication costs to offer mutual authentication and secret key agreements. Jan et al. [28] proposed robust and lightweight authentication (RLAuth) for network-enabled healthcare applications. They use data broadcasts in conjunction with lightweight security features to assess internal storage information and resist potential vulnerabilities, such as identity guessing and stolen verifiers. Khan et al. [29] applied anonymous-based authentication (A-Auth) to preserve user privacy and withstand server impersonation and password-guessing attacks.

Seifelnasr et al. [34] utilized a strategy of forward secrecy to construct an effective privacy preserving (EPP) protocol that eliminates the process of cloud administration during device authentication requests. Liu et al. [35] applied the elliptic-curve and Paillier algorithm to design a novel privacy preserving with proper reputation updating (PP-PRU). The designed protocol uses a trusted authority to collect the reputation feedback of users in prior in order to reduce cost efficiencies, including computation and communication. Saleem et al. [36] adopted a hashing technique to devise a privacy preserving key agreement protocol (PP-KAP) with secure transmission and lightweight operation. The devised protocol has a proper formal analysis to show its resilience against vulnerabilities such as key impersonation and password guessing. Al Sibahee et al. [37] formulated an efficient privacy preserving authentication with a two-factor strategy (PPA-2F) to analyze the deployment scenario of forgery-resistant PUF technology.

The designed scenario shows that their strategy can mask the real identities of the devices to preserve the security parameters against conventional attacks such as side-channeling and privileged-insider. However, the above existing schemes [28], [29], [34]–[37] fail to incorporate the significant parameters such as timestamp and random nonce during the exchange of authentication request to analyze the security level of a derived session key, and thus cannot protect the end devices against traceability attacks. Table I summarizes the key issues with existing authentication schemes in the IoMT. To fulfill the essential features of a CHI, including security and privacy, this paper constructs an authentication protocol using data analytics.

III. Preliminaries

This section discusses the key primitives of the proposed AID-PPKAF, such as mathematical assumptions plus network and threat models, signifying its appropriateness for resource-constrained IoMT environments.

TABLE I: Key Challenges of Existing Authentication Schemes in IoMT with Security Factors

Existing Scheme	Description	Technique Used	Security Factors				
			KP_1	KP_2	KP_3	KP_4	KP_5
Wang et al. [24]	High-level privacy-aware mechanism using fine-grained access control to secure large volumes of cloud data	Privacy Time Optimization	No	No	No	No	No
Merabet et al. [23]	Efficient lightweight authentication for M2M and M2C healthcare applications	Privacy Time Optimization	Yes	No	No	No	No
Kim et al. [25]	Multi-level authentication to strengthen device security and guarantee data integrity	Hash-based Mutual Authentication	No	No	No	No	No
Kang et al. [26]	Enhanced RFID-based authentication using homogeneous linear equations to minimize tag costs and patient expenses	Batch Authentication and Per-tag Protocol	Yes	No	No	No	No
Kumar et al. [22]	Lightweight authentication using elliptic curve cryptography to achieve security features in a cloud healthcare infrastructure	Key Agreement and Cloud Healthcare Infrastructure	Yes	No	No	No	No
Deebak and Al-Turjman [27]	Smart service authentication to analyze common features of session keys among communication entities	Secret Session Key and Mutual Authentication	Yes	No	No	Yes	Yes
Jan et al. [28]	Robust and lightweight authentication to address the security issues associated with patient monitoring systems	Public-Private Key Pair and Cryptographic Hash Derivatives	Yes	No	No	No	Yes
Khan et al. [29]	Privacy-preserving authentication to gain cloud access remotely without compromising performance	Three-Factor Authentication and Key Agreement	Yes	Yes	Yes	Yes	No

KP_1 - Mutual Authentication; KP_2 - Secret Key Agreement; KP_3 - Stolen Verifier; KP_5 - Password Guessing; and KP_5 - Privileged Insider

A. Mathematical Assumptions

To minimize bandwidth usage, communication systems use public key cryptosystems of different key sizes, i.e., the ratios for ECC and Rivest–Shamir–Adleman (RSA) shown in Table II. It is also worth noting that ECC uses a small key size to offer a high level of security, whereas other cryptographic algorithms use a large key size to achieve such a degree of assurance. Therefore, this paper prefers ECC to secure data transmissions and improve computation and communication efficiencies. Significantly, this paper applies physically unclonable functions to generate a random function where it is simply hard to obtain a specific output without accessing a real object.

1) ECC Background: Let E define an elliptic curve over the prime field of a finite order, F_q, where q is a large prime integer. An expression of the elliptic curve over F_q can be stated with $x^2 = y^3 + \alpha.y + \beta \pmod q$ where $\alpha, \beta \in F_q$. Also, the given expression is declared nonsingular in the case of $4.\alpha^3 + 27\beta^2 \pmod q \neq 0$. An interesting property of the elliptic curve is an additive group, G, which typically shows the set of points on a curve as $G = \{(x,y) : x,y \in F_q(x,y) \in E\} \cup \{\emptyset\}$ where $\emptyset$ is the asymptotic point to find zero elements in G.

TABLE II: Different Key Sizes for ECC and RSA

ECC Size (bits)	RSA Size (bits)	Size Ratio	Cost Ratio
163	1024	1:6	1:3
256	3072	1:12	1:10
384	7680	1:20	1:32
512	15360	1:30	1:64

Suppose group operation G has the following assumptions [38].

The Elliptic Curve Computational Diffie-Hellman Problem (EC-CDHP): If g is the generator of an additive group G, and the computation of $\alpha.g$ and $\beta.g$ are supplied with system parameters $\{g, \alpha.g, \beta.g\}$, then finding the computational value for $\alpha.\beta.g$ is hard.

2) PUF Background: The primitive of PUF hardware agrees to receive a challenge C, and generates its equivalent matching response R from the physical properties of chip C and the integrated circuit (IC). A one-way function $R = PUF(C)$ is worked out for the PUF of challenge C, and response R is said to be a bit string.

In particular, PUF security reveals that various ICs may use a similar fabrication process; however, each IC has its own production variance to simulate a unique response over the given inherent features. The random physical factors of the PUF are characterized as follows.

1) *Uniqueness* The PUF utilizes integrated circuits to generate unique identities, and thus, cannot be cloned or copied even by extracting or accessing units of the manufacturing process.
2) *Unidirectionality* Since the generated response for manufacturing units is fixed and unpredictable, any specific PUF module cannot find its appropriate one-way random function to map the input-output variance.
3) *Invulnerability* Tampering with the identity of the PUF device may cause serious changes in its behavior, which, as a result, will destroy its physical characteristics to ensure trustworthiness.

B. Network Model

Fig.1 shows a network model of the proposed AID-PPKAF to illustrate the significance of implantable medical devices. Medical devices such as gastric simulators and cardiac pacemakers continuously monitor electronic gadgets via application servers to collect sensitive data using wireless technologies, i.e., radio frequency identification, Bluetooth, and WiFi. Moreover, a cloud server uses a dedicated access point to store and analyze sensitive information processed by the application server. The communication parties (namely, the patient and medical experts) utilize smart computing devices to sense physiological data such as blood pressure, heart rate, respiratory rate, etc. To register medical devices and servers in real-time, a trusted authority is employed. Each user can gain access to the cloud server upon successful authentication.

In practice, each communication demands secure transmission using a session key to transmit sensitive data among the engaging parties. Since the cloud server has limited processing power and computation and storage capacities, in order to perform encryption, implantable devices prefer lightweight cryptographic operations to exchange health-related records. Additionally, to authorize data access to a cloud server, medical devices with limited resources utilize a data analytics phase. To predict a health condition, specialized systems,

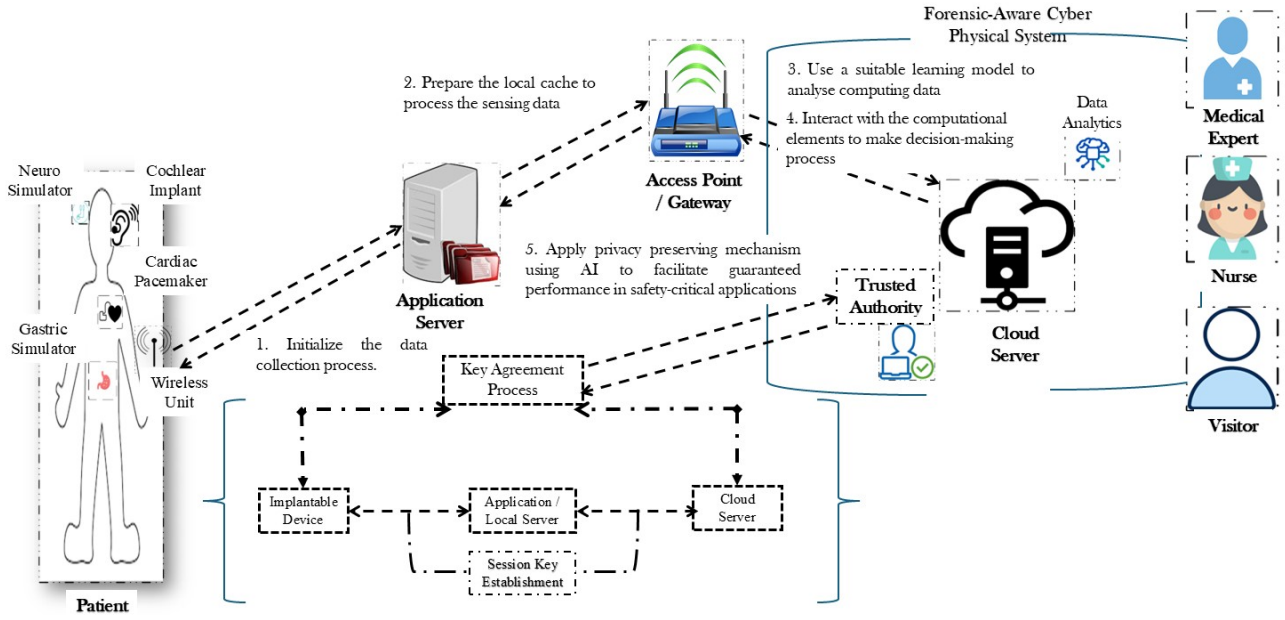


Fig. 1: Network Model of the Proposed AID-PPKAF.

i.e., FA-CPS, collect, analyze, and interpret medical data via security intelligence during the registration and authentication processes. Therefore, this paper constructs a privacy-preserving mechanism using AI to assess and improve the scientific principles, including drug treatment and discovery, and the prediction of suspicious activities.

C. Threat Model

The proposed AID-PPKAF utilizes Dolev-Yao (DY) and Canetti-Krawczyk (CK) guidelines to design a threat model characterizing the capabilities of compromising the session key information. Under DY-CK, real-time entities such as implantable devices, users, and application servers are untrusted objects that always attempt to establish communication over an insecure channel. As a result, adversary A_{dv} may exploit a few significant key parameters of the entities to modify, overhear, or delete shared messages. Additionally, this paper considers the DY-CK model as a de facto standard for examining authentication and KAP phases. The CK model has the same abilities as the DY-CK model to imitate the behavior of random adversaries. Random adversaries can successfully launch various potential attacks, such as device impersonation, replay, and man-in-the-middle, against the provably secure key agreement framework in order to extract confidential information reserved by real-time entities. Moreover, A_{dv} may even compromise system parameters or session states to capture or deduce storage information on implantable devices.

On the other hand, A_{dv} may apply a sophisticated attack like power analysis to infer sensitive information in the storage device. Later, A_{dv} may use the tampered-with information to perform various malicious activities, namely, session key computation and guessing session keys. Therefore, in this paper, a trusted authority, T_A, is a legal entity to secure key properties, such as session key security, user anonymity, and mutual authentication, because it is assumed to be uncompromised. Similarly, a cloud server is viewed as a semi-trusted entity of the given network to enable the execution of data analytics.

D. Analytical Model

This proposed AISec not only monitors the non-intrusive behavior of users but also verifies robust feature sets of users to build a reliable authentication model [39]. As a result, the authentication model can be more feasible in fulfilling the key constraints of a real-time environment (like prediction accuracy). The main objectives are as follows.

- Formulate a data acquisition procedure that gathers user activities transparently without excessive computational overhead.
- Discover a relevant key feature set to verify user behavior via smart computing devices that assess user behavior to authenticate the legitimacy of a user profile.
- Monitor session establishment to check the efficiency of pre-built user profiling that detects session hijacking of a legitimate user.
- Carry out identity verification from data acquisition to handle the feature extraction process, whereby the accuracy of the authentication process cannot be compromised.
  - In particular, feature extraction involves mining technologies to analyze the relevant processes of the computing devices transmitted via a dedicated network.
  - To achieve a scalable and accurate solution, a complex process uses ad hoc computing that focuses on behavioral features of the authentication mechanism to analyze the feasibility of parallel and distributed environments.

IV. Proposed AID-PPKAF Scheme

This section highlights the significance of the proposed privacy-preserving method to guarantee data integrity. To ensure key factors of security, AID-PPKAF includes registration, login, and authentication and key establishment, dynamic device addition and verification, and service-ware analytics. In AID-PPKAF, the implantable device I_{MD} and application server App_S successfully register with service-ware analytics SW_A to establish secure communications. Table III defines the notations used for AID-PPKAF.

Similarly, App_S and C_S utilize the timeliness property to compute and verify the session key during the authentication phase via the

dedicated access gateway A_G by using three-factor authentication (3FA). The descriptions of the execution phases are as follows:

- *Registration* generates the system parameters to initialize the local instance, which preserves the connection information of the server to manage the console applications.
- *Login and Authentication and Key Establishment* confirm user identities before accessing profiles from the integrated IT center via registered application server App_S, which generates a login request to verify the identity of the user and to establish secure communications using the challenge-and-response method.
- *Dynamic I_{MD} Addition* accesses cloud server C_S to inspect user identities via A_G to build a dynamic device collection that validates session key agreement with the device in order to exchange message transmissions with other authentic I_{MD} devices.
- *Service-ware Analytics* is when either I_{MD} or App_S builds a flexible software platform to adopt intelligent functions that mainly focus on decision-making and control processes to analyze data transmissions via C_S.

TABLE III: Important Notations Used in AID-PPKAF

Parameter	Description
A_{dv}	Adversary
I_{MD}	Implantable Device
App_S	Application Server
SW_A	Service-Ware Analytics
C_S	Cloud Server
G_A	Gateway Access
UR_{req}	User Registration Request
U_{UID}	Unique User Identity
HI	Healthcare Institute
Sys_{Admin}	System Administrator
D_M	Device Memory
C_H	Challenge
R_P	Response
s_k	Secret Key
U_D	User Device
x_p, y_p,x_a, y_a	Random Key Values
Sys_{Admin}	System Administrator
$h(.)$	Secure One-Way Hash Function
$\oplus$	Bitwise Ex-OR Operation
$\|\|$	Concatenation Operation
$<g>$	Multiplicative Cyclic Group Order N
g, g^t, and g^k	Cyclic Group

A. Registration Phase

The steps involved in the execution phases are as follows.

*1) **User Device Registration in Cloud Server** C_S:* Entities such as medical experts, nurses, and visitors who wish to access a medical network on the IoT must register their credentials via the healthcare institute (as shown in Fig.2). Execution is as follows.

Step 1: User device U_D generates message request $Mg^1_{UD} = (UR_{req} \parallel U_{UID})$, which has user registration request UR_{req} and unique user identity U_{UID} provided by HI, before delivering it to the system administrator, Sys_{Admin}. It is worth noting that entities such as U_D and Sys_{Admin} access a secure communication network to complete the registration process using a unique input-output pair $R = PUF(C)$, where R defines *Response* and C defines *Challenge*.

Step 2: Sys_{Admin} validates the message request processed by U_D and generates a valid U_{UID} to reserve it in the device's memory, D_M. Accordingly, Sys_{Admin} initiates a prompt challenge, C_H, to the PUF of U_D.

Step 3: U_D generates a valid response, R_P, with the help of I_{MD} in order to register the identities in App_S and C_S via G_A. To select an authentic secret key, s_k, App_S generates

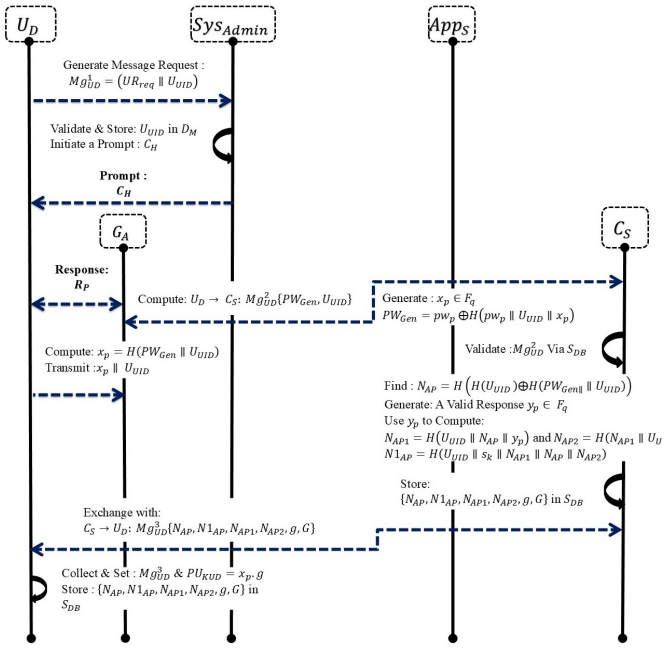


Fig. 2: Registration Process :($U_D \rightarrow C_S$).

a random number, $x_p \in F_q$. Subsequently, App_S generates $PW_{Gen} = pw_p \oplus H(pw_p \parallel U_{UID} \parallel x_p)$ to transmit message request $U_D \rightarrow C_S : Mg^2_{UD}\{PW_{Gen}, U_{UID}\}$ via A_G. Additionally, U_D computes $x_p = H(PW_{Gen} \parallel U_{UID})$ and transmits $x_p \parallel U_{UID}$ to Sys_{Admin} to protect the security parameters embedded in PUF-based cyber-physical systems.

Step 4: After obtaining request Mg^2_{UD}, C_S validates the credentials of U_D, including PW_{Gen} and U_{UID}, in server database S_{DB}. If the validation is unsuccessful, then C_S finds $N_{AP} = H(H(U_{UID}) \oplus H(PW_{Gen} \parallel U_{UID}))$ to generate a valid random number, $y_p \in F_q$. Additionally, C_S uses the value of y_p to compute $N_{AP1} = H(U_{UID} \parallel N_{AP} \parallel y_p)$, $N_{AP2} = H(N_{AP1} \parallel U_{UID} \parallel N_{AP})$ and $N1_{AP} = H(U_{UID} \parallel s_k \parallel N_{AP1} \parallel N_{AP} \parallel N_{AP2})$, and stores the computation values, $\{N_{AP}, N1_{AP}, N_{AP1}, N_{AP2}, g, G\}$, in S_{DB}. Finally, the parameters are exchanged with $C_S \rightarrow U_D : Mg^3_{UD}\{N_{AP}, N1_{AP}, N_{AP1}, N_{AP2}, g, G\}$. Notably, we adopt the operative features of PUF to prevent unauthorized access and to protect sensitive information stored in any cyber-physical system.

Step 5: Upon collecting message Mg^3_{UD}, U_D sets its public key, $PU_{KUD} = x_p.g$, and stores the parameters, $\{N_{AP}, N1_{AP}, N_{AP1}, N_{AP2}, g, G\}$, in S_{DB}.

*2) **Application Server Registration in Cloud Server** C_S:* App_S accesses trusted authority T_A to regulate the registration process of App_S via G_A, which operates the key distribution center to ensure secure U_D communications (as shown in Fig. 3).

Step 1: App_S uses T_A to select a unique identity, UD_{APP_i}, which computes $RUD_{APP_{S_j}} = H(UD_{APP_i} \parallel k_{T_A} \parallel k_{APP_{S_j}})$ to find the pseudo-identity of App_{S_j}, where UD_{APP_i} is the unique identity of App_S, k_{T_A} is the secret key of T_A, and $k_{APP_{S_j}}$ is the secret key of APP_{S_j} Subsequently, T_A finds zone number $Z_{APP_{S_j}}$ for App_{S_j}.

Step 2: To register App_S with C_S, T_A generates a key input, App_{SID}, to compute the message request, $App_S \rightarrow C_S : Mg^1_{App_S} = \{App_{SID}, UD_{APP_i}, k_{T_A}, k_{APP_{S_j}}\}$

Step 3: After collecting request $Mg^1_{App_S}$, C_S verifies the parameters, i.e., $App_{SID}, UD_{APP_i}, k_{T_A}$, and $k_{APP_{S_j}}$, with S_{DB}. If verifica-

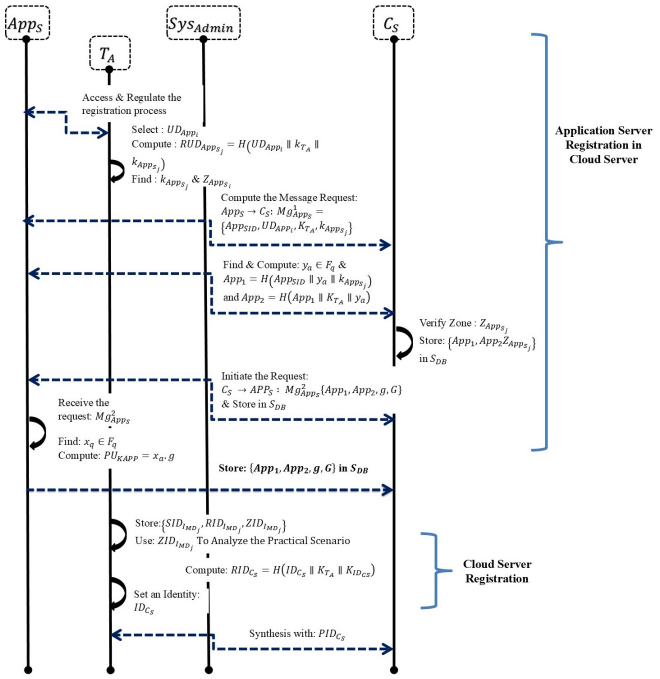


Fig. 3: Registration Process :($App_S \rightarrow C_S$).

tion is unsuccessful, then C_S finds a random number, $y_a \in F_q$, to compute $App_1 = H(App_{SID} \| y_a \| k_{APP_{S_j}})$ and $App_2 = H(App_1 \| k_{T_A} \| y_a)$. Lastly, C_S verifies zone number $Z_{APP_{S_j}}$ to store the parameters, $\{App_1, App_2, Z_{APP_{S_j}}\}$, in S_{DB}, which can initiate message request $C_S \rightarrow App_S : Mg^2_{App_S}\{App_1, App_2, g, G\}$ via T_A.

Step 4: After receiving request $Mg^2_{App_S}$, App_S finds a random value, $x_a \in F_q$, to compute public key $PU_{KAPP} = x_a.g$. Lastly, C_S stores the system parameters, $\{App_1, App_2, g, G\}$, in S_{DB}.

Step 5: Additionally, T_A stores the system parameter values $\{SID_{I_{MD_j}}, RID_{I_{MD_j}}, Z_{I_{MD_j}}\}$, where $SID_{I_{MD_j}}$ is the set timestamp value of I_{MD_j}, $RID_{I_{MD_j}}$ is the temporarily reset timestamp of I_{MD_j}, and $Z_{I_{MD_j}}$ is the zone number of I_{MD_j} in the memory of I_{MD_j} before the time of its deployment in any practical scenario.

*3) **Cloud Server Registration**:* Trusted authority T_A executes C_S registration as follows.

Step 1: T_A sets a unique identity, ID_{C_S}, to find the pseudo-identity of C_S, i.e., $RID_{C_S} = H(ID_{C_S} \| k_{T_A} \| k_{ID_{C_S}})$, where $k_{ID_{C_S}}$ is the secret key of C_S.

Step 2: After obtaining the value for PID_{C_S}, T_A synthesizes the system parameters in the C_S cache before its deployment in any practical scenario.

B. Login, Authentication, and Key Establishment

U_D communicates with I_{MD} to regulate the operation of medical records in App_S, which utilizes C_S via A_G to establish a secure session key as shown in Fig.4. The execution phase is as follows.

Step 1: U_D initializes login credentials such as $U^{'}_{UID}$ and $pw^{'}_p$ via App_S to compute $PW^{'}_{Gen} = pw^{'}_p \oplus H(pw^{'}_p \| U^{'}_{UID} \| x_p)$ and $N^{'}_{AP} = H(H(U^{'}_{UID}) \oplus H(PW^{'}_{Gen} \| U^{'}_{UID}))$ and verifies the parameters, i.e., $N^{'}_{AP} = N_{AP}$.

Subsequently, U_D finds random number $x \in F_q$ to compute $\alpha = x.g$ to insert medical data $M_D = (U_{UID}, Pt_{Data})$ and compute signature verifier $Sig_{UD} = S_{SK_{UD}}(H(M_D))$.

On obtaining the signature verifier, U_D finds two significant values, i.e., $V_1 = H(H(U_{UID} \| PU_{KUD} \| U_{UID} \oplus SID_{I_{MD_1}})$ and $V_2 = H(N_{AP} \| N1_{AP} \| U_{UID})$, to encrypt $EN_1 = EN_{H(U_{UID} \| N_{AP1} \| N_{AP2})}(V_1, M_D, \alpha, Sig_{UD}, SID_{I_{MD_1}})$ using key value $H(U_{UID} \| N_{AP1} \| N_{AP2})$. Lastly, $U_D \rightarrow C_S : Msg_1 = \{EN_1, V_2, TS_1\}$ is processed for verification with C_S via App_S.

Step 2: C_S verifies the credentials of U_D, such as $U^{'}_{UID}$ and $pw^{'}_p$, via G_A to locate the pseudo-identity of C_S, i.e., RID_{C_S} via $Z_{APP_{S_1}}$.

Upon successful verification, G_A selects corresponding parameters C_H and R_P and generates a random nonce, x. To ensure self-reliance, G_A finds $\beta = C_H \oplus G_{s_k}$.

Furthermore, G_A computes $j = H(G_{s_k} \| R_P)$ to assist U_D in confirming mutual authentication with G_A. Then, $C_S \rightarrow U_D : Msg_2 = \{RID_{C_S}, x, \beta, j\}$ is transmitted to verify the system parameters with U_D via App_S.

Step 3: On obtaining message request Msg_2, App_S verifies timestamp $TS_2 - TS_1 \leq \Delta TS$ to validate the significant parameter, i.e., $V^*_2 \stackrel{?}{\Rightarrow} H(U_{UID} \| U_D \| x_p)$. Subsequently, App_S computes $UD_{APP_1} = UD_{App} \oplus H(App_1 \| U_{UID} \| U_D)$ and $V_3 = H(U_{UID} \| U_D \| N1_{AP} \| TS_3)$ to encrypt system parameter $EN_2 = E_{H(U_{UID} \| U_D \| N1_{AP})}(EN_1, V_3, UD_{APP_1}, App_1, App_2, x_p)$ using secret value $H(U_{UID} \| U_D \| N1_{AP})$.

App_S initiates a random number, $x_1 \in F_q$, with timestamp TS_3 to compute the message requests: $Msg_3 = x_1 \oplus H(SID_{I_{MD_j}} \| TS_3)$ and $Msg_4 = H(x_1 \| SID_{I_{MD_j}} \| TS_3 \| Z_{APP_{S_j}})$.

Step 4: On collecting message requests Msg_3 and Msg_4, U_D verifies timestamp $TS_3 - TS^*_3 \leq \Delta TS$ to compute $U^*_{UID} = U_{UID_1} \oplus H(Sig_{UD} \| M_D \| V_1)$. Additionally, U_D applies $H(N_{AP} \| N1_{AP} \| U_{UID})$ to decrypt $(U_{UID_1}, MAC_D, Sig_{UD}, M_D, \beta, TS_4) = DK_{H(Sig_{UD} \| M_D \| V_1)}(EN_2)$, which verifies $V_{U_D}(Sig_{UD}) = H(M_D)$. Lastly, U_D finds $MAC_D = H(U_{UID} \| U^{'}_{UID} \| x_p \| M_D \| TS_4)$ to verify the hardware address with $MAC_{UD} = MAC_D$.

Step 5: Furthermore, C_S checks timeliness TS_3 of App_S via G_A using $TS_3 - TS^*_3 \leq \Delta TS$ to verify whether TS^*_3 is the receiving timestamp of Msg_3 or not. If the timeliness of Msg_3 holds, then C_S instructs App_S via G_A to compute $H(R_P \| RID_{C_S}) = MAC_D \oplus H(RUD_{APP_{S_j}} \| Z_{APP_{S_j}} \| TS_1 \| TS_2), SK_{APP_{S_j}}), C_S) = H(H(R_P \| RID_{C_S}) \| RUD_{APP_{S_j}} \| Z_{APP_{S_j}} \| TS_1 \| TS_2)$ and $M^{'}_1 = H(SK_{APP_{S_j}, C_S} \| RUD_{APP_{S_j}} \| SID_{I_{MD_j}} \| TS_3)$.

Subsequently, App_S verifies message transmission $M^{'}_1 \stackrel{?}{\Rightarrow} M_1$ to establish secure communications with C_S via G_A. If verification holds, then App_S creates current timestamp TS_4 and computes $V_4 = H(SK_{APP_{S_j}, C_S}) \| TS_4)$.

Otherwise, App_S aborts communication with C_S. Then, App_S sends the computed values, $Msg_5 = \{V_4, TS_4\}$, to U_D via secure network.

Step 6: After collecting message request Msg_5 from C_S via App_S, U_D checks TS_4 using $TS_4 - TS^*_4 \leq \Delta TS$, where TS^*_4 represents the timestamp of Msg_4. If valid, then U_D finds $M^{'}_2 = H(SK_{APP_{S_j}, C_S} \| TS_4)$ to verify whether $M^{'}_2 \stackrel{?}{\Rightarrow} M_2$ holds or not.

If it holds, then U_D finds the computed session key with App_S is correct to successfully complete execution. Otherwise, U_D aborts communication with App_S. Finally, App_S and C_S utilize established session key $SK_{APP_{S_j}, C_S} = (SK_{C_S, APP_{S_j}})$ to secure message transmissions with U_D.

C. Dynamic I_{MD} Addition Phase

To offer device scalability or to resolve failure issues, adding a new computing device, i.e., I^{New}_{MD}, is dynamically set with a secret

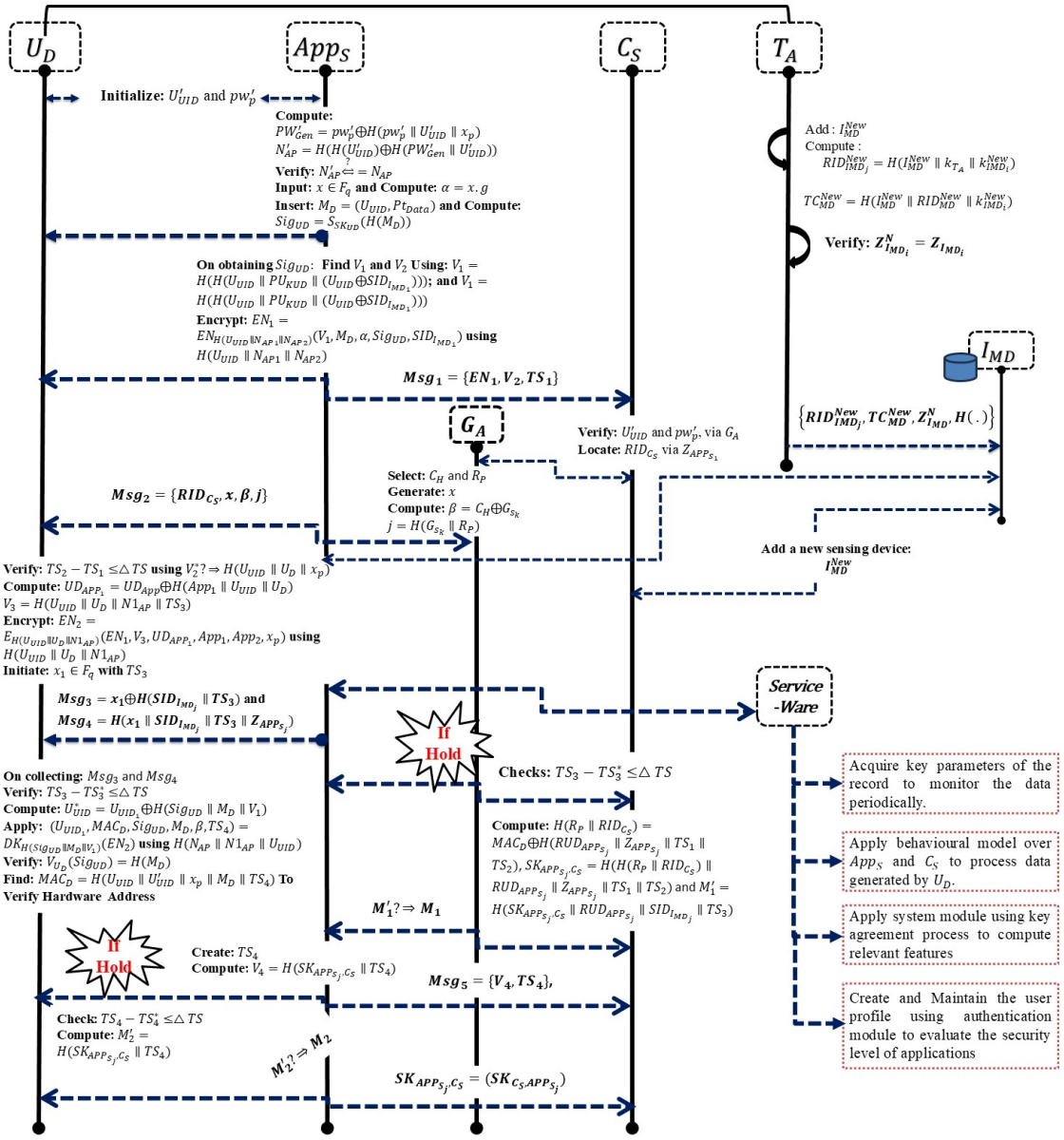


Fig. 4: Key Establishment Process: ($U_D \rightarrow App_S \rightarrow C_S \rightarrow$ via G_A and T_A).

key and unique pseudo-identity. T_A has the following steps to carry out the addition of I^{New}_{MD}.

Step 1: T_A selects a unique identity for the new computing device I^{New}_{MD}. Subsequently, it computes $RID^{New}_{IMD_j} = H(I^{New}_{MD} \| k_{T_A} \| k^{New}_{IMD_i})$ as the pseudo-identity of I^{New}_{MD}, where k_{T_A} and $k^{New}_{IMD_i}$ are the secret keys of I^{New}_{MD}.

Step 2: Additionally, T_A uses the temporal credentials of I^{New}_{MD} to compute $TC_{I^{New}_{MD}} = H(I^{New}_{MD} \| RID_{I^{New}_{MD}} \| k_{I^{New}_{MD}}$, where $RID_{I^{New}_{MD}}$ is the registration value of I^{New}_{MD}. Again, T_A uses temporal and zone numbers of I^{New}_{MD}, such as $TID_{I^N_{MD}}$ and $Z_{I^N_{MD}}$, respectively, to verify whether $Z^N_{I_{MD_i}} = Z_{I_{MD_i}}$ or not.

Step 3: On computing the above values, T_A keeps data such as $RID^{New}_{IMD_j}, TC^{New}_{I_{MD}}, TID^N_{I_{MD}}, Z^N_{I_{MD}}$, and $H(.)$ in the memory of I_{MD} before its deployment in any practical scenario. Moreover, T_A utilizes entities such as App_S and C_S to add a new computing device I_{MD} via the secure network. It is worth noting that a new App_S can be added to the network to process computing device I^{New}_{MD}.

D. Service-Ware Analytic Phase

AID-PPKAF focuses on continuous authentication to analyze the features of computing devices, such as data statistics, sensor information, and communication services. Implantable devices utilize the behavioral profile of users, such as patients or experts, to examine AID-PPKAF's authentication levels. Each device operates a hidden network pattern that maintains a large-scale application dataset to build a precise authentication system. To test the relevant data and extract the configuration parameters of the application, various computing strategies are applied using S_{DB}. It uses machine learning mechanisms such as the decision tree, logistic regression, and the support vector machine to examine authentication levels.

To obtain AID-PPKAF's viability, the AI-driven framework is utilized to evaluate the deployment of App_S and C_S via classifier mechanisms. The framework creates behavior profiles of users,

including patients and experts, to monitor and aggregate different sources of medical data, e.g., blood pressure, heart rate, and respiratory rate. The main execution phases are as follows.

Step 1: The smart device utilizes the components of I_{MD} to monitor and process the computation data carried out by the data acquisition module. It uses a timing window to configure different kinds of medical data, i.e., compiling electronic health records, and deploys connection modules such as App_S and C_S to define sensitive data in vector form.

Step 1.1: Acquire two key dimensions of the records, such as sensors and statistics, to monitor data periodically.

Step 1.2: Use a behavioral module over the time interval to collect medical data using connection modules such as App_S and C_S.

Step 1.3: Process the principal elements of the communication platform to store or process data generated by users.

Step 1.4: Apply a computing module using an authentication framework to verify the application data via T_A.

Step 2: Include system modules such as data sender and receiver to normalize the processing technique and gather the authentication levels of the users.

Step 3: Implement two basic components, such as preparation and aggregation, to process data vectors and to compute relevant features of the medical data.

Step4: Create the storage module to maintain the user profile and aggregate different forms of vector data, resulting in the preparation of the dataset.

Step 5: Maintain the behavior of the user profiles using authentication modules to analyze offline user models and evaluate authentication levels in real-time.

Step 6: Run the basic components in practice to train the server workload by using machine learning algorithms such as the decision tree, logistic regression, and the support vector machine to analyze the authentication levels of the applications.

To learn and improve the pattern features, the analytical phase foresees a few crucial outcomes from the authorized App_S and C_S. The execution phase includes data aggregation to train on and test diverse medical data, uncovering the hidden network pattern. As a result, the deployed AI executes the fundamental steps on the accumulated data to visualize and predict overall performance from the results.

V. Security Analysis

This section systematically analyzes the proposed AID-PPKAF to show proof of resiliency over potential attacks such as replay, man-in-the-middle, impersonation, ephemeral secret leakage, privileged insiders, etc.

A. Formal Security Proof

In this section, we show the formal security proof of the random oracle model (ROM) to demonstrate that the key assumptions of the proposed AID-PPKAF are provably secure under the DY-CK model. Suppose the key assumption holds Γ to represent a context-aware session key which makes the participant $\mathbf{P}$ to initialize two non-empty sets containing client data $c \in \mathbf{P}$ and server information $s \in \mathbf{P}$. Assume $\Gamma^i_{\mathbf{P}}$ represent the random oracle model to execute i^{th} instance of $\mathbf{P}$. Moreover, each instance draws an order of $N-$ elements to analyze a few security parameters such as hash value h_v and length of random integers r_l. To analyze the false positive rate, denoted by τ_{fpr}, the instance uses a generated private string p_{str}. Considering this, adversary A_{dv} can use the security features of the protocol to communicate with Γ and also applies a few executable queries to obtain s response. As a result, A_{dv} obtaining the s response can process send query q_{snd}, hash oracle q_{hah}, and query execution q_{ext} to generate a proposed key agreement $\mathbf{A}^{PPKAF}_{EC-CDHP}$.

To assess the query response executed by A_{dv}, the challenger C_H may exploit the sensitive parameters of $\mathbf{A}^{PPKAF}_{EC-CDHP}$, whereby C_H can execute the proposed AID-PPKAF to perform the following queries.

- **Setup** $(\Gamma^i_{\mathbf{P}}, m_{sg})$**:** In order to obtain the query response, C_H obtains s_k and other sensitive parameters of C_S and I_{MD}.
- **Execute** (Γ^i_c, Γ^i_s)**:** Using this query, A_{dv} simulates its passive attack which makes c and s to establish a secure communication over i^{th} instances via a proper execution of oracle model. Moreover, each instance carries out the queries of A_{dv} to provide interactive information.
- **Send** $(\Gamma^i_{\mathbf{P}}, m_{sg})$**:** Initially, C_H sends a transmitted message m_{sg} to $\Gamma^i_{\mathbf{P}}$. $\mathbf{P}$ utilizes the parameters of m_{sg} in compliance with the specification of $\mathbf{A}^{PPKAF}_{EC-CDHP}$, including per-session state, updates the state information, and outgoing transmitted message $m^{'}_{sg}$. Lastly, the **Send** query uses A_{dv} to initiate the execution of $\mathbf{A}^{PPKAF}_{EC-CDHP}$.
- **Reveal** $(\Gamma^i_{\mathbf{P}})$**:** A_{dv} can use the session key of $\mathbf{P}$ to establish a secure communication. Moreover, each instance tries to obtain the successful key establishment $\Gamma^i_{\mathbf{P}}$ in order to return its k^{th} instance, i.e., $\Gamma^i_{\mathbf{P}}.k$.
- **Corrupt** $(\mathbf{P})$**:** Using this query, $A-dv$ can obtain the long-term secret key information of $\mathbf{P}$ to read the computing data of I_{MD}.
- **Test** $(\Gamma^i_{\mathbf{P}})$**:** This query applies semantic security of $\mathbf{A}^{PPKAF}_{EC-CDHP}$ protocol to test whether A_{dv} can uses its query instance to derive its session key SK or not via a random hidden bit $r_h \in \{0,1\}$. In the case of deriving a bit $r_h = 1$, A_{dv} proves that it has k^{th} iteration of its query process to return SK. Otherwise, the query instance returns the random value of the related key size with the appropriate SK.

The security of the proposed AID-PPKAF can express its probability to distinguish the query instances of A_{dv} in order to exploit its key parameters, such as uniform r_i and SK. Moreover, the exploited instances execute numerous Oracle queries to Γ to gain the probability P_r. As a result, the proposed $\mathbf{A}^{PPKAF}_{EC-CDHP}$ utilizes its key indistinguishability K_{ID} to achieve the probability of occurrence through proper challenges C_H, representing as $\mathbf{A}^{PPKAF}_{EC-CDHP}[A_{dv}] = |P_r[Guess_i] - \frac{1}{2}|$ where $Guess_i$ is an event occurrence to guess an appropriate instance correctly using security game sg_i. By the above information, we derive the below theorem with genuine analysis, and they are as follows.

Theorem 1. Considering any polynomial adversary $A-dv$, let us assume n_{snd}, n_{ext}, and n_{hah} are the number of send, execute, and hash queries of the Oracle model to define the size of password dictionary deriving by A_{dv}. Hence, the probability gain of the adversarial act in violating the security of the proposed AID-PPKAF can be expressed as follows.

$$\mathbf{A}^{PPKAF}_{EC-CDHP}[A_{dv}] \leq \frac{q^2_{hah}+(q_{snd}+q_{ext})^2}{2^{r_l}} + \frac{(q_{snd}+q_{ext})^2}{(n_p-1)} + \frac{(2q_{hah}+3q_{snd})}{2^{r_1-1}} + 2max\{q_{snd}(\tau_{fpr}, \frac{1}{N}), \frac{1}{p_{str}}\} \quad (1)$$

Proof. To assess the security features of $\mathbf{A}^{PPKAF}_{EC-CDHP}$, we formulate eight consecutive games from $Game_0$ to $Game_7$. In the game modeling, $Success_i$ represents the possibility of A_{dv} accurately estimating the guessing bit g_b during the session connectivity to probe the game modeling $Game_i$. In this case, A_{dv} claims to learn

the credentials of c, i.e., U_{UID}, by itself, and thus does not require realizing its guessing bit g_b as stated in the key agreement process.

$Game_0$**:** In this modeling, we initiate an original game to simulate the game theory process via A_{dv}, which makes the entities c and s establish an interactive session using the source attributes of $\mathbf{A}_{EC-CDHP}^{PPKAF}$. As a result, in $Game_0$, we specify the occurrence of guessing bit $g_b^{'}$ over A_{dv} to gain the probability defining the upper bound to terminate or abort the response processed by A_{dv}.

$$\mathbf{A}_{EC-CDHP}^{PPKAF}[A_{dv}] = 2P_r[Success_0] - 1 \tag{2}$$

$Game_1$**:** In this process, A_{dv} uses an eavesdropping attack to extract the source attributes of the proposed $\mathbf{A}_{EC-CDHP}^{PPKAF}$ including $\{EN_1, V_2, TS_1\}$, $\{RID_{C_S}, x, \beta, j\}$, $Msg_3 = x_1 \oplus H(SID_{I_{MD_j}} \parallel TS_3)$, and $Msg_4 = H(x_1 \parallel SID_{I_{MD_j}} \parallel TS_3 \parallel Z_{APP_{S_j}})$. As a result of this, A_{dv} has the possibility of intercepting the transmitted messages using q_{ext} to determine whether the key attributes such as SK and r_i are authentic or not using *Reveal* and *Test* queries. These queries prefer to assess the features of the proposed $\mathbf{A}_{EC-CDHP}^{PPKAF}$ i.e., $SK_{APP_{S_j},C_S} = (SK_{C_S,APP_{S_j}})$ to intercede the message transmission. In contrast, A_{dv} exploits the relevant source parameters, i.e., r_i where i=1,2,3,... to probe the genuineness of SK. However, A_{dv} cannot be aware of any random integers r_i to validate the session establishment with the communication entities, including I_{MD}, App_S, and C_S. At the end of this, A_{dv} cannot have any chance of winning the probability of $Game_1$ to intercept the secure communication or fabricate the transmitted messages. Thus, the modeling process $Game_0$ and $Game_1$ cannot be changed until any source attribute is realized by A_{dv}. Then, we can specify $P_r[Success_1]$ as follows:

$$P_r[Success_1] = P_r[Success_0] \tag{3}$$

Most importantly, we have a list of stored parameters to analyze the query modeling, which corresponds to

1) $\mathcal{L}_{\mathcal{A}^{\lceil\sqsubseteq}}$ uses hash query q_{hah} to generate system response.
2) $\mathcal{L}_{\mathcal{P}\nabla^{\wr}}$ saves the generated transcripts during the authentication procedure to validate the query response.

$Game_2$**:** Using active probing, this modeling process simulates the attacks via A_{dv} to analyze the behavior of q_{hah} query. The query function applying using $h(.)$ protects the source attributes of the proposed $\mathbf{A}_{EC-CDHP}^{PPKAF}$ i.e., $V_1 = H(H(U_{UID} \parallel PU_{KUD} \parallel U_{UID} \oplus SID_{I_{MD_1}})$ and $V_2 = H(N_{AP} \parallel N1_{AP} \parallel U_{UID})$, and $EN_1 = EN_{H(U_{UID} \| N_{AP1} \| N_{AP2})}(V_1, M_D, \alpha, Sig_{UD}, SID_{I_{MD_1}})$ to find an authentic SK. Moreover, because of collision resistance $h(.)$, the security parameters $\{EN_1, V_2, UD_{APP_1}, V_3\}$ utilize a few arbitrary r_i to secure the message transmission among the real-time entities I_{MD}, C_S, and App_S. Moreover, the involved parameters are computationally infeasible since there is no existence of collision issuing q_{ext} to examine the probability of guessing bit g_b. Exclude the integration of query q_{hah} in $Game_2$, $Game_1$ is quietly equivalent. While applying the *birthday paradox*, we obtain the below desirable result:

$$|P_r[Success_2] - P_r[Success_1]| \leq \frac{(q_{hah}^2 + (q_{snd} + q_{ext})^2)}{(2^{r_i+1})} + \frac{(q_{snd} + q_{ext})^2}{2(n_q - 1)} \tag{4}$$

$Game_3$**:** In this modeling, we exploit the following queries *Corrupt* and *Send* to simulate the power analysis attacks. This makes A_{dv} to find the key attributes of the proposed $\mathbf{A}_{EC-CDHP}^{PPKAF}$ i.e., $\{N_{AP}, g, G, SK_{APP_{S_j}}, RUD_{APP_{S_j}}\}$ which derive a reliable secret key s_k to obtain a context-aware SK. As a result, we firmly believe that A_{dv} cannot guess a legitimate password to operate various vulnerabilities in the consumption pattern of smartcards. In other words, $Game_2$ and $Game_3$ are imperceptible due to the lack of password guessing, including credential stuffing and dictionary attacks, to gain system access. Hence, we obtain the following expression:

$$|P_r[Success_3] - P_r[Success_2]| \leq \frac{(2q_{hah} + 3q_{snd})}{2q^{(r_i - 1)}} \tag{5}$$

$Game_4$**:** This modeling considers a data forging attack to analyze the features of the proposed $\mathbf{A}_{EC-CDHP}^{PPKAF}$, i.e., $\{EN_1, V_3, UD_{APP_1}, App_1, App_2, x_p\}$. Moreover, it makes A_{dv} to operate $V_2^* \stackrel{?}{\Rightarrow} H(U_{UID} \parallel U_D \parallel x_p)$, $UD_{APP_1} = UD_{App} \oplus H(App_1 \parallel U_{UID} \parallel U_D)$, and $V_3 = H(U_{UID} \parallel U_D \parallel N1_{AP} \parallel TS_3)$ to authenticate the service requests processed by the real-time entities I_{MD}, C_S, and $App_S \in \mathcal{L}_{\mathcal{P}\nabla^{\wr}}$. In case the authentication requests are terminated due to insufficient security features, the successful probability of q_{hah} (i.e., $\frac{q_{hah}}{2^{r_i}}$ and $\frac{q_{snd}}{2^{r_i}}$) is as follows.

$$|P_r[Success_4] - P_r[Success_3]| \leq \frac{(2q_{hah} + 3q_{snd})}{(2^{r_i} - 1)} \tag{6}$$

$Game_5$**:** The possibility of forging the transmitted messages Msg_3 and Msg_4 explore the significant features of the proposed $\mathbf{A}_{EC-CDHP}^{PPKAF}$ using *Send* query to determine whether $M_2^{'} \stackrel{?}{\Rightarrow} M_2$ and $App_S \in \mathcal{L}_{\mathcal{P}\nabla^{\wr}}$ obtain their evaluation criteria or not. Without proper evaluation, the random oracle model cannot issue q_{snd} queries to terminate its execution process. Thus, we derive:

$$|P_r[Success_5] - P_r[Success_4]| \leq \frac{2q_{snd}}{2^{r_i}} \tag{7}$$

$Game_6$**:** In this game modeling, the possibility of forging the messages uses Msg_5 to check whether $M_2^{'} = H(SK_{APP_{S_j},C_S} \parallel TS_4)$ verifies the computed session key with App_S or not. Moreover, the simulator explores $M_1^{'} \stackrel{?}{\Rightarrow} M_1$ and $V_4 = H(SK_{APP_{S_j}}, C_S) \parallel TS_4)$ via q_{snd} query to ensure whether $Msg_5 \in \mathcal{L}_{\mathcal{P}\nabla^{\wr}}$ or not. In the above cases, q_{hah} has two executable sets $\frac{q_{snd}}{2^{r_i}}$ and $\frac{q_{hah}}{2^{r_i}}$ to predict its secure transmission with U_D. As a result, we obtain:

$$|P_r[Success_6] - P_r[Success_5]| \leq \frac{(2q_{hah} + 2q_{snd})}{2^{r_i}} \tag{8}$$

$Game_7$**:** This modeling prefers to use $Game_3$, which actively explores *Corrupt* and *Send* queries to discuss the key challenges of privacy preserving key agreement framework (PPKAF). To validate its key parameters, A_{dv} can obtain the secret credentials of U_D using q_{snd}. Moreover, A_{dv} applies *Corrupt* query to classify its salient features into three cases using online and offline password guessing attacks. The first two cases apply online password guessing, whereas the last one infers the properties of offline password guessing attacks to intercept the communication between U_D, App_S, and C_S.

- A_{dv} employs *Corrupt* query to relate the source attribute PW_{Gen} and also executes N *Send* queries to return its probability $\frac{q_{snd}}{N}$.
- In order to gain data access via I_{MD}, A_{dv} can execute *Corrupt* query. This query relates the probability of occurrence with user credentials to define its upper bound $q_{snd}.\tau_{fpr}$, where τ_{fpr} is the possibility of false positive rate to solve issues of open channel access.
- A_{dv} may obtain the secret parameter of the communication entities s_k which refers its key size k_s to issue q_{snd} query. Then, it can obtain $\frac{q_{snd}}{k_s}$ to derive its arbitrary credentials in order to establish secure communication.

The above case reveals that A_{dv} cannot execute more than one instance in parallel, and thus the successful probability becomes $max\{q_{snd}(\frac{1}{N}, \frac{1}{2^{k_s}}, \tau_{fpr})\}$. As a result of this, we obtain

$$|P_r[Success_7] - P_r[Success_6]| \leq max\{q_{snd}(\frac{1}{N}, \frac{1}{2^{k_s}}, \tau_{fpr})\} \tag{9}$$

Moreover, estimating the successful probability of A_{dv} requires $P_r[Success_7] = \frac{1}{2}$ to prove the assumption of ***Theorem 1***. Hence, the given proof is defined as follows.

$$\mathbf{A}_{EC-CDHP}^{PPKAF}[A_{dv}] \leq \frac{(q_{hah}^2+(q_{snd}+q_{ext})^2)}{2^{r_i}} + \frac{(q_{snd}+q_{ext})^2}{(n_{\mathbf{P}}-1)} + \frac{(2.q_{hah}+3.q_{snd})}{2.^{r_i-1}} + 2max\{q_{snd}(\tau_{fpr},\frac{1}{N}),\frac{1}{p_{str}}\}\blacksquare \quad (10)$$

B. Informal Security Analysis

We show the informal analysis below to highlight the security efficiency of the proposed AID-PPKAF against properties of key agreements and vulnerabilities.

1) KP_1 - Protect against Replay Attacks:: AID-PPKAF uses current timestamp values to exchange message requests among system entities such as U_D, App_S, and C_S. On receiving a message request, U_D, App_S, and C_S verify the timestamp value with system timing to consider and generate a new one. Otherwise, the corresponding entity terminates the message request to secure the communication channel. Thus, AID-PPKAF can protect system entities against replay attacks.

2) KP_2 - Protect against Impersonation and Man-in-the-Middle Attacks:: AID-PPKAF uses the timestamp and random values to preserve message requests and secret keys in exchanging data transmissions. U_D, App_S, and C_S verify message requests via the timestamp value, which finds authorized entities to create an original message over the proper secret value. As a result, A_{dv} cannot intercept a decrypted message of interest to an authentic network entity. Additionally, A_{dv} cannot be involved as a legal entity to perform any exchange of message requests, since A_{dv} is not aware of the secret values of legal entities such as U_D, App_S, and C_S. Thus, AID-PPKAF can prevent impersonation and man-in-the-middle attacks to ensure a secure environment and to create or analyze sensitive information within the network via App_S.

3) KP_3 - Protect against Ephemeral Secret Leakage:: To check the security features of authentication and key agreement frameworks, the CK adversary model is recommended. It has the capabilities of the DY model to steal session states of legal entities that recommend using system parameters of secret session keys, including timestamps, secret keys, and random nonces. As a result, the proposed AID-PPKAF uses short-term and long-term secret keys to compute a new session key, which is set among legal entities, namely, U_D, App_S, and C_S, to secure data transmissions. Since A_dv cannot generate a valid session key without long-term and short-term secret values, AID-PPKAF can preempt ephemeral secret leakage under the guidelines of the CK model.

4) KP_4 - Protect against Privileged Insider Attacks:: In AID-PPKAF, the obtained confidential information is inaccessible to subentities of T_A because it has an arrangement with other entities such as U_D, App_S, and C_S to remove all the registered information from T_A. Additionally, privileged users cannot initiate other relevant attacks, such as impersonation and session key computing, since the proposed AID-PPKAF has a pre-arrangement of behavioral patterns to detect the threats proactively. Thus, AID-PPKAF can restrain a privileged insider attack to proactively determine the damages caused by A_{dv}.

5) KP_5 - Protect against Physical I_{MD} Capture:: In particular, AID-PPKAF does not store confidential information in a readable form. Even if A_{dv} tries to physically capture I_{MD} using complex power analysis to determine sensitive information about the user, A_{dv} cannot uncover the session key of any I_{MD} because I_{MD} has its own unique identity and session key to prevent malicious behavior. On the other hand, malicious activity may uncover the session key of one specific I_{MD}, but it cannot be applied to any other I_{MD} because AID-PPKAF maintains unique secret session keys among communication entities such as U_D, App_S, and C_S. Thus, AID-PPKAF can unconditionally secure I_{MD} against physical capture.

TABLE IV: Comparing the Security Efficiency of the Proposed AID-PPKAF and Other Existing Schemes.

Key Agreement Schemes	KP_1	KP_2	KP_3	KP_4	KP_5	KP_6	KP_7	KP_8
LAuth [22]	✔	✗	✗	✗	✗	✗	✗	✗
SAuth [27]	✔	✔	✗	✔	✗	✗	✗	✗
RLAuth [28]	✔	✔	✗	✔	✗	✔	✗	✗
A-Auth [29]	✔	✔	✗	✔	✗	✔	✗	✔
EPP [34]	✔	✗	✗	✔	✗	✔	✗	✗
PP-PRU [35]	✔	✔	✗	✔	✗	✔	✗	✗
PP-KAP [36]	✔	✔	✗	✗	✗	✔	✗	✗
PPA-2F [37]	✔	✗	✗	✗	✗	✔	✗	✗
AID-PPKAF	✔	✔	✔	✔	✔	✔	✔	✔

6) KP_6 - Protect against Stolen Verifier Attacks:: Under AID-PPKAF, confidential information is maintained in congruence with system entities like App_S and C_S, and thus, A_{dv} cannot steal stored data to generate user identities or to compute secret keys to impersonate a legal user. Moreover, S_{DB} has $\{PW_{Gen}$,$U_{UID}\}$ as the published parameters, but A_{dv} cannot compute the user password without random integer x_p. On the other hand, A_{dv} cannot generate a legal message request, $\{N_{AP}$,$N1_{AP}$,N_{AP1},N_{AP2},g,$G\}$, to App_S and C_S without PW_{Gen},x_p, and y_p. Thus, AID-PPKAF can defend against a stolen verifier attack to avoid illegitimate access.

7) KP_7 - Support for User Anonymity and Untraceability:: Under AID-PPKAF, user identities cannot be exchanged in readable form, and thus, the entities maintain their anonymity to prevent data leakage. Additionally, user identities cannot be inferred by any A_{dv} because they use temporal identities, such as U_{UID}, UD_{APP_i}, $RID_{I_{MD_j}}$, and RID_{C_S}, to exchange message requests or to transmit sensing data. Moreover, temporal identities such as U_{UID}, UD_{APP_i}, $RID_{I_{MD_j}}$, and RID_{C_S} are changed each session. On the other hand, message requests use fresh timestamps and a random nonce to establish a unique session that processes data transmission among entities such as U_D, App_S, and C_S. As a result, A_{dv} cannot trace any information about the message request, because each session has its own timestamp and random nonce. Thus, AID-PPKAF achieves user anonymity and ensures untraceability to secure implantable devices against vulnerability.

8) KP_8 - Support for Forward Secrecy:: Under AID-PPKAF, communication entities such as U_D, App_S, and C_S use $H(H(R_P \parallel RID_{C_S}) \parallel RUD_{APP_{S_j}} \parallel Z_{APP_{S_j}} \parallel TS_1 \parallel TS_2)$ to establish a secure session, where $H(R_P \parallel RID_{C_S}) = M_3 \oplus H(RUD_{APP_{S_j}} \| Z_{APP_{S_j}} \| TS_1 \| TS_2)$. Say that secret information such as R_P, RID_{C_S}, $RUD_{APP_{S_j}}$, and $Z_{APP_{S_j}}$ are leaked. A_{dv} still cannot compute a legal session key $SK_{APP_{S_j},C_S}$ because he/she is still unaware of x_p and M_D to validate the message request. Under the circumstances, AID-PPKAF ensures that A_{dv} cannot infer any past, current, and future sessions to compute the shared session keys of the communication entities. Thus, AID-PPKAF ensures forward secrecy. Support for Credible Mutual Authentication: In AID-PPKAF, C_S validates the shared session key with $M_1^{'} = H(SK_{APP_{S_j},C_S} \parallel RUD_{APP_{S_j}} \| SID_{I_{MD_j}} \| TS_3)$ via G_A. Subsequently, U_D verifies TS_4 to determine $M_2^{'} = H(SK_{APP_{S_j},C_S} \parallel TS_4)$, which uses $M_2^{'} \stackrel{?}{\Rightarrow} M_2$ to exchange session key $SK_{APP_{S_j},C_S} = (SK_{C_S,APP_{S_j}})$ among two external entities, such as App_S and C_S, via T_A. Thus, AID-PPKAF achieves credible mutual authentication.

From Table IV, it is evident that AID-PPKAF fulfills security properties such as key freshness, data integrity, anonymity, secrecy, untraceability, and mutual authentication to meet the standard

IoMT/6G requirements. Additionally, AID-PPKAF strengthens the security features of the mechanism to resist vulnerabilities such as replay, man-in-the-middle, and privileged insider attacks, as well as device capture, ephemeral secret leakage, etc. It is also apparent that the existing schemes cannot resist a few of the prominent attacks, like device capture, ephemeral secret leakage, and stolen verifier, to achieve better security efficiency than the proposed AID-PPKAF.

VI. Performance Analysis

This section discusses comparative features such as the computation and communication of AID-PPKAF against other schemes to exhibit the significance of its performance efficiency. In the analysis, execution phases such as login, authentication, and key establishment are preferred to compare the cost efficiency of the authentication schemes, since the registration phase executes only once for each user. In AID-PPKAF, two significant cases are considered.

Case 1 uses entities such as U_D and App_S via G_A to examine the cost factors of authentication and key agreement, including computation and communication.

Case 2 uses entities such as App_S and C_S via T_A to analyze the cost factors of authentication and key establishment, including computation and communication.

A. Analysis I - Computation Cost

This subsection discusses the computation efficiencies of the proposed AID-PPKAF and existing schemes to signify the factor of execution time. It is worth noting that estimated computation costs such as T_{Hash}, T_{ECC-PM}, T_{ECC-PA}, T_{SE}, T_{SD}, T_{sig}, T_{RNG}, and T_{ME} are represented because they execute cryptographic parameters requiring time duration's of $0.00032sec$, $0.0171sec$, $0.0044sec$, $0.0056sec$, $0.0056sec$, $0.3317sec$, $0.053sec$, and $0.0192sec$, respectively [22]. The comparative analysis includes login, authentication, and key establishment phases to assess the computation costs of AID-PPKAF compared with other schemes. Different execution times were used to analyze the computation parameters of the login and authentication phases.

To register cryptographic parameters with the system kernel, a rigorous analysis was conducted using a Debian-based operating system running *Ubuntu 22.10* on an *Intel Core i7 CPU* with *16GB RAM*, a *256GB SSD*, and a *2.59GHz* clock speed. The analysis examined cryptographic operations that integrated *Raspberry Pi 4* on an *ARM-Core Cortex A72* at *1.5GHz* to evaluate the key features of I_{MD}. Table V shows the computation costs of AID-PPKAF and the other schemes. The computation analysis proved that AID-PPKAF incurs low computation costs, i.e., $\approx 0.50754sec$ compared to the other schemes at $\approx 0.827sec$, $\approx 1.768sec$, $\approx 0.524sec$, $\approx 0.747sec$, $\approx 3.021sec$, $\approx 0.930sec$, $\approx 0.518sec$, and $\approx 0.597sec$, respectively.

During the login, authentication, and key establishment phases under AID-PPKAF, U_D costs were $5T_{Hash}+4T_{ME}+1T_{SE}+1T_{SD}+1T_{sig} \approx 0.4213sec$, whereas the costs of App_S and C_S were $6T_{Hash}+2T_{ME}+1T_{SE} \approx 0.04592sec$ and $6T_{Hash}+2T_{ME} \approx 0.04032sec$ to validate established session key $SK_{APP_{S_j},C_S}$. As a result, the total computation cost between $U_D \overset{APP_S}{\Leftrightarrow} C_S$ was $\approx 0.50754sec$, which is considered the execution time of the cryptographic parameters utilized in AID-PPKAF. Promisingly, the key establishment module with three-factor authentication integrates its functional components with system hardware to improve overall cost-effectiveness, including scalability and reliability of accelerator-based cyber-physical systems.

B. Analysis II - Communication Cost

In this subsection, a few critical components of the cryptographic protocol, such as random number generation, identity length, symmetric encryption/decryption, and hash output, were chosen to evaluate the message requests processed by U_D, App_S, and C_S. During login, authentication, and key establishment phases, U_D, App_S, and C_S successfully generated five message requests, $Msg_1 \sim Msg_5$, to validate established session key $SK_{APP_{S_j},C_S}$. Each message request used components of the cryptographic protocol to compute and verify the value with the timestamp to perform either encryption or decryption.

To analyze the composition of the cryptographic protocol, the computed sizes of the random number, the identity length, the timestamp, and the hash output were $160bits$, $32bits$, $160bits$, and $256bits$, respectively [32]. In the proposed AID-PPKAF, the message request sizes were $Msg_1 = \{EN_1, V_2, TS_1\} \approx 480bits$, $Msg_2 = RID_{C_S}, x, \beta, j \approx 512bits$, $Msg_3 = x_1 \oplus H(SID_{I_{MD_j}} \parallel TS_3) \approx 608bits$; $Msg_4 = H(x_1 \parallel SID_{I_{MD_j}} \parallel TS_3 \parallel Z_{APP_{S_j}}) \approx 640bits$; and $Msg_5 = \{V_4, TS_4\} \approx 320bits$ in verifying the legitimacy of the communication entities. Furthermore, this computation estimated the total communication cost of the proposed AID-PPKAF at $\approx 2560bits$ for U_D, App_S, and C_S. A comparison of communication cost efficiency is shown in Table VI, signifying the features of AID-PPKAF in comparison with other schemes. The computation results revealed that AID-PPKAF had lower communication costs, i.e., $\approx 2560bits$, than the other schemes at $\approx 3520bits$, $\approx 7646bits$, $\approx 6496bits$, $\approx 6368bits$, $\approx 4032bits$, $\approx 2688bits$, $\approx 4352bits$, and $\approx 4576bits$, respectively.

C. Analysis III - Simulation Study

This section presents a comprehensive analysis describing a quantitative analysis of chain-based IoMT using NS3 to analyze the functional attributes of the proposed AID-PPKAF and other relevant schemes. To examine the practicality of the schemes, we installed the NS3.28 version on Ubuntu 22.04, which builds a high-level network modeling to carry out the simulation using a 3D network with a degree of $800m \times 800m \times 800m$. In this network scenario,

1) we utilized a gateway node A_G at a specific location to coordinate with the medical devices I_{MD} via App_S.
2) We randomly distributed I_{MD} within the range of $20m$ to 100 from A_G to analyze the impact of the network. This network uses *RandomWalk [2D Mobility Model]* to move the coordinate at a speed of $1-3m/s$ as discussed in [40].
3) We allowed I_{MD} to transit across $180m$ close to A_G with the utmost speed of $5m$ per second.
4) We permitted the users of I_{MD} to access the source attributes of the proposed AID-PPKAF and other relevant schemes to examine the quality metrics such as throughput (bytes per second), end-to-end delay (sec), energy consumption (%), and network lifetime (%) after the successful establishment of the session keys with I_{MD} via authorized A_G.
5) We applied a carrier transmission protocol (i.e., carrier sense multiple access/collision detection (CSMA/CA) as a MAC protocol to limit the impact of a collision occurring when two or more A_G carry their signals over a reliable data link layer. It is worth noting that we exploited the source parameters of I_{MD}, such as SendEnable, ReceiveEnable, TxQueue, etc., to analyze the propagation delay associated with each I_{MD} to probe the data packets attached to the protocol stack.
6) We also modified the MAC protocol into a faster one to mitigate the transmission delay closely related to energy efficient duty

TABLE V: Comparison of Computation Cost Efficiency

Key Agreement Schemes	Login, Authentication and Key Establishment Phase			Total Cost	Execution Time (sec)
	U_D	App_S	C_S		
LAuth [22]	$20T_{Hash}+6T_{ME}+1T_{SE}+2T_{SD}+1T_{sig}$	$4T_{Hash}+1T_{ME}+1T_{SE}$		$24T_{Hash}+7T_{ME}$ $+2T_{SE}+2T_{SD}+2T_{sig}$	$\approx$0.827
SAuth [27]	$1T_{Hash}+2T_{ME}+1T_{sig}$	$29T_{Hash}+5T_{SD}+6T_{SE}+4T_{sig}$		$30T_{Hash}+2T_{ME}+6T_{SE}$ $+5T_{SD}+5T_{sig}$	$\approx$1.768
RLAuth [28]	$18T_{Hash}+14T_{ME}+1T_{SE}+1T_{SD}$	$19T_{Hash}+11T_{ME}+3T_{SE}+1T_{SD}$		$34T_{Hash}+25T_{ME}$ $+4T_{SE}+2T_{SD}$	$\approx$0.524
A-Auth [29]	$11T_{Hash}+12T_{ME}+11T_{ECC-PM}$	$7T_{Hash}+7T_{ME}+11T_{ECC-PM}$		$18T_{Hash}+19T_{ME}$ $+22T_{ECC-PM}$	$\approx$0.747
EPP [34]	$5T_{RNG}+6T_{ECC-PA}+20T_{ECC-PM}+7T_{Hash}$			$5T_{RNG}+6T_{ECC-PA}$ $+20T_{ECC-PM}+7T_{Hash}$	$\approx$3.021
PP-PRU [35]	$3T_{ECC-PA}+8T_{ECC-PM}+5T_{Hash}+6T_{ME}+2T_{sig}$			$3T_{ECC-PA}+8T_{ECC-PM}$ $+5T_{Hash}+6T_{ME}+2T_{sig}$	$\approx$0.930
PP-KAP [36]	$20T_{Hash}+15T_{ME}+2T_{SE}+2T_{SD}$			$16T_{Hash}+11T_{ME}$ $+2T_{SE}+2T_{SD}$	$\approx$0.518
PPA-2F [37]	$30T_{Hash}+16T_{ME}+2T_{SE}+3T_{SD}$			$30T_{Hash}+16T_{ME}$ $+2T_{SE}+3T_{SD}$	$\approx$0.597
AID-PPKAF	$5T_{Hash}+4T_{ME}+1T_{SE}+1T_{SD}+1T_{sig}$	$6T_{Hash}+2T_{ME}+1T_{SE}$	$6T_{Hash}+2T_{ME}$	$17T_{Hash}+8T_{ME}+2T_{SE}$ $+1T_{SD}+1T_{sig}$	$\approx$0.507

T_{Hash} - One-way Hash Function; T_{ECC-PM} - Elliptic-Curve Point Multiplication; T_{ECC-PA} - Elliptic-Curve Point Addition; T_{SE} - Symmetric Key Encryption; T_{SD} - Symmetric Key Decryption; T_{ME} - Modular Exponentiation; T_{sig} - Verify/Execute with a Signature

TABLE VI: Comparison of Communication Cost Efficiency

Key Agreement Scheme	Message Rounds			Total Cost (bits)
	U_D	App_s	C_S	
LAuth [22]	4			3520
SAuth [27]	5			7646
RLAuth [28]	11			6496
A-Auth [29]	3			6368
EPP [34]	4			4032
PP-PRU [35]	4			2688
PP-KAP [36]	4			4352
PPA-2F [37]	4			4576
AID-PPKAF	5			2560

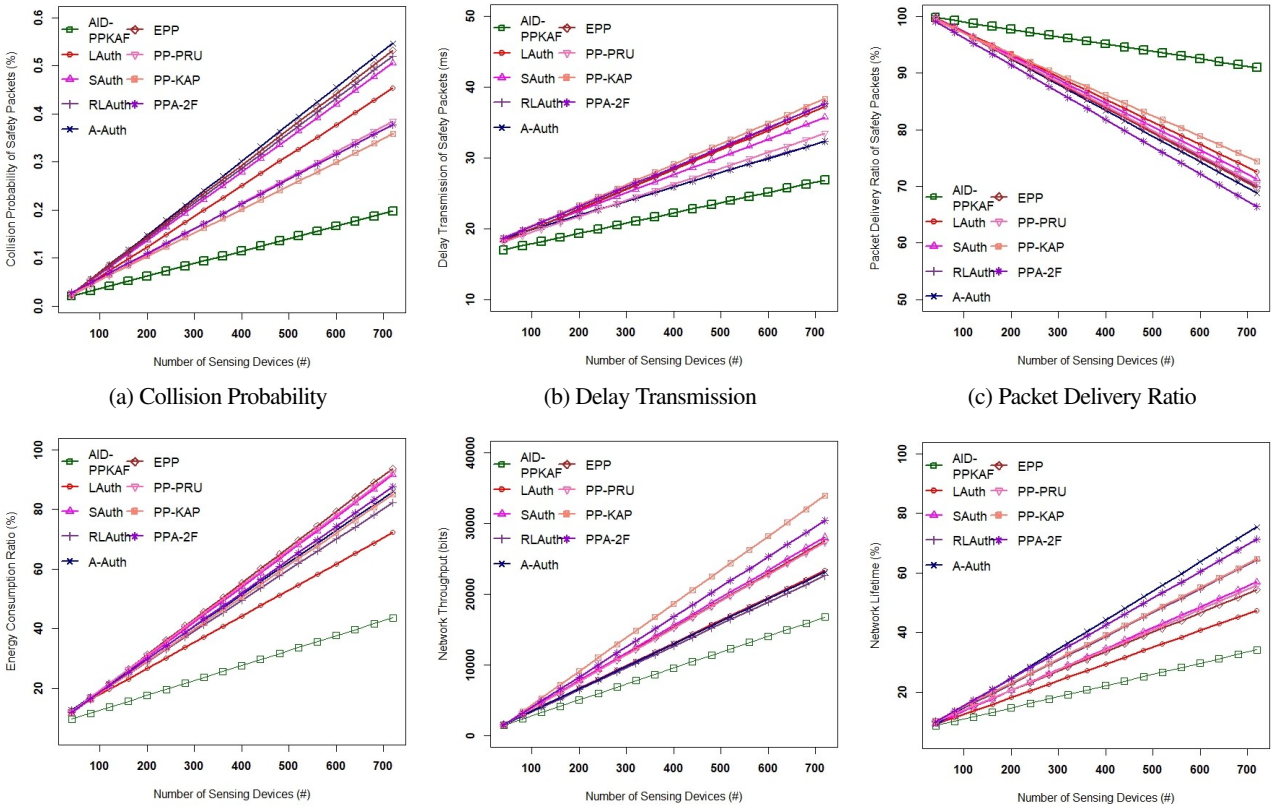
cycling (EEDC) i.e., producing efficient data collection with less transmission delay.

7) We adopted a producer mobility support scheme (PMSS) and hybrid network mobility (Hybrid NeMo) to transmit the medical data, providing binding information using Named Data Networking (NDN). The operational processes are as follows.
   - *Process 1:* While performing handover transmission, U_D and A_G transmits the requesting data to App_S. Subsequently, App_S validates the data contents with C_S to maintain add-on cloud storage and to make I_{MD} to process the transmission of data.
   - *Process 2:* Apply *content retrieval* function via I_{MD} to process the data transmission between U_D and C_S via App_S.
   - *Process 3:* Utilize *PMSS* and *Hybrid NeMo* to operate data processing via I_{MD} and exploit the behavioral characteristics of the mobility model while transferring the data to C_S.
   - *Process 4:* Update the routing information of U_D in advance to control the collision of data packets while transmitting the data among the application systems App_S.
   - *Process 5:* While completing the process of data transmission, U_D re-propagates their data requests via App_S to collect the medical data i.e., using I_{MD}.
   - *Process 6:* Use C_S to manage the transmitted information and to store the status of data transmission, i.e., maintained or interrupted, while updating C_S using the forward information base (FIB) to speed up the transmission.
8) We handled the functionalities of Crypto++ to perform various cryptographic operations such as encryption schemes, hash functions, message authentication codes, etc., over the converted packet payload.
9) We discovered a PHY-level model i.e., 802.11a as a wireless hub which operates the modeling frequencies $\approx 5.752GHz$ to $\approx 5.850GHz$ to simulate the communication among I_{MD}, App_S, and C_S as a part of point-to-point connection.
10) We firmly set usage of power transmission, i.e., for computing nodes I_{MD} ($\approx$0.75W to $\approx 2W$) and accordingly, limited their transmission rate $\approx 10kbps$ over a time of $1800sec$. Above all, the simulation was re-iterated over 420 rounds to analyze various communication metrics such as packet delivery ratio (%), energy consumption, throughput (bps), and network lifetime. Table VII shows the significant parameters involved in the NS3 simulation.

TABLE VII: Parameters Involved in Network Simulation.

Parameter	Set Value
3D-Deployment	$800m \times 800m \times 800m$
Node Density	120 to 550
Modulation Technique	BPSK
Routing Protocol	EE-CMRP
Mobility	1.25 to $3.75m/s$
Transmission Range	$120m$
Packet Size	$100bytes$
Channel Transmission Rate	$8kbps$
Bandwidth	$4Khz$
Transmission Power (T_x)	$90dbre\mu Pa$
Packet Transmission Rate Δ	1% Uplink (UL)
Simulation Time	$1800sec$
Transmission Rounds	420
Tool Used	NS3
Number of end users U_D	720
Number of Application Gateway A_G	12

1) Performance Metrics: To simulate network topology with an established connection, the computing devices, i.e., I_{MD}, were configured with the network interface cards controlled by *NetDevices*, i.e., CSMA and WiFi. The connective elements, including the channel and network interface, configured their devices with the protocol stacks to share the frequency spectrum. The network containing I_{MD}, App_S, and C_S is considered a point-to-point connection via A_G to manage and instantiate the source attributes of the proposed AID-PPKAF and other relevant schemes via 420 end users, i.e., U_D. The participating users U_D employed the dedicated channel model and PHY layer to probe the exchange of routing packets among I_{MD}, App_S, and C_S, addressing the issues related to network density, channel allocation, and transmission rate. Using communication modules like 802.11, entities such as I_{MD} and A_G utilized a dedicated channel model to exploit the characteristics of the infrastructure network.



(a) Collision Probability (b) Delay Transmission (c) Packet Delivery Ratio

(d) Energy Consumption Ratio (e) Network Throughput (f) Network Lifetime

Fig. 5: Simulation Results of the proposed AID-PPKAF and other relevant schemes using NS3.

To perform active probing of data packets via InternetStackHelper and IPv4AddressHelper, we apply a chain-based IoMT that evaluates the following metrics.

Packet Delivery Rate (PDR) - defines the total number of packets successfully received ($Total_{PktRcvd}$) at surface gateway A_G to the total number of packets transmitted ($Total_{PktTmt}$) by the source I_{MD} to compute the delivery rate. This process can be determined by,

$$P_{DR} = \frac{Total_{PktRcvd}}{T_{PktTmt}} \tag{11}$$

According to the scalability study proposed in [41], we evaluated the frequency assignment against high network densities, i.e., up to 42 devices per km^2, and subsequently, tested the data connectivity with 720 end users (U_D) per communication channel using a chain-based routing protocol (i.e., Energy Efficient Clustering Multi-hop Routing Protocol (EE-CMRP). In the practical analysis, the metrics such as collision probability rate, delay transmission, and packet delivery ratio were chosen to analyze different contention window (CW) sizes of data packets over the packet arrival rate, i.e., $\lambda_e = \lambda_s = 28$ packet per second.

While comparing the delay metric based on CW, the proposed AID-PPKAF considerably reduces its collision probability with a higher delivery ratio under various numbers of end users U_D than other relevant schemes. Also, we chose to double the initial size of CW in order to fulfill the properties of the application system (like eHealth). Notably, the proposed AID-PPKAF optimizes key generation techniques associated with hashing and encryption to provide a scalable and highly secure solution. It uses promising key establishment processes among U_D, App_S, and C_S to preserve their integrity in order to offer scalable data management in any sensitive-aware application system.

Because of this, we realize that the proposed AID-PPKAF experiences a few packet collisions as and when the number of end users periodically increases over time, as shown in Fig.5[a-c]. However, the conditional state of the network remains more effective for the proposed AID-PPKAF than other relevant schemes in achieving a better transmission ratio under various numbers of end users U_D. It is worth noting that the other relevant schemes could not perform a proper synchronization with their source attributes to establish data connectivity among I_{MD} and App_S, resulting low delivery rate and increased packet collision.

Energy Consumption (EC) defines the total quantity of energy consumed by I_{MD} while performing the network operation over the simulation period. During the period of execution, I_{MD} utilizes the storage of energy sources to perform various computing tasks, including transmitting T_{EC}, receiving R_{EC}, and idling I_{EC}. This process can mathematically be expressed as,

$$E_C = \sum_{N=1}^{N} T_{EC} + R_{EC} + I_{EC} \tag{12}$$

Additionally, we apply a normalized value of E_C using Eq.12 by the overall amount of energy ToT_{EG}. It is mathematically expressed as,

$$EC_{Norm} = \frac{E_C}{ToT_{EG}} \tag{13}$$

The analytical results shown in Fig.5d illustrate the energy consumption ratio of the proposed AID-PPKAF and other relevant schemes using EC-CMRP, which explores the maximum number

of transmissions over the dedicated communication channels, i.e., A_G, to probe the connectivity of the fully loaded networks. The course of data connectivity and its evaluation considered different traffic intensities to probe the consumption ratio of I_{MD} over traffic intensity t_i in order to analyze the average packet transmission rate by App_S. It is important to note that App_S considers a suitable sub-band, i.e., $\approx 125kHz$ with available channels used by I_{MD} to initiate the process of up-link transmission to C_S. In the plotted graph, we show the mean residual energy of I_{MD} over the increasing number of U_D, which utilizes the data collection point at C_S to process the transmission over the simulation period. Due to multiple transmissions in the available networks through dedicated A_G, the proposed AID-PPKAF experiences fewer packet collisions than other relevant schemes. Moreover, the proposed AID-PPKAF effectively uses its source attributes (i.e., R_P, RID_{C_S}, and RUD_{APP_S}) of duty cycling to minimize collision rate and transmission delay, whereby the energy consumption of A_G and I_{MD} is minimal.

Network Throughput (NT) To analyze this metric, the dedicated network applies the transmission range of A_G over the densely populated devices I_{MD}. Moreover, the data network uses the closest A_G to measure the transmission range of serving devices I_{MD} and utilizes adaptive dynamic slicing to control the collision rate caused by co-channel interference. Fig. # shows the network throughput trading different network loads to analyze their collision rate. While assessing A_G with available I_{MD} distributed across a $5km$ radius, we observe that the proposed AID-PPKAF manages network workloads based on the density of I_{MD} using adaptive rate selection (ADR) to achieve a better transmission rate than other relevant schemes. It is also worth noting that the proposed AID-PPKAF can handle T_A effectively to fully utilize its computing resources to maximize the transmission rate of I_{MD} as shown in Fig.5.

Network Lifetime (NL) operates the network activities over a period to examine its lifetime. Mathematically, it can be expressed as,

$$N_{LT} = \sum_{T=1}^{T_{Max}} N_{LT}t) \tag{14}$$

where $N_{LT}(t)$ is the network lifetime relating to *time*, which analyzes the network degrading its service at the rate of 0.9% under $8nodes/km^2$. We plot the graph outlining the network's lifetime of the proposed AID-PPKAF and other relevant schemes that assign its dedicated A_G among other App_S to initiate multiple copies of data packets using I_{MD} to C_S. Fig.5f shows the results of network lifetime among the proposed AID-PPKAF and other relevant schemes. In the analysis, we varied the network load, i.e., $T_i = 1$ over the available sensing devices I_{MD} to examine the possibility of collision rate through the available A_G. Note that A_G explores the source attributes of C_S, such as RUD_{APP_S} and UD_APP, to probe the active transmission rate of I_{MD} over the available channels. From Fig.5f, we can notice that the proposed AID-PPKAF minimizes the rate of packet collision, though the density of packet transmission increases among I_{MD} and App_S via A_G. Moreover, the source attributes of the proposed AID-PPKAF synchronize with the routing protocol, i.e., EE-CMRP, to limit the duty cycle with negligible value using the primitive of MAC and accordingly, mitigate the external interference incurred by A_G. However, the other relevant authentication schemes do not have any specific attributes to consider a uniform density among I_{MD}, whereby they cannot operate a high number of A_G over I_{MD} to reduce the rate of packet collision.

D. Pragmatic Study

This section presents a practical demonstration of the proposed AI scheme in order to analyze its behavioral pattern in a real-time scenario. To analyze a few capabilities of user behavior as an authentication factor, and to expose different test cases of interaction scenarios, an ad hoc application was developed with a guided dataset (heart disease) accessible from the IEEE Dataport [42]. For this purpose, the proposed AISec was executed among the communication entities U_D,App_S, and C_S relying on data authenticity [43]. The real environment considered sessions and timestamps, among other information, to establish the legitimacy of the sessions. To analyze the source attributes of the proposed and other relevant schemes, the computing variables and their sensing data were dealt with proper data analysis using a machine learning approach, i.e., support vector machine (SVM).

This approach utilized the data points of the guided dataset containing stationary data to evaluate the issues of imbalanced class size without any data removal. Since the data points have a linear reconstruction error, we applied the extracted feature space over annotated samples to authenticate whether the collected data had any imbalanced data or not. As a result, the proposed AID-PPKAF and other relevant schemes utilize the source parameters of the communication entities U_D and T_A via authenticated channels to analyze the execution time of the authentication requests processed through public-private key pairing. The steps involved in the verification process are as follows (as shown in Algorithm 1). Noticeably, the other learning models (decision tree and logistic regression) cannot separate data points efficiently to find the best hyperplane to predict the probability of a structural binary pattern.

Algorithm 1 Modeling Structure.

Require: Allow key agreement KA scheme to execute $KA_{Setup}(\lambda)$ to generate a context parameter c_p

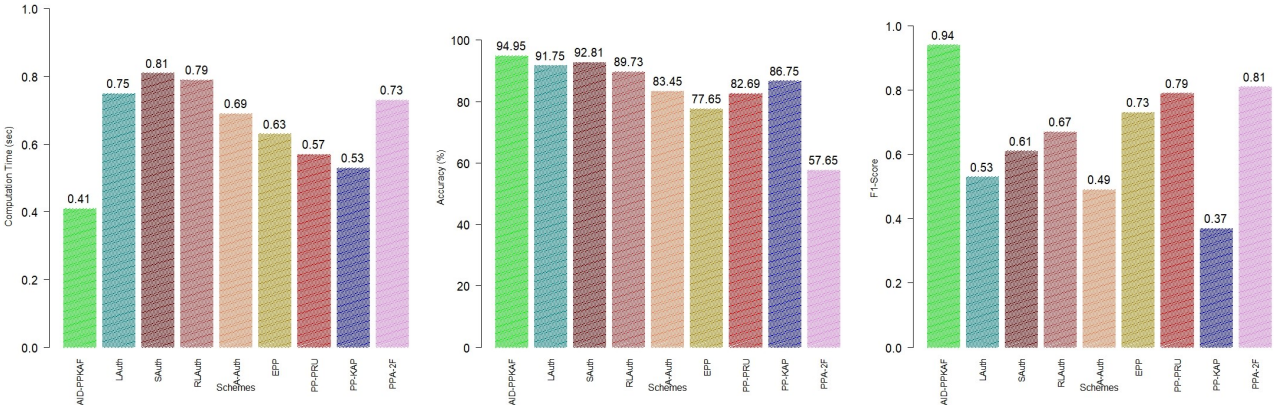
Ensure: Select the key agreement scheme to verify their source attributes via a threshold parameter τ

1: Each U_D executes the key agreement scheme $KA_{Setup}(\lambda)$ via T_A to obtain a session key S_K in order to establish a secure communication.
2: Apply a learning classifier, i.e., SVM, to choose the related parameters, e.g., learning rate l_r, batch size b_s, and local epoch l_e, which generates its local model to analyze the security features.
3: Use local training and data aggregation to probe the private-public key pairing, negotiating the generation of shared session key via timestamp T_S (i.e., authentication request a_r)
4: ▷ Learning Rules
5: Check whether the entities have a successful synchronization via S_K generation to share data features to C_S
6: Initialize a random weight through $KA_{Setup}(\lambda)$ to analyze the behavior of source attributes
7: Choose an input vector k consisting of $X \times Y$ to read the status of wireless channel
8: Based on T_S, the classifier, i.e., SVM, uses the input vector a_r to discover a learning model with complex binary values/vectors
9: The learning model matches the weights of the output vector using *Hebbian Learning Rule* ▷ Learning Model l_m

$$l_m^{'} = l_{xy} + \tau_{xy}\Theta(\lambda,\tau) \tag{15}$$

▷ Θ returns *1* if the argument satisfies, l_{xy} is the learning input/weight to operate the attributes of $KA_{Setup}(\lambda)$, and $l_m^{'}$ is the upgraded input value.

System Specification - A system with an Intel Core i7 processor with *8GB RAM* and *an Nvidia GeForce RTX 3090* was used to



(a) Computation Time (b) Accuracy (c) F1-Score

Fig. 6: Analytical Results of the proposed AID-PPKAF and other relevant schemes using SVM.

leverage the performance of the training models and to handle the machine learning tasks using the proposed AISec.

Software Platform and Libraries - A real-time platform known as Google Colab was chosen to explore key libraries such as Pandas, Seaborn, Matplotlib, and Scikit-Learn. To support multi-dimensional arrays, data science/machine learning tasks utilize Pandas, which shows the correlation between column functions. In order to visualize the correlation strength, Seaborne simplifies sensible defaults that find specific features to transform matrix correlations. To draw graphical plots in interactive form, Matplotlib uses the numerical extension NumPy. To offer statistical modeling, Scikit-Learn includes classification, regression, and clustering, which reduce dimensionality to provide an efficient predictive analysis.

Medical Data - This scenario was categorized into different attributes, such as chest pain levels ranging from 1 to 4, blood pressure, sugar levels, ECG readings, heart rates, and cholesterol levels. The compiled dataset included 1190 patients in order to analyze 12 feature rows of computing data, examining the binary results of heart disease using classification techniques such as support vector machine (SVM).

Data Processing and Learning - To analyze a large amount of data, the real-time scenario independently used different chunk configurations, such as time-based and fixed-size. The former configuration used high variability to make the records move within a short duration, and thus, cannot produce movement during the waiting period of a loading window. However, the latter inspected the training algorithms to load and use the feature columns over the entire user session in a continuous manner. The learning activities effectively used the libraries and datasets to visualize the targets: i.e., Healthy or Unhealthy. Additionally, the integrated environment processed execution times over a different number of chunks to analyze the predictive ratio of legitimate users.

Data Preprocessing and Splitting - To test and train the dataset, primary credentials such as chest pain, blood pressure, sugar level, etc., were considered as a prepared dataset. Using a standard scalar to homogenize its nature in one form reinforced the detection threshold to increase the prediction ratio.

Modeling and Hyper-Tuning - The learning algorithms (support vector machine) found optimal hyperparameter values to maximize modeling performance, which predefined the loss functions to optimize the processing infrastructure.

1) Computation Time: The proposed AISec applied effective machine learning techniques such as the decision tree, logistic regression, and the support vector machine to conduct a rigorous analysis and to build a continuous authentication system over user sessions. In descriptive statistics, a set of values was defined over a time series from a heart disease dataset to identify the components of cyclicity and to detect class attributes of chest pain levels among the participants. In the sensitivity analysis, the learning algorithm pruned confidence to observe performance that evaluated parameter changes to identify feature selections of the heart disease dataset, e.g., the level of chest pain. The classifier used the proposed AISec technique to produce the actual computation time of the proposed AID-PPKAF and other relevant schemes, which show the optimized execution time without any predetermined model.

Furthermore, to compare the performance of the SVM classifier in terms of computations, the proposed AID-PPKAF and other relevant schemes utilizing AISec extracted the relevant attributes more sensitive to heart disease, potentially detecting the number of estimators over time, as shown in Fig.6a. The classifiers had computation times of 0.41 sec, 0.75 sec, 0.81 sec, 0.79 sec, 0.69 sec, 0.63 sec, 0.57 sec, 0.53 sec, and 0.73 sec, respectively, in assessing the prediction accuracy and observing systematic discrepancies between the predicted and measured solutions. It was evident that the proposed AID-PPKAF required less computation time than the other relevant schemes.

2) Accuracy: The quality and performance of the classifier techniques used the matrix elements to identify correct and incorrect predictions and applied a confusion matrix to obtain the percentages of predicted values. Each classifier technique utilized the proposed AISec scheme to find a predictive ratio for heart disease. It could even exploit medical attributes such as chest pain ranging from 1 to 4, blood pressure, etc., to detect the risk factors for heart problems. As a result, the classifier utilizing the proposed AID-PPKAF and other relevant schemes normalized the distribution of the dataset to address the issue of modeling error, i.e., detecting outliers. To obtain better accuracy, the SVM classifier technique was embedded with the proposed AISec. It used a selective feature set with hyper-tuning to offer a productive application for medical experts.

To estimate prediction accuracy, the available classes were equally defined, obtaining different values of the proposed AID-PPKAF and other relevant schemes using an SVM classifier (94.95%, 91.75%, 92.81%, 89.73%, 83.45%, 77.65%, 82.69%, 86.75%, and 57.65%) as the roles and data points from a measurement of the receiver operating characteristics (RoC) curve, as shown in Fig.6b. From this measurement, it is apparent that the SVM with the proposed AID-PPKAF

achieved better accuracy (94.95%) than other relevant schemes.

3) F1-Score: In the proposed AISec, the components of AID-PPKAF are applied in an ensemble model to evaluate robustness over the other relevant schemes. The binary classification system included a heart disease dataset to extract precise feature selections and measure modeling accuracy. To calculate precisely, the precision and recall metrics were considered, which set distribution classes to find scores for false positives and false negatives.

While the proposed AISec returned different values for false positives and false negatives, the F-1 scores were evaluated using the SVM classifier to determine assessment ratios of the proposed AID-PPKAF and other relevant schemes, which were 0.94,0.53,0.61,0.67,0.49,0.73,0.79,0.37, and 0.81, respectively. These assessment ratios show that the proposed AID-PPKAF utilizing SVM had better cost efficiency (0.94) than the other schemes (as shown in Fig.6c), providing high-level modeling quality that optimized the precision value to detect heart disease via a proper authentication process.

VII. Conclusion and Future Works

Of late, computations in medical devices have played a crucial role in the deployment of the IoMT framework while being massively transformed by the mobile IoT. Fortunately, 6G next-generation networks will redefine their communication environments and setups to meet resource recommendations for medical devices. However, forensic-aware cyber-physical systems in the IoMT demand trustworthiness and privacy to satisfy the significant requirements of intelligent services and applications. Thus, in this paper, a robust, AI-driven, privacy-preserving key authentication framework was proposed to address the security issues associated with healthcare systems using the IoMT. In the proposed AID-PPKAF, cryptography primitives such as elliptic curve cryptography and the physically unclonable function were applied to build a lightweight authentication protocol and deal with device vulnerabilities from the perspective of hardware structure. To demonstrate its security efficiency, an informal analysis of a few of the relevant attacks showed the resilience features of AID-PPKAF. Moreover, a comparative analysis of computation and communication costs showed that AID-PPKAF can determine feasibility in resource-constrained IoMT devices because it generates less overhead to establish a session key with communication entities such as U_D, App_S, and C_S.

Lastly, a detailed simulation and pragmatic studies were carried out using NS3 and SVM to provide a comprehensive analysis: 1. Explore the composition of the proposed AISec with the deployment of App_S and C_S; and 2. Evaluate the value of its existence with learning components of the PPKAF and other relevant schemes to categorize performance measurements in terms of computation time, accuracy, and F1-score. Compared to the existing authentication modules, the proposed AID-PPKAF can seamlessly integrate the security model with data analytics during the implementation process to achieve the basic key requirements of cyber-physical systems. By analyzing the balanced metrics (computing time and accuracy), the designers can develop a cost-effective privacy-aware module to enhance the overall performance efficiency of IoMT applications. In the future, we will employ cryptographic assumptions such as zero-knowledge proofs and homomorphic encryption to process device information with integrity-preserving authentication that applies a MAC algorithm in exchange for a message with a secret key.

References

[1] M. M. Ozcelik, I. Kok, and S. Ozdemir, "A survey on internet of medical things (iomt): Enabling technologies, security and explainability issues, challenges, and future directions," *Expert Systems*, vol. 42, no. 5, e70010, 2025.

[2] I. Majdoub and K. Atmani, "Privacy paradigm shift: Zero knowledge proofs in criminal e-evidence collection," in *Cybercrime Unveiled: Technologies for Analysing Legal Complexity*, Springer, 2025, pp. 151–175.

[3] E. Akbal, F. Günes, and A. Akbal, "Digital forensic analyses of web browser records.," *J. Softw.*, vol. 11, no. 7, pp. 631–637, 2016.

[4] I. V. Kotenko, M. Kolomeets, A. Chechulin, and Y. Chevalier, "A visual analytics approach for the cyber forensics based on different views of the network traffic.," *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, vol. 9, no. 2, pp. 57–73, 2018.

[5] N. Shafqat, "Forensic investigation of user's web activity on google chrome using various forensic tools," *IJCSNS Int. J. Comput. Sci. Netw. Secur*, vol. 16, no. 9, pp. 123–132, 2016.

[6] K. S. L. Kazi, "Machine learning-driven internet of medical things (ml-iomt)-based healthcare monitoring system," in *Responsible AI for Digital Health and Medical Analytics*, IGI Global Scientific Publishing, 2025, pp. 49–86.

[7] H. Kim, "Security enhancement of biometric-based authentication systems using smart card," *IEEE Access*, 2024.

[8] B. Deebak and S. O. Hwang, "Privacy preserving based on seamless authentication with provable key verification using miomt for b5g-enabled healthcare systems," *IEEE Transactions on Services Computing*, 2024.

[9] B. Deebak and S. O. Hwang, "Federated learning-based lightweight two-factor authentication framework with privacy preservation for mobile sink in the social iomt," *Electronics*, vol. 12, no. 5, p. 1250, 2023.

[10] M. Aljanabi, "Safeguarding connected health: Leveraging trustworthy ai techniques to harden intrusion detection systems against data poisoning threats in iomt environments," *Babylonian Journal of Internet of Things*, vol. 2023, pp. 31–37, 2023.

[11] J. Xiong, M. Zhao, M. Z. A. Bhuiyan, L. Chen, and Y. Tian, "An ai-enabled three-party game framework for guaranteed data privacy in mobile edge crowdsensing of iot," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 922–933, 2019.

[12] S. Zou, Q. Cao, C. Huangqi, *et al.*, "A physician's privacy-preserving authentication and key agreement protocol based on decentralized identity for medical data sharing in iomt," *IEEE Internet of Things Journal*, 2024.

[13] S. S. Ahamad and A.-S. Khan Pathan, "A formally verified authentication protocol in secure framework for mobile healthcare during covid-19-like pandemic," *Connection Science*, vol. 33, no. 3, pp. 532–554, 2021.

[14] C. Romero and S. Ventura, "Educational data mining and learning analytics: An updated survey," *Wiley interdisciplinary reviews: Data mining and knowledge discovery*, vol. 10, no. 3, e1355, 2020.

[15] 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.

[16] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the iot world: Present and future challenges," *IEEE Internet of things journal*, vol. 5, no. 4, pp. 2483–2495, 2017.

[17] M. Wickham, "Exploring data breaches and means to mitigate future occurrences in healthcare institutions: A content analysis (order no. 13861149)," *Available from ProQuest Dissertations & Theses Global.(2216485062)*, 2019.

[18] M. Shariq, I. T. Ahmed, M. Masud, A. D. E. Berini, and N. Jamil, "Design of a provable secure lightweight privacy-preserving authentication protocol for autonomous vehicles in iot systems," *Computer Networks*, vol. 261, p. 111 155, 2025.

[19] C. Pu, A. Wall, K.-K. R. Choo, I. Ahmed, and S. Lim, "A lightweight and privacy-preserving mutual authentication and key agreement protocol for internet of drones environment," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9918–9933, 2022.

[20] N. Lath, K. Thapliyal, K. Kandpal, M. Wazid, A. K. Das, and D. Singh, "Bdesf-its: Blockchain-based secure data exchange and storage framework for intelligent transportation system," in *IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, IEEE, 2022, pp. 1–6.

[21] M. Papaioannou, M. Karageorgou, G. Mantas, *et al.*, "A survey on security threats and countermeasures in internet of medical things (iomt)," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 6, e4049, 2022.

[22] V. Kumar, M. S. Mahmoud, A. Alkhayyat, J. Srinivas, M. Ahmad, and A. Kumari, "Rapchi: Robust authentication protocol for iomt-based cloud-healthcare infrastructure," *The Journal of Supercomputing*, vol. 78, no. 14, pp. 16 167–16 196, 2022.

[23] F. Merabet, A. Cherif, M. Belkadi, O. Blazy, E. Conchon, and D. Sauveron, "New efficient m2c and m2m mutual authentication protocols for iot-based healthcare applications," *Peer-to-Peer Networking and Applications*, vol. 13, pp. 439–474, 2020.

[24] X. Wang, L. Wang, Y. Li, and K. Gai, "Privacy-aware efficient fine-grained data access control in internet of medical things based fog computing," *IEEE Access*, vol. 6, pp. 47 657–47 665, 2018.

[25] S. Kim, H.-J. Mun, and S. Hong, "Multi-factor authentication with randomly selected authentication methods with did on a random terminal," *Applied Sciences*, vol. 12, no. 5, p. 2301, 2022.

[26] J. Kang, K. Fan, K. Zhang, X. Cheng, H. Li, and Y. Yang, "An ultra light weight and secure rfid batch authentication scheme for iomt," *Computer Communications*, vol. 167, pp. 48–54, 2021.
[27] 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*, vol. 39, no. 2, pp. 346–360, 2020.
[28] S. U. Jan, S. Ali, I. A. Abbasi, M. A. Mosleh, A. Alsanad, and H. Khattak, "Secure patient authentication framework in the healthcare system using wireless medical sensor networks," *Journal of Healthcare Engineering*, vol. 2021, 2021.
[29] S. Yu and K. Park, "Puf-based robust and anonymous authentication and key establishment scheme for v2g networks," *IEEE Internet of Things Journal*, 2024.
[30] M. Wazid, A. K. Das, N. Kumar, M. Conti, and A. V. Vasilakos, "A novel authentication and key agreement scheme for implantable medical devices deployment," *IEEE journal of biomedical and health informatics*, vol. 22, no. 4, pp. 1299–1309, 2017.
[31] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *Journal of biomedical informatics*, vol. 55, pp. 272–289, 2015.
[32] S. Challa, M. Wazid, A. K. Das, and M. K. Khan, "Authentication protocols for implantable medical devices: Taxonomy, analysis and future directions," *IEEE Consumer Electronics Magazine*, vol. 7, no. 1, pp. 57–65, 2017.
[33] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. Rodrigues, and Y. Park, "Bakmp-iomt: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment," *IEEE Access*, vol. 8, pp. 95 956–95 977, 2020.
[34] M. Seifelnasr, R. AlTawy, A. Youssef, and E. Ghadafi, "Privacy-preserving mutual authentication protocol with forward secrecy for iot-edge-cloud," *IEEE Internet of Things Journal*, 2023.
[35] Z. Liu, L. Wan, J. Guo, *et al.*, "Ppru: A privacy-preserving reputation updating scheme for cloud-assisted vehicular networks," *IEEE Transactions on Vehicular Technology*, 2023.
[36] M. A. Saleem, X. Li, M. F. Ayub, S. Shamshad, F. Wu, and H. Abbas, "An efficient and physically secure privacy-preserving key-agreement protocol for vehicular ad-hoc network," *IEEE Transactions on Intelligent Transportation Systems*, 2023.
[37] M. A. Al Sibahee, V. O. Nyangaresi, Z. A. Abduljabbar, C. Luo, J. Zhang, and J. Ma, "Two-factor privacy preserving protocol for efficient authentication in internet of vehicles networks," *IEEE Internet of Things Journal*, 2023.
[38] M. Safkhani, C. Camara, P. Peris-Lopez, and N. Bagheri, "Rseap2: An enhanced version of rseap, an rfid based authentication protocol for vehicular cloud computing," *Vehicular Communications*, vol. 28, p. 100 311, 2021.
[39] M. Tanveer, A. U. Khan, H. Shah, A. Alkhayyat, S. A. Chaudhry, and M. Ahmad, "Arap-sg: Anonymous and reliable authentication protocol for smart grids," *IEEE Access*, vol. 9, pp. 143 366–143 377, 2021.
[40] H. Yu, N. Yao, T. Wang, G. Li, Z. Gao, and G. Tan, "Wdfad-dbr: Weighting depth and forwarding area division dbr routing protocol for uasns," *Ad Hoc Networks*, vol. 37, pp. 256–282, 2016.
[41] A. Mahmood, E. Sisinni, L. Guntupalli, R. Rondón, S. A. Hassan, and M. Gidlund, "Scalability analysis of a lora network under imperfect orthogonality," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1425–1436, 2018.
[42] M. Siddhartha, "Heart disease dataset (comprehensive)," *IEEE Dataport*, 2020.
[43] L. Xu, L. Chen, Z. Gao, X. Fan, T. Suh, and W. Shi, "Diota: Decentralized-ledger-based framework for data authenticity protection in iot systems," *IEEE Network*, vol. 34, no. 1, pp. 38–46, 2020.

B D Deebak (Member, IEEE) received his Ph.D. in computer science from SASTRA Deemed University, Thanjavur, India, in 2016. He is currently a Brain Pool Fellow with the Department of Computer Engineering at Gachon University, South Korea. His research interests include Information Security, Cryptography, Integrating AI with Cyber Security, IoT with 5G/6G, and Blockchain.

Seong Oun Hwang (Senior Member, IEEE) received his Ph.D. degree in computer science from the Korea Advanced Institute of Science and Technology, South Korea, in 2004. He is currently a Full Professor at the Department of Computer Engineering, Gachon University, South Korea. His research interests include cryptography, cybersecurity, data-centric artificial intelligence, and artificial intelligence.