Lightweight Mutual Authentication and Privacy-Preservation Scheme for Intelligent Wearable Devices in Industrial-CPS

Mian Ahmad Jan, *Senior Member, IEEE*, Fazlullah Khan, *Senior Member, IEEE*, Rahim Khan, *Member, IEEE*, Spyridon Mastorakis, *Member, IEEE*, Varun G. Menon, *Senior Member, IEEE*, Mamoun Alazab, *Senior Member, IEEE*, and Paul Watters, *Senior Member, IEEE*

***Abstract*—Industry 5.0 is the digitalization, automation, and data exchange of industrial processes that involve artificial intelligence, industrial Internet of Things (IIoT), and industrial cyber-physical systems (I-CPS). In healthcare, I-CPS enables the intelligent wearable devices to gather data from the real-world and transmit to the virtual world for decision-making. I-CPS makes our lives comfortable with the emergence of innovative healthcare applications. Similar to any other IIoT paradigm, I-CPS capable healthcare applications face numerous challenging issues. The resource-constrained nature of wearable devices and their inability to support complex security mechanisms provide an ideal platform to malevolent entities for launching attacks. To preserve the privacy of wearable devices and their data in an I-CPS environment, in this article we propose a lightweight mutual authentication scheme. Our scheme is based on client-server interaction model that uses symmetric encryption for establishing secured sessions among the communicating entities. After mutual authentication, the privacy risk associated with a patient data is predicted using an AI-enabled hidden Markov model. We analyzed the robustness and security of our scheme using Burrows–Abadi–Needham logic. This analysis shows that the use of lightweight security primitives for the exchange of session keys makes the proposed scheme highly resilient in terms of security, efficiency, and robustness. Finally, the proposed scheme incurs nominal overhead in terms of processing, communication and storage and is capable to combat a wide range of adversarial threats.**

***Index Terms*—Artificial intelligence (AI), authentication, client-server model, industrial cyber-physical systems (I-CPS), Industrial Internet of Things (IIoT), privacy, security.**

Manuscript received August 21, 2020; revised November 5, 2020; accepted December 1, 2020. Date of publication December 10, 2020; date of current version May 3, 2021. This work was supported by a pilot award from the Center for Research in Human Movement Variability and the NIH under Grant P20GM109090 and a planning award from the Collaboration Initiative of the University of Nebraska system. Paper no. TII-20-4001. *(Corresponding author: Fazlullah Khan.)*

Mian Ahmad Jan and Rahim Khan are with the Department of Computer Science, Abdul Wali Khan University Mardan, Mardan 23200, Pakistan.

Fazlullah Khan is with the Institute of Social and Economic Research, Duy Tan University, Da Nang 550000, Vietnam, and also with the Department of Computer Science, Abdul Wali Khan University Mardan, Mardan 23200, Pakistan (e-mail: fazlullahkhan@duytan.edu.vn).

Spyridon Mastorakis is with the Computer Science Department, University of Nebraska Omaha, Omaha, NE 68 182-0002 USA.

Varun G. Menon is with the Computer Science Engineering Department, SCMS Group of Educational Institutions, Ernakulam 683576, India.

Mamoun Alazab is with the Charles Darwin University, Casuarina, NT 0811, Australia.

Paul Watters is with the School of Engineering and Mathematical Sciences, La Trobe University Melbourne, Melbourne, VIC 3086, Australia.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2020.3043802.

Digital Object Identifier 10.1109/TII.2020.3043802

I. Introduction

THE latest developments in Industry 5.0 have enabled the integration of industrial Internet of Things (IIoT), industrial cyber-physical systems (I-CPS), big data technologies, cloud computing, and artificial intelligence (AI) [1]. It has resulted in collecting huge amounts of data from different industrial applications using intelligent IIoT devices. For example, in I-CPS enabled healthcare applications, wearable devices implanted on a patient body are capable to stream the real-time data to the cyberspace for computation, storage, and bigdata analytics [2]. I-CPS facilitate the healthcare entities with cyber computational capabilities for making quicker decisions. To deliver high-quality services at low cost, the healthcare practitioners need to adopt I-CPS based practices. In a healthcare ecosystem, the smart devices of IIoT are capable to gather, analyze, and broadcast a diverse range of data. These devices ensure the real-time monitoring of patients to save lives in an event of emergency, e.g., heart failure, severe pain, asthma, etc. The proliferation in mobile communication bridges the gap among these smart devices and the practitioners by providing seamless and reliable delivery of gathered data [3]. The patient-centric approach of I-CPS enables the remote monitoring of patients with shorter hospital stays and, in most cases, avoiding the hospital altogether. Using industrial techniques in I-CPS, we need to consider the patients' willingness and feelings about these techniques.

The increasing use of industrial techniques in I-CPS brings new risks, vulnerabilities, and challenges for practitioners and their patients. Not only the IIoT devices and their data, but the complete healthcare ecosystem needs to be secured against the adversarial attacks [4]. The IIoT devices hosting the healthcare applications contain sensitive information, e.g., date of birth, prescriptions, medical histories, and social security numbers of the patients. These devices act as gateways to the secured Internet. An adversary may compromise these devices to inject fabricated data, ransomwares and other malwares into the network [5]. In the traditional computing platforms, cybersecurity is a matured domain and can defend against most of these adversarial threats. The existing cybersecurity solutions include cryptographic techniques, secured protocols and privacy protections that require ample of network resources. However, the security requirements and system architecture of IIoT-based I-CPS are different and as such, these existing solutions are not directly applicable [6], [7]. In I-CPS, most of the devices are connected to the Internet for the first time. It is extremely difficult to predict the nature of adversarial threats posed by these devices, if compromised. To secure the I-CPS, data integrity, data confidentiality, data availability, authenticity, and nonrepudiation need to be in place [8].

I-CPS enabled healthcare applications consist of resource-constrained sensor nodes and requires lightweight and low-cost protective measures. To deal with the aforementioned challenges, datagram transport layer security (DTLS) is proposed as a lightweight secured approach for these applications of I-CPS [9]. In literature, numerous DTLS-enabled authentication approaches exist for secured data transmission, and privacy of patients in healthcare applications [8], [10]–[12]. In [10], the authors proposed an end-to-end authentication scheme for a mobility-enabled healthcare application. A certificate-based DTLS handshake approach is used for the end-users authentication and authorization. The proposed scheme provides robust mobility using the interconnected smart gateways at the expense of computational overhead due to the use of certificate-based DTLS. In [11], a secured authentication approach was proposed using a body sensor network. The use of crypto-primitives enable the proposed approach to achieve system efficiency and robustness, and at the same time, provides the transmission confidentiality and authentication among the wearables and a backend server. However, the use of an asymmetric algorithm, i.e., Elliptic-curve cryptography, incurs additional overhead for these intelligent wearables. In [12], the authors presented a lightweight DTLS-enabled authentication approach for wearables of a smart healthcare system. The proposed approach allows a user to authenticate his/her wearable device(s) and a mobile terminal, prior to establishing a session key among them. The use of bitwise exclusive-OR (XOR) and hash functions make the proposed scheme significantly lightweight for the resource-constrained wearables. The security analysis of DTLS via different techniques, such as the random oracle model [13] and the Burrows–Abadi–Needham (BAN) logic [14], showed that the use of DTLS for secured message exchanges leaves a handful of payload for most of healthcare applications. This remaining payload is not sufficient for these applications due to their larger packet sizes, e.g., healthcare streaming applications.

Besides authentication, the privacy of patients and their data needs to be dealt with utmost care in I-CPS. Different machine learning (ML) algorithms have been used in the literature for this purpose. An ML-based privacy-preserved healthcare framework was presented in [15]. This framework uses ML-based scoring service for the classification, and cryptographic algorithms for data protection. It is a cloud-based framework for privacy risk prediction in healthcare applications. In [16], the authors have provided general guidelines about privacy challenges in AI-based healthcare applications. The proposed work mainly focuses on policies for the usage of AI-based healthcare guidelines to preserve the privacy of patients. In [17], the authors have proposed a framework known as ModelChain. This framework uses ML and blockchain for privacy preservation of patients in a decentralized environment. ModelChain embeds the intelligence in private blockchains to preserve the privacy of patients and increases the interoperability between healthcare centers. In [18], the authors have discussed AI-based cyber-physical security and privacy for healthcare applications. They proposed a ciphertext-policy attribute-based encryption scheme. In the proposed scheme, complex computation tasks are offloaded to the third parties for reducing load on wearables while preserving their privacy at the same time. Most of these approaches use asymmetric encryption that require ample resources on part of the wearables to perform effectively.

In view of the resource-constrained nature of the healthcare devices, we propose a lightweight mutual authentication scheme for I-CPS. The proposed scheme uses symmetric encryption for the exchange of handshake messages that can be used as an alternative to the DTLS scheme. We perform its security analysis using BAN logic to determine whether the exchanged information is trustworthy and secured against eavesdropping attack, and predict the privacy leakage using a hidden Markov model (HMM). The hidden and observable states of HMM are used to measure the risk of data leakage by preserving the privacy of a patient and his/her connected devices. The major contributions of the proposed work are as follows.

1) An authentication scenario is proposed in which a client-server authentication takes place only if the clients, i.e., wearable patients, are within the coverage of their designated servers. Each server maintains a record of preshared keys for the clients in its proximity. For the aforementioned scenario, a set of theorems are proposed and their proofs are provided. Each theorem corresponds to a handshake message that takes into account the possibility and probability of an adversarial attack.
2) A privacy risk prediction model is proposed using HMM. The proposed model is used to predict the risk of privacy leakage of the patient identity and his/her data. If the privacy risk is predicted, the patients' data is altered with a loss in utility. To the best of our knowledge, this is the first ever work on HMM for predicting the privacy leakage.
3) Security analysis of mutual authentication and session key exchange of our proposed scheme is performed using

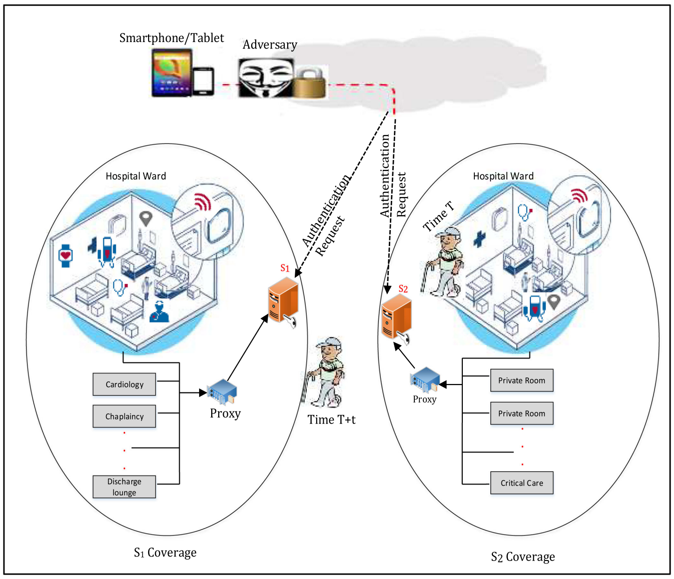


Fig. 1. Smart and secured healthcare facilitation center.

BAN logic. The security goals are set according to the exchanged messages and are proven using the postulates of BAN logic.

The rest of the article is organized as follows. In Section II, the network and threat model is briefly explained. In Section III, our proposed lightweight mutual authentication and privacy-preservation scheme are presented. In Section IV, the security analysis of the proposed scheme is performed using BAN logic. In Section V, we present the experimental results of our proposed scheme. Finally, the article is concluded in Section VI.

II. Network and Threat Model

We have considered a healthcare facilitation center, i.e., a hospital within an industry, as a case study of our proposed I-CPS scheme. Various units such as critical care, chaplaincy, cardiology, radiology, wards, and discharge lounge, along with private rooms provide timely healthcare facilities to the patients. These units and rooms are connected to remote servers for storing the patients' data and other credentials to provide on-demand and responsive services. In Fig. 1, the sensor-embedded wearables, i.e., clients, in various units and rooms are connected to servers via their proxies. Each server facilitates a number of clients within its coverage region. A client is static in the context of the server's coverage region, i.e., a client remains within the coverage region of its associated server. For seamless and interoperable communication, these clients need to establish secured communication links to their concerned servers.

In healthcare applications, any adversarial attack can lead to the loss of precious lives and the associated medical data. An adversary may establish secured connections to the servers if its authentication requests are accepted. The smart healthcare environment of Fig. 1 is prone to various types of adversarial attacks. An adversary may infiltrate the network by seizing the identities of clients and servers to pose various threats. It is important to mention that in Fig. 1 the adversary uses a smartphone to launch the attacks. Moreover, it may clone itself for a large-scale adversarial effect on the overall system. To prevent such threats, we propose a lightweight mutual authentication approach for resource-starving intelligent wearables. Our authentication approach is resilient against the following threats.

1) Replay: An adversary may replay a stream of previously transmitted messages to the clients or servers.
2) Forward and backward secrecy: An adversary may launch this attack by seizing the session key to predict the outcome of previous or future sessions.
3) Client and server impersonation: An adversary may impersonate a legitimate client to the server by fabricating the preshared key of the given client. Moreover, it may impersonate a legitimate server to one or more clients by fabricating the session key of the given server.
4) Anonymity and untraceability: An adversary may launch this attack by extracting the one-time nonces, and the identities of clients and servers from exchanged messages. In doing so, it may interlink various sessions to maliciously affect the clients and servers.
5) Eavesdropping: An adversary may launch active or passive eavesdropping by listening to the communication in transit. It may seize various messages, manipulate them, and may launch other types of attacks. The use of pseudorandom nonces in our approach restricts an adversary from launching this attack.
6) Denial of service (DoS): An adversary may broadcast excessive requests to the clients or servers to authenticate itself. By doing so, it may deprive the legitimate clients from exchanging their data with the legitimate servers. The use of preshared keys restricts an adversary from launching a DoS attack in our approach.

III. Lightweight Mutual Authentication and Privacy-Preservation Scheme

In this section, we discuss our mutual authentication and privacy preservation scheme for the healthcare facilitation center of Fig. 1. Numerous wearables within the hospital communicate with their concerned servers for authentication, as shown in Fig. 2. In this figure, A is the set of attackers, C is the set of clients, and S is the set of servers, where C_i can communicate either directly with S_j or via a proxy (P). Our proposed scheme comprises of C_i clients and S_j servers, where $i=\{1,2,3,\ldots,I\}$ and $j=\{1,2,3,\ldots,J\}$, such that $i,j \in N$, and $i > j$. Here, N is the total number of C_i and S_j in the network, i.e., $N=C_i \cup S_j$. C_i are dynamic in nature and may change their positions quite frequently, whereas S_j are static in nature. Our proposed scheme initiates a four-way handshake between any C_i and S_j for mutual authentication. If the handshake is successful, S_j provides a session key to C_i for data transmission. The list of Symbol used in authentication is given in Table I. We discuss mutual authentication in Section III-A and privacy risk prediction using HMM in Section III-B.

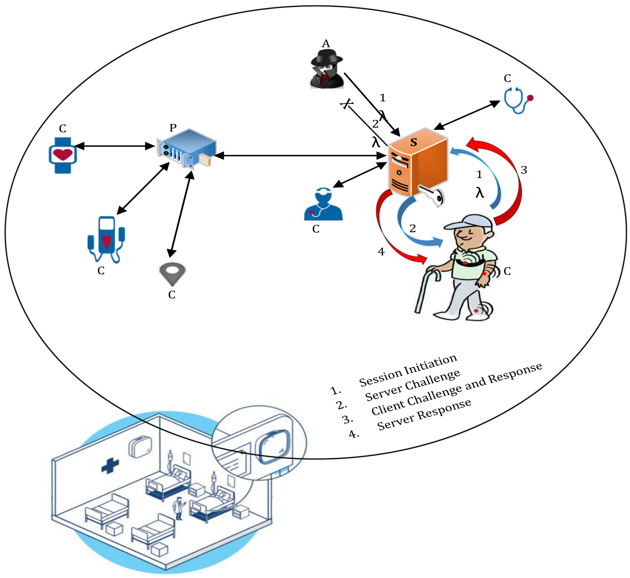


Fig. 2. Proposed mutual authentication scheme.

TABLE I
SYMBOLS AND MEANING USED IN AUTHENTICATION

Symbols	**Meanings**
C_i	Client i
S_j	Server j
A_k	adversary k
λ	128-bit pre-shared key
μ	128-bit session key
ID_i	Identity of Client i
h()	hash function
η	one-time 128-bit pseudo nonce
$\gamma_{challenge}$	256-bit server challenge
$\gamma_{response}$	Server response to client
$\beta_{challenge}$	256-bit client challenge

A. Mutual Authentication

Each C_i periodically collects the desired data and transmits to the nearest S_j. However, prior to the data transmission, both C_i and S_j need to be authenticated. Our lightweight authentication scheme verifies the identities of C_i and S_j before their engagement for data exchange. The authentication is performed using the following four handshake messages.

1) Session initiation.
2) Server challenge.
3) Client response and challenge.
4) Server response.

Initially, both C_i and S_j are assumed to be unauthentic, and thus, untrustworthy. Prior to mutual authentication, each C_i is assigned a unique 128-b preshared key (λ_i), and an identity (ID_i) in an offline phase. These secret primitives are also shared with their associated S_j, located in their vicinity. The offline phase is a prerequisite for the initialization of C_i and S_j, respectively. Next, each C_i initiates a session request to its associated S_j. This session initiation request contains the encrypted identity $\lambda_i(ID_i)_{h()}$ of C_i, i.e., ID_i is encrypted by C_i using its λ_i and hashed using $h()$. The transmitted request message is meaningless to the neighboring C_{i-1} clients and adversaries A_k, where $k=\{1, 2, 3, \ldots, K\}$, such that $k \notin \{i, j\}$. The recipient, be it C_i, S_j or A_k, needs to decrypt $\lambda_i(ID_i)_{h()}$ with the same λ_i and $h()$. Please note that the mode of wireless communication means that any device can intercept the session initiation request.

Theorem 1: At least one legitimate C_i, not an adversary A_k, initiates a session with the corresponding S_j.

Proof: Each C_i shares its λ_i with its associated S_j in an offline phase. The set of identities and keys of C_i, i.e., $\{ID_1, ID_2, ID_3, \ldots, ID_i\}$ and $\{\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_i\}$, respectively, are stored by S_j in a database. An A_k may initiate a session request by transmitting a message $\lambda_k(ID_k)_{h(ID_k)}$, encrypted with a fabricated λ_k and $h(ID_k)$. S_j checks the authenticity of this request by retrieving the corresponding decrypting key λ_k. Since, $\lambda_k \notin \{\ \lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_i\}$, S_j assumes that the request was initiated by an adversary. The λ_i for encryption and decryption is computed using the equality to compute λ_i and λ_i', respectively [19].

$\lambda_i =$ *from-state* $\oplus$ *Round*$_{0-9}$ $\oplus$ *Add-Round*$_{key}$ $\oplus$ *to-state* λ_i' $=$ *from-state* $\oplus$ *Round*$'_{0-9}$ $\oplus$ *Add-Round*$_{key}$ $\oplus$ *to-state*

Here, λ_i and λ_i' are the secret encryption and decryption keys, where λ_i=λ_i'. The only difference is that in λ_i, from-state represents the plain text and to-state represents the cipher text. For λ_i', from-state and to-state work oppositely to λ_i. Round is a function used to compute a unique key every time [19], as explained below.

Round$_0$ *state*$_{key}$ = *AddRound*$_{key}$ (*ShiftRows*(*SubBytes state*)) $\oplus$ (*Round*$_{n+1}$ *state*$_{key}$ = *Round*$_n$*state*$_{key}$ (*AddRound*$_{key}$ (*MixColumns* (*ShiftRows* (*SubBytes state*))))). where, AddRound is a pairwise XOR operation, ShiftRows applies permutation to the block, SubBytes applies an S-Box operation on every state and MixColumns transforms every column of the metric.

The session initiation request is terminated by S_j either by ignoring it or by sending a denial message, i.e., when $\lambda_k \notin \{\ \lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_i\}$. Hence, any C_i with an appropriate λ_i is capable of initiating the session with an S_j. Conversely, if the session initiation request, encrypted with λ_i, is received by an A_k, the latter is unable to decrypt it. This is because the λ'_i is known only to encrypting C_i and to the associated S_j.

Upon the reception of a session initiation request, S_j retrieves $\lambda_i(ID_i)_{h()}$ and decrypts it with λ'_i and $h()$ to check ID_i in it. If the embedded ID_i matches with an entry in S_j database, it means that the session initiation request was received from a legitimate C_i. At this point, S_j creates a challenge for the concerned C_i to confirm its authenticity by establishing a session with it. For this purpose, S_j generates a 128-b session key (μ_j), and a temporary one-time 128-b pseudononce (η_{server}). The nonce is computed by generating two pseudorandom numbers η_{s_1} and η_{s_2}, and an XOR operation is performed on them using (1).

$$\eta_{\text{server}} = \eta_{s_1} \oplus \eta_{s_2}. \tag{1}$$

Next, an XOR operation is performed on μ_j and λ_i, and their 128-b resultant is concatenated with η_{server}. Finally, $\lambda_i \oplus \mu_j|\eta_{\text{server}}$ is encrypted with λ_i and hashed with $h()$ to generate a

256-b server challenge ($\gamma_{\text{challenge}}$) as shown in (2). The advanced encryption standard (AES) of 128 b is used for symmetric encryption in Cipher block chaining mode.

$$\gamma_{\text{challenge}} = \text{AES}((\lambda_i, (\lambda_i \oplus \mu_j | \eta_{\text{server}}))_{h()}). \tag{2}$$

Theorem 2: An encrypted $\gamma_{\text{challenge}}$ is resolved **iff** a C_i or an A_k has the required λ'_i for decryption.

Proof: Any C_i receiving the $\gamma_{\text{challenge}}$ that contains μ_j needs to have the required λ'_i for decryption. Assume that the $\gamma_{\text{challenge}}$ is received by A_k, and $f(x_k)$ is the function used by A_k to compute a matching λ_i from the set $\{\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_i\}$ as shown in (3).

$$f(x_k) = \{S_j, (C_1, \lambda_1), (C_2, \lambda_2), (C_3, \lambda_3), ..(C_i, \lambda_i)\}. \tag{3}$$

Here, $\{C_1, C_2, C_3, \ldots, C_i\}$ represents the client devices' IDs that are generated by A_k based on historic data collection, and $\{\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_i\}$ are their dummy secret keys. These dummy keys are computed using (4).

$$\lambda_i = C_i \oplus statistics(\lambda_i). \tag{4}$$

Since, the $\gamma_{\text{challenge}}$ is encrypted with a particular λ_i known only to a legitimate C_i and S_j, A_k will compute and apply different λ_i values, as shown in (3), to decipher the cipher text of (2). However, the success probability is $\frac{1}{2^{128}}$. Thus, A_k will not be able to decrypt the $\gamma_{\text{challenge}}$ within a stipulated time. Conversely, if a C_i has the required λ_i, then it will decrypt $\gamma_{\text{challenge}}$ within its stipulated time. Hence, an encrypted $\gamma_{\text{challenge}}$ is resolved only by a single C_i that has the required λ_i.

Upon the reception of $\gamma_{\text{challenge}}$, if C_i successfully deciphers it, then it will have access to the corresponding η_{server} and μ_j. Additionally, it proves the authenticity of C_i to S_j. It is because η_{server} and μ_j are known only to a given S_j and λ_i to the concerned C_i. To authenticate an S_j, C_i generates a client challenge for the given S_j. Initially, a temporary one-time 128 b pseudononce (η_{client}) is computed by generating two pseudorandom numbers η_{c_1} and η_{c_2}. Next, an XOR operation is performed on them using (5).

$$\eta_{\text{client}} = \eta_{c_1} \oplus \eta_{c_2}. \tag{5}$$

Next, an XOR operation is performed on η_{server} and λ_i, their resultant is concatenated with η_{client}, and finally encrypted with μ_j to generate a 256-b client challenge $\beta_{\text{challenge}}$, as shown in (6).

$$\beta_{\text{challenge}} = \text{AES}((\mu_j, (\eta_{\text{server}} \oplus \lambda_i | \eta_{\text{client}}))_{h()}). \tag{6}$$

Theorem 3: An encrypted $\beta_{\text{challenge}}$ is resolved and responded **iff** a device, such as S_j, has the shared information, i.e., η_{server} and μ_j.

Proof: The μ_j and η_{server} are known only to a given C_i and S_j. Assume that an A_k receives $\beta_{\text{challenge}}$ and tries to decrypt it using a probabilistic function $g(x)$. This function is used to compute the desired μ_j by using (7).

$$g(x) = \text{probability}((C_1, \mu_1), (C_2, \mu_2), ..(C_i, \mu_j)). \tag{7}$$

The function $g(x)$ utilizes the C_i and S_j information to return a single pair of values for A_k, i.e., (ID_i, μ_j). However, this scenario is applicable only if A_k maintains a complete record of the overall communication between C_i and S_j, which is not a realistic assumption especially in a resource-constrained health-CPS environment. In addition to μ_j and λ_i values that are known only to C_i and S_j, A_k needs to verify its authenticity to C_i as well. Conversely, if $\beta_{\text{challenge}}$ is received correctly by the concerned S_j, then the latter deciphers $(\eta_{\text{server}} \oplus \lambda_i | \eta_{\text{client}})_{h()}$ of (6) correctly with μ_i and $h()$ to retrieve η_{client}. Thus, $\beta_{\text{challenge}}$ of a given C_i is resolved by a particular S_j that possesses the required μ_j.

Finally, during the server response, the concerned S_j creates a response by concatenating the C_i's η_{client} to its μ_j, and generates an encrypted server response (γ_{response}) using λ_i (8).

$$\gamma_{\text{response}} = \text{AES}((\lambda_i, \{\eta_{\text{client}} | \mu_j)_{h()}). \tag{8}$$

Upon reception, a C_i having a valid λ'_i will be able to decipher γ_{response} and retrieve η_{client} to confirm the authenticity of the given S_j.

Theorem 4: The encrypted γ_{response} of an S_j is decrypted by a C_i **iff** it has the required λ_i.

Proof: In the prerequisite offline phase, C_i shared their λ_i with their concerned S_j. The γ_{response} is decrypted by an A_k only if it has the required λ_i, which is not the case. An A_k uses the functions $f(x)$ and $g(x)$, as discussed earlier, to find an exact copy of λ_i.

$$\lambda_i = f(x) \oplus g(x). \tag{9}$$

Where, $f(x)$ and $g(x)$ return a pair of values, i.e., (C_i,λ_i) and (C_i,μ_j), respectively. However by adopting the approach of (9), A_k will only be able to obtain μ_j at the expense of excessive resource consumption. However, it will still not be able to collect the desired λ'_i that is required to decrypt γ_{response}. Conversely, if γ_{response} is received by the concerned C_i having the appropriate λ_i, it will be able to decrypt this message within the stipulated time. Thus, a given C_i having λ_i is able to successfully decrypt the γ_{response} of C_i. Upon successful decryption of γ_{response}, both C_i and S_j have mutually authenticated each other and are authorized to exchange data. After successful authentication, data are transmitted from C_i to S_j. During data transmission and storage at S_j, the C_i privacy can be leaked, and hence needs to be preserved. To solve the privacy leakage issues, we use HMM to predict the privacy of C_i. In the next section, we present an approach to predict the privacy risks of C_i using HMM.

B. Privacy Risk Prediction Using HMM

In this section, we predict the risk of a client's privacy leakage using HMM. In HMM, states are partially observed that helps in solving real-world problems using sequential or temporal data. The aim of the proposed model is to measure the risk of data privacy leakage using HMM. The graphical representation of HMM is shown in Fig. 3. The HMM uses two sets of random variables, hidden variable $\mathbf{H} = \{H_1, H_2, \cdots, H_m\}$ and observed variable $\mathbf{O} = \{O_1, O_2, \cdots, O_n\}$, where $\mathbf{O} \in$ {discrete values, real values, R^d}. In our proposed scheme, $\mathbf{H}$ is the data generated by the patients and $\mathbf{O}$ is the usage pattern of C_i devices associated

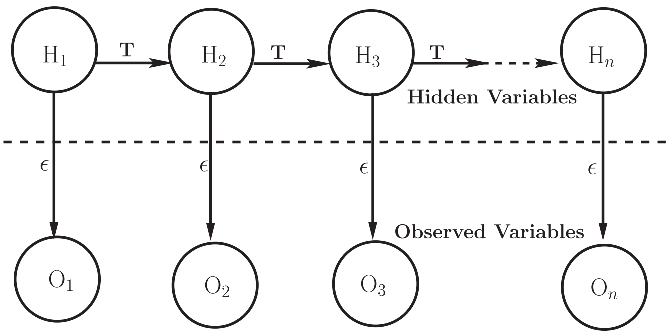


Fig. 3. Graphical demonstration of HMM.

with a patient. The joint probability distribution of HMM in terms of **H** and **O** is given in (10).

$$P(O_1, O_2, \ldots, O_n, H_1, H_2, \ldots, H_n)$$
$$= P(H_1)P(O_1|H_1)\prod_{k=2}^{n} P(H_k|H_{k-1})P(O_k|H_k). \tag{10}$$

1) Probabilities of the HMM: The HMM works on the initial probability $\pi(i)$, the observation probability $E_i(O)$, and the transition probability $T_{(ij)}$. The initial probability ($\pi(i)$) of a patient's data in the context of HMM is given in (11),

$$\pi(i) = P(H_1 = i), \text{for } i \in \{1, 2, \ldots, m\}. \tag{11}$$

where, $\pi(i)$ is based on the previous data shared by a patient, which include personal identification (PI) such as patient's name, patient's location, and his/her illness, etc. $\pi(i)$ is important in the privacy risk identification because it reveals PI of a patient that can be linked to anonymized data shared by the patient using HMM. The initial risk probability of a client C_i is computed by observing data D_t. (11) can be re-written as

$$\pi(C_i) = \begin{cases} p(C_i|D_t) > 0, & \text{for a patient having a shared PI} \\ p(C_i|D_t) = 0, & \text{for a patient having no shared PI} \end{cases}. \tag{12}$$

E_i is the probability distribution on **O**, which can be defined as a probability density function for $\{H_1, H_2, \cdots, H_m\}$ and $\forall\, O \in \mathbf{O}$, it can be written as

$$E_i(O) = P(O|H_k = i), \text{for } i \in \{1, \ldots, m\}, \text{and } O \in \mathbf{O}. \tag{13}$$

When **O** takes discrete random numbers, then (13) can be written as the probability mass function as shown in (14).

$$E_i(O) = P(O_k = O|H_k = i), \text{for } i \in \{1, \ldots, m\},$$
$$\text{and } O \in \mathbf{O}. \tag{14}$$

E_i is the probability of the data stored previously by C_i that can reveal the consistency in the patient data and his/her usage pattern. We modeled E_i as the probability of data (D_t) shared by various patients in (12). It is needed to embed inconsistency in the frequency of data sharing by a patient. The data frequently shared by a patient reveal his/her concern of causing higher risk, that can easily be inferred from the shared data. To increase the inconsistency in the patient data and reduce the privacy risk, a weight is multiplied with each probability and then it is inversed, as shown in (15).

$$W_{E_i(O)} = 1 - \frac{p(C_i|D_t)}{\text{count}(C_i|D_t)}. \tag{15}$$

where, $1/\text{count}(C_i| D_t)$ is the weight multiplied to each probability.

The transition probability T_{ij} is given in (16), which is the conditional probability of current data given a sequence of previously shared data.

$$T_{ij} = P(H_{k+1} = j|H_k = i), \forall\, i, j \in \{1, 2, \ldots, m\}. \tag{16}$$

Eq. (16) models the distinctiveness of a patient's data from all other patients because the data distinguishability depends on the previous data. The T_{ij} between $p(O_j| O_{j-1})$ are weighted by the number of occurring transitions. To decrease the distinctiveness and privacy risk in the patient data, weighted transition probabilities are computed as in (17).

$$W_{T_{ij}} = \frac{p(O_j|O_{j-1})}{\text{count}(O_j|O_{j-1})}. \tag{17}$$

where, $1/\text{count}(O_j| O_{j-1})$ is the weight multiplied to each probability.

The probability of a patient's (C_i) privacy along with a sequence of his/her observed data $O_1 \to O_2 \to \cdots \to O_j$ is calculated based on the Markov probability of (10),

$$p(O_1, \ldots, O_j|C_i) = \min(\text{HMM}_{PI|C_i}) \times \omega_T$$
$$\times\ p(O_1) \times (1 - \omega_O \times p(C_i|O_1))$$
$$\times \prod_{k=2}^{n} \omega_T \times p(O_k|O_{k-1}) \times (1 - \omega_O \times p(C_i|O_k)) \tag{18}$$

where, ω_T is $1/\text{count}(O_j| O_{j-1})$, and ω_O is $1/\text{count}(C_i| D_t)$. The $\text{HMM}_{PI|C_i}$ returns the list of privacy probabilities computed from the PI. It includes probabilities from the paths where E_i of a patient is greater than 0.

Upon identification of the privacy risk using (18), we alter the data to circumvent the privacy risk with a utility loss (ul). The ul uses a semantic similarity function [20], [21] to distinguish the original data D_t from the altered data D'_t, which is calculated as

$$ul(D, D') = 1.0 - \text{sim}(D, D') \tag{19}$$

The similarity function (sim) returns values within the range [0,1]. The higher the similarity is, the lower ul is by using altered data. In this fashion, using HMM, the privacy of C_i is preserved. After privacy preservation, we need to analyze the correctness and efficiency of our proposed scheme. In the next section, we perform the security analysis of the proposed scheme using BAN logic.

IV. Security Analysis

In this section, we analyze the mutual authentication and session key (μ) of our proposed scheme using BAN logic [22]. BAN logic describes the trust of two parties involved in the

TABLE II
NOTATIONS AND RULES USED IN BAN LOGIC

Notations	Meanings
$P \mid\equiv X$	P believes X
$P \lhd X$	P sees X or P receives X
$P \mid\sim X$	P once said X
$P \mid\Rightarrow X$	P has jurisdiction over X
#(X)	X is fresh
$P \xleftrightarrow{K} Q$	P and Q may use the shared key K
$(X)_K$	X hashed under the key K
$\{X\}_\lambda$	X encrypted under the key K
Rule-1	Message meaning rule
Rule-2	Nonce verification rule
Rule-3	Jurisdiction rule
Rule-4	Freshness conjuncatenation rule

communication. The notations and rules used in BAN logic are given in Table II.

1. The Postulates of BAN logic are given below,

1) Postulate of Rule-1 is,

$$\lambda_i = \frac{S_j \text{ believes } C_i \xleftrightarrow{\lambda_i} S_j, S_j \text{ sees}\{X\}_{\lambda_i}}{S_j \text{ believes } C_i \text{ said X}}$$

2) Postulate of Rule-2 is,

$$\frac{S_j \text{ believes fresh (X)}, S_j \text{ believes } C_i \text{said X}}{S_j \text{ believes } C_i \text{ believes X}}$$

3) Postulate of Rule-3 is,

$$\frac{S_j \text{ believes } C_i \text{ controls X}, S_j \text{ believes } C_i \text{ believes X}}{S_j \text{ believes X}}$$

4) Postulate of Rule-4 is,

$$\frac{S_j \text{ believes fresh (X)}}{S_j \text{ believes fresh (X,Y)}}$$

2. The following security goals must be met by the proposed scheme,

G_1. $S_j| \equiv C_i \Rightarrow \mu_j$
G_2. $C_i| \equiv S_j \Rightarrow \mu_j$
G_3. $S_j| \equiv C_i| \equiv S_j \xleftrightarrow{\mu_j} C_i$
G_4. $C_i| \equiv S_j| \equiv C_i \xleftrightarrow{\mu_j} S_j$

3. The proposed scheme should be transformed into an idealized form as below,

Msg_1. $C_i \rightarrow S_j : (\lambda_i(ID_i))_{h()}$
Msg_2. $S_j \rightarrow C_i : (\lambda_i(\lambda_i \oplus \mu_j||\eta_{server}))_{h()}$
Msg_3. $C_i \rightarrow S_j : (\mu_j(\eta_{server} \oplus \lambda_i||\eta_{client}))_{h()}$
Msg_4. $S_j \rightarrow C_i : (\lambda_i(\eta_{client}||\mu_j))_{h()}$

4. The following assumptions are mandatory for BAN logic.

A_1. $C_i| \equiv S_j \xleftrightarrow{\lambda_i} C_i$
A_2. $S_j| \equiv C_i \xleftrightarrow{\lambda_i(ID_i)} S_j$
A_3. $C_i| \equiv S_j \xleftrightarrow{\lambda_i(\eta_{server})} C_i$
A_4. $S_j| \equiv C_i \xleftrightarrow{\lambda_i(\eta_{client})} S_j$
A_5. $C_i| \equiv \#(\lambda_i(\eta_{server}))$
A_6. $S_j| \equiv \#(\lambda_i(\eta_{client}))$
A_7. $S_j| \equiv C_i \Rightarrow S_j \xleftrightarrow{\mu_j} C_i$
A_8. $C_i| \equiv S^{\lambda_i}\ C_i \xleftrightarrow{\mu_j} S_j$

5. We analyze security of the proposed scheme based on the idealized form,

s_1. From Msg_1, we obtain $S_j \lhd (\lambda_i(ID_i))_{h()}$

s_2. Applying Rule-1 and A_2, we get $S_j| \equiv C_i| \sim (\lambda_i(ID_i))_{h()}$

s_3. Applying Rule-4 and A_6, we obtain $S_j| \equiv \#((\lambda_i(ID_i))_{h()})$
Then, we apply Rule-2 to get $S_j| \equiv C_i| \equiv \#(\lambda_i(ID_i))_{h()}$

s_4. From Msg_2, we obtain $C_i \lhd (\lambda_i(\lambda_i \oplus \mu_j||\eta_{server}))_{h()}$

s_5. Applying Rule-1 and A_1, we get $C_i| \equiv S_j| \sim (\lambda_i(\lambda_i \oplus \mu_j||\eta_{server}))_{h()}$

s_6. Applying Rule-4 and A_5, we obtain $C_i| \equiv \#(\lambda_i(\lambda_i \oplus \mu_j||\eta_{server}))_{h()}$
Then, we apply Rule-2 to get $C_i| \equiv S_j| \equiv (\lambda_i(\lambda_i \oplus \mu_j||\eta_{server}))_{h()}$

s_7. From Msg_3, we obtain $S_j \lhd (\mu_j(\eta_{server} \oplus \lambda_i||\eta_{client}))_{h()}$

s_8. Applying Rule-1 and A_2, we get $S_j| \equiv C_i| \sim (\mu_j(\eta_{server} \oplus \lambda_i||\eta_{client}))_{h()}$

s_9. Applying Rule-4 and A_6, we obtain $S_j| \equiv \#(\mu_j(\eta_{server} \oplus \lambda_i||\eta_{client}))_{h()}$
Then, we apply Rule-2 to get $S_j| \equiv C_i| \equiv (\mu_j(\eta_{server} \oplus \lambda_i||\eta_{client}))_{h()}$

s_{10}. From Msg_4, we obtain $C_i \lhd (\lambda_i(\eta_{client}||\mu_j))_{h()}$

s_{11}. Applying Rule-1 and A_1, we get $C_i| \equiv S_j| \sim (\lambda_i(\eta_{client}||\mu_j))_{h()}$

s_{12}. Applying Rule-4 and A_5, we obtain $C_i| \equiv \#(\lambda_i(\eta_{client}||\mu_j))_{h()}$
Then, we apply Rule-2 to get $C_i| \equiv S_j| \equiv (\mu_j(\eta_{server} \oplus \lambda_i||\eta_{client}))_{h()}$

s_{13}. Applying the logic rule of BAN to s_{12} and A_4, which split conjunctions that yields $C_i| \equiv S_j| \equiv C_i \xleftrightarrow{\mu_j} S_j$, (Goal 4)

s_{14}. Applying the logic rule of BAN to s_9 and A_3, which split conjunctions that yields $S_j| \equiv C_i| \equiv S_j \xleftrightarrow{\mu_j} C_i$, (Goal 3)

s_{15}. Applying Rule-3 to s_{13} and A_8, which results in $C_i| \equiv S_j \Rightarrow \mu_j$, (Goal 2)

s_{16}. Applying Rule-3 to s_{14} and A_7, which results in $S_j| \equiv C_i \Rightarrow \mu_j$, (Goal 1)

By performing the security analysis of our proposed scheme using BAN logic, the four security goals G_1, G_2, G_3, and G_4 are achieved. In the next section, we present the experimental results of our proposed scheme.

V. EXPERIMENTAL RESULTS

In this section, we evaluate the performance of our approach against existing state of the art schemes. For authentication, we used Netduino Plus 2 boards as clients and Netduino 3 boards as servers. The Netduino 3 boards were interfaced with MATLAB ThingSpeak server via the μ PLibrary 1.8.[1] This library abstracts the ThingSpeak API and works with these boards using. NET Micro Framework. For privacy-preservation, we relied on MATLAB simulation at the ThingSpeak server. We evaluate the performance of our approach in term of computational, communication, storage overheads, and its resilience against various adversarial threats. These boards are resource-constrained and as such, lightweight authentication approaches need to be designed. For this purpose, we tested our proposed authentication in terms of computation, communication, and storage overhead incur by our authentication. For privacy preservation, we tested our approach through privacy risk prediction and privacy risk alleviation.

[1][Online]. Available: https://www.nuget.org/packages/uPLibrary

TABLE III
COMPUTATIONAL OVERHEAD COMPARISON

Schemes	Client Side	Server Side	Total Cost
Li et. al [23]	$3T_h$+$7T_{XOR}$	$4T_h$+$12T_{XOR}$	$7T_h$+$19T_{XOR}$
Gupta et. al [6]	$4T_h$ +$4T_{XOR}$	$5T_h$+$3T_{XOR}$	$9T_h$ +$7T_{XOR}$
Gope et. al [7]	$3T_h$+$1T_{XOR}$	$9T_h$+$4T_{XOR}$	$12T_h$+$5T_{XOR}$
Chang et. al [9]	$5T_h$+$4T_{XOR}$	$8T_h$+$1T_{XOR}$	$13T_h$+$5T_{XOR}$
Proposed Scheme	$2T_h$+$2T_{XOR}$	$2T_h$+$2T_{XOR}$	$4T_h$+$4T_{XOR}$

TABLE IV
COMMUNICATION OVERHEAD COMPARISON

Schemes	Number of messages	Number of bits
Li et. al [23]	4	4672
Gupta et. al [6]	5	3808
Gope et. al [7]	4	3184
Chang et. al [9]	4	3104
Proposed Scheme	4	896

TABLE V
STORAGE OVERHEAD COMPARISON

Schemes	Client Side	Server Side
Li et. al [23]	$(ID_i+\lambda_i)$+ $(ID_G+\lambda_G)$	$n(ID_i+\lambda_i)$ + $m(ID_G+\lambda_G)$
Gupta et. al [6]	-	-
Gope et. al [7]	-	-
Chang et. al [9]	$(ID_i+\lambda_i)$+ $(ID_G+\lambda_G)$	$n(ID_i+\lambda_i)$ + $m(ID_G+\lambda_G)$
Proposed Scheme	$ID_i+\lambda_i$	$n(ID_i+\lambda_i)$

TABLE VI
RESILIENCE AGAINST VARIOUS ATTACKS

Attacks	*[23]*	*[6]*	*[7]*	*[9]*	*Proposed*
Replay	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Eavesdropping	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Forward & Backward Secrecy	*Yes*	*Yes*	*Yes*	*No*	*Yes*
Client Impersonation	*No*	*Yes*	*Yes*	*Yes*	*Yes*
Server Impersonation	*No*	*Yes*	*Yes*	*Yes*	*Yes*
Anonymity	*No*	*Yes*	*No*	*No*	*Yes*
DoS	*No*	*No*	*No*	*No*	*Yes*

In Table III, we provide a summary of the computational overhead analysis. We compare the execution time of our scheme against the existing schemes. In this table, T_h and T_{XOR} refer to the computational time needed to perform the hash and XOR operations. In our scheme, the encryption with λ_i and μ_j works similar to hashing. The proposed scheme requires only $2T_h$+$2T_{XOR}$ execution time at the C_i and S_j. The low computational overhead is contributed mainly to the lightweight mechanism adopted by $\lambda_k(ID_k)_{h()}$, $\gamma_{\text{challenge}}$, $\beta_{\text{challenge}}$, and γ_{response} of the proposed scheme.

In Table IV, we provide a summary of the communication overhead analysis of our scheme against the existing schemes. The proposed scheme requires four handshake messages for the authentication. In this scenario, $\lambda_k(ID_k)_{h()}$ is 128 b, and $\gamma_{\text{challenge}}$, $\beta_{\text{challenge}}$, and γ_{response} are 256 b each. Hence, total of 896 b communication overhead is incurred by these messages. In comparison, the existing schemes have much higher communication overhead due to the complex cipher-suites and the involvement of resource-intensive operators.

In Table V, we compare the storage overhead incurred by C_i and S_j of our proposed authentication scheme. In the proposed scheme, each C_i stores its ID_i and λ_i, respectively. On the other hand, each S_j stores ID_i and λ_i for n clients associated with it. In comparison, in [23] and [9], each C_i stores its ID_i and λ_i along with ID_G and λ_G of the gateway. In these schemes, each C_i is connected to its S_j via a gateway. Moreover, each S_j in these schemes incur excessive storage overhead as they need to store the security primitives of n clients and m gateways. As discussed earlier, λ_i is of 128 b. Thus, the cost incurred by S_j is n times higher than C_i for storing λ_i of n clients in [23] and it is m times higher than C_i for storing λ_G of m gateways. Similar to [23], the cost incurred by S_j is n times higher than C_i for storing λ_i of n clients, and it is m times higher than C_i for storing λ_G of m gateways.

In Table VI, the resilience of our scheme against various adversarial attacks is compared with the existing schemes. In our scheme, η_{client} and η_{server} are generated by a pseudorandom number R_i and appended to a timer T_i. This combination of T_i and R_i makes it extremely difficult for an adversary to replay messages. In our scheme, the use of one-time nonces η_{client} and η_{server} restrict the adversary from active eavesdropping. An A_k may compromise the μ_j; however, the latter does not reveal any information about the previous or future sessions. This is mainly because μ_j is a one-time session key generated every time. Hence, forward and backward secrecy are maintained by our scheme. An A_k may intercept the exchanged handshake messages $\langle \lambda_i(ID_i)_{h()}, \gamma_{\text{challenge}}, \beta_{\text{challenge}}, \gamma_{\text{response}} \rangle$ and may generate different message patterns such as $\langle \lambda_k(ID_k)_{h()}, \gamma^k_{\text{challenge}}, \beta^k_{\text{challenge}}, \gamma^k_{\text{response}} \rangle$. The A_k may impersonate as C_i by transmitting $\lambda_k(ID_k)_{h()}$, and $\beta^k_{\text{challenge}}$ to S_j. Also, the same A_k impersonates as S_j by transmitting $\gamma^k_{\text{challenge}}$ and $\gamma^k_{\text{response}}$ to C_i. To impersonate as C_i or S_j, A_k would need λ_i. Because, A_k fabricates its own λ_k that does not exist either with C_i or S_j, i.e., $\lambda_k \neq \lambda_i$, hence it is unable to launch client or server impersonation attack. Moreover, A_k would need to fabricate η_k, μ_k, and ID_k as well to launch these attacks. These parameters are computationally inefficient to be calculated as each one would require 2^{128} attempts. In our scheme, the identities of C_i and S_j are masked in the messages $(\lambda_i(ID_i))_{h()}$, $\gamma_{\text{challenge}}$, $\beta_{\text{challenge}}$, and γ_{response}. An A_k cannot interpret the identities of C_i

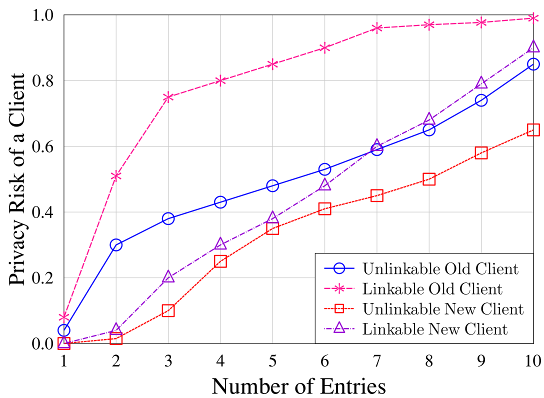


Fig. 4. Privacy risk prediction against number of entries.

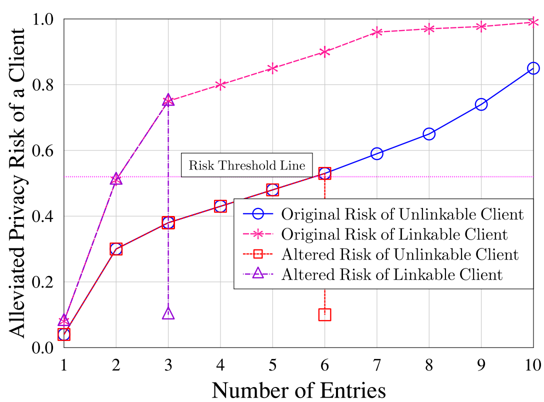


Fig. 5. Privacy risk alleviation against number of entries.

and S_j from the aforementioned messages as they are protected upon encryption by λ_i and μ_j. As a result, the anonymity of C_i and S_j is preserved. Moreover, our proposed scheme uses fresh nonces, i.e., η_{client} and η_{server} for every new session, and a new timer T_i as well. Hence, all sessions are nonlinkable and A_k is unable to trace any C_i and S_j from previous messages, thus providing untraceability feature. Finally, S_j restricts a C_i to only one connection at a given time. As a result, it is extremely difficult for an adversary to launch a DoS attack. In comparison to our scheme, all the existing schemes are susceptible to one or more such attacks and affect the privacy of C_i and S_j in one way or the other.

Our proposed scheme has used HMM to predict the privacy leakage of a client. In Fig. 4 , we have shown the client's privacy risk against the number of entries. The privacy risk is associated with the number of visits, i.e., entries, a client makes to a hospital server. As evident from this figure, the privacy of linkable clients is higher than unlinkable clients, where a linkable client is the one whose personal identification can be extracted from entries and search results on a particular topic. For example, when a client searched for a specialist practitioner and read his/her profile or read about a particular disease etc. When a client visits the hospital server for the first time, his/her privacy risk is relatively low and increases with each entry to the hospital server. If the personal identification of this new client is linkable, the privacy risk is higher in comparison to unlinkable client. Similarly, for old linkable clients, the privacy risk is highest and is moderate for unlinkable clients. The proposed scheme preserve the privacy of clients by predicting the privacy leakage using HMM. When the predicted privacy leakage crosses a specified threshold, the risk is altered, as shown in Fig. 5. The threshold is probabilistic and application-dependent that can be changed according to the application requirements. In this article, the threshold probability is 0.52, and once privacy leakage crosses it, the client's information is altered, and risk is alleviated, as shown in Fig. 5.

VI. Conclusion

In this article, we proposed a lightweight mutual authentication and key establishment scheme for IIoT wearable devices of I-CPS. The proposed scheme was based on client-server interaction model that used symmetric encryption. It was extremely lightweight and was suitable for large-scale I-CPS infrastructures. It was feasible for clients having limited resources and requires low computational, communication, and storage overhead while interacted with the servers for the exchange of session keys. After authentication, the privacy leakage of clients and their data was predicted using HMM. Upon privacy leakage detection, the data were altered through semantic similarity function with a loss in utility. The efficiency, correctness, and robustness of the security scheme were analyzed using BAN logic. The analysis showed that the proposed scheme was highly resilient against various adversarial attack. Moreover, it was efficient in terms of computation, communication, and storage overhead due to lightweight primitives, fewer number of exchanged messages and the absence of gateways, respectively. In the future, we aimed to use software-defined network for analyzed the exchanged data and the behavior of interacting entities of our scheme.

References

[1] Z. Lv, H. Song, P. Basanta-Val, A. Steed, and M. Jo, "Next-generation big data analytics: State of the art, challenges, and future research topics," *IEEE Trans. Ind. Informat.*, vol. 13, no. 4, pp. 1891–1899, Aug. 2017.

[2] J. Xu, L. Wei, W. Wu, A. Wang, Y. Zhang, and F. Zhou, "Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber–physical system," *Future Gener. Comput. Syst.*, vol. 108, pp. 1287–1296, 2018.

[3] F. Al-Turjman and S. Alturjman, "Context-sensitive access in industrial internet of things (IIoT) healthcare applications," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2736–2744, Jun. 2018.

[4] E. Luo, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and M. Atiquzzaman, "Privacyprotector: Privacy-protected patient data collection in IoT-based healthcare systems," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 163–168, Feb. 2018.

[5] H. Tao, M. Z. A. Bhuiyan, A. N. Abdalla, M. M. Hassan, J. M. Zain, and T. Hayajneh, "Secured data collection with hardware-based ciphers for IoT-based healthcare," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 410–420, Feb. 2019.

[6] A. Gupta, M. Tripathi, T. J. Shaikh, and A. Sharma, "A lightweight anonymous user authentication and key establishment scheme for wearable devices," *Comput. Netw.*, vol. 149, pp. 29–42, 2019.

[7] P. Gope and T. Hwang, "A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 63, no. 11, pp. 7124–7132, Nov. 2016.

[8] J. Srinivas, A. K. Das, N. Kumar, and J. Rodrigues, "Cloud centric authentication for wearable healthcare monitoring system," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 5, pp. 942–956, Sep./Oct. 2020.

[9] C.-C. Chang and H.-D. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 357–366, Jan. 2016.
[10] S. R. Moosavi *et al.*, "End-to-end security scheme for mobility enabled healthcare Internet of Things," *Future Gener. Comput. Syst.*, vol. 64, pp. 108–124, 2016.
[11] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wirelessbody area networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 332–342, Feb. 2014.
[12] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K.-K. R. Choo, and Y. Park, "Design of secure and lightweight authentication protocol for wearable devices environment," *IEEE J. Biomed. Health Informat.*, vol. 22, no. 4, pp. 1310–1322, Jul. 2018.
[13] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited," *J. ACM*, vol. 51, no. 4, pp. 557–594, 2004.
[14] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proc. Roy. Soc. London A. Math. Phys. Sci.*, vol. 426, no. 1871, pp. 233–271, 1989.
[15] K. Fritchman *et al.*, "Privacy-preserving scoring of tree ensembles: A novel framework for ai in healthcare," in *Proc. IEEE Int. Conf. Big Data*, 2018, pp. 2413–2422.
[16] I. Bartoletti, "Ai in healthcare: Ethical and privacy challenges," in *Proc. Conf. Artif. Intell. Med. Eur.*, 2019, pp. 7–10.
[17] T.-T. Kuo and L. Ohno-Machado, "Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks," Cornell Univ., 2018, pp. 1–13, *arXiv:1802.01746*.
[18] S. Wang *et al.*, "A fast CP-ABE system for cyber-physical security and privacy in mobile healthcare network," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4467–4477, Jul./Aug. 2020.
[19] J. Duan, J. Hurd, G. Li, S. Owens, K. Slind, and J. Zhang, "Functional correctness proofs of encryption algorithms," in *Proc. Int. Conf. Log. Program. Artif. Intell. Reasoning*, 2005, pp. 519–533.
[20] R. Masood, D. Vatsalan, M. Ikram, and M. A. Kaafar, "Incognito: A method for obfuscating web data," in *Proc. World Wide Web Conf.*, 2018, pp. 267–276.
[21] L. Lyu, K. Nandakumar, B. Rubinstein, J. Jin, J. Bedo, and M. Palaniswami, "PPFA: Privacy preserving fog-enabled aggregation in smart grid," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3733–3744, Aug. 2018.
[22] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, S. Kumari, and M. Jo, "Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2884–2895, Aug. 2018.
[23] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K.-K. R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Comput. Netw.*, vol. 129, pp. 429–443, 2017.

Mian Ahmad Jan (Senior Member, IEEE) received the Ph.D. degree in computer systems from the University of Technology Sydney (UTS), Ultimo, NSW, Australia, in 2016.

He is currently an Assistant Professor with the Department of Computer Science, Abdul Wali Khan University Mardan, Mardan, Pakistan. He has been actively involved in ML, big data analytics, smart cities infrastructure and vehicular ad hoc networks. He has authored or coauthored the IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE TRANSACTIONS ON CLOUD COMPUTING, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, IEEE INTERNET OF THINGS JOURNAL, IEEE JOURNAL OF SELECTED AREAS OF COMMUNICATIONS and ACM COMPUTING SURVEYS are few to mention. His research interests include energy-efficient and secured communication in wireless sensor networks and Internet of Things.

Dr. Ahmad Jan had been the recipient of various prestigious scholarships during his Ph.D. studies. He was the recipient of International Research Scholarship, UTS and Commonwealth Scientific Industrial Research Organization scholarships. He has been awarded the best Researcher awarded for the year 2014 with the University of Technology Sydney Australia. He has been a Guest Editor of numerous special issues in various prestigious journals such as the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATION, *Springer Neural Networks and Applications*, and *Elsevier Future Generation Computer Systems*, etc.

Fazlullah Khan (Senior Member IEEE) received the Ph.D. degree in computer science from AWKUM, in 2019.

He is currently an Assistant Professor with the Computer Science Department, Abdul Wali Khan University Mardan, Mardan, Pakistan. He has been involved in latest developments in the field of Internet of Vehicles security and privacy issues, software-defined networks, fog computing and big data analytics. He has authored his research work in top-notch journals and conferences. His research has been published in the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE INTERNET OF THINGS, IEEE ACCESS, *Elsevier Computer Networks*, *Elsevier Future Generations Computer Systems*, *Elsevier Journal of Network and Computer Applications*, *Elsevier Computers and Electrical Engineering*, *Springer Mobile Networks and Applications*. His research interests include intelligent and robust protocol designs, security and privacy of wireless communication systems, Internet of Things, ML, and AI.

Dr. Khan had been the recipient of various prestigious scholarships during his Ph.D. studies and has been awarded the best Researcher awarded for the year 2017. He has served more than ten conferences in leadership capacities including General Chair, General Co-Chair, Program Co-Chair, Track Chair, Session Chair, and Technical Program Committee member, including the IEEE International Conference on Trust, Security and Privacy in Computing and Communications 2017, 2018, EuroCom, Global Conference on Consumer Electronics 2019, International Conference on Information Technology: New Generations 2018, Future5V 2017, CCODE-2017, IoT-BC2 2016. He has been an active reviewer for high-cited and highly ranked international journals, including IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, *Elsevier Computer Networks*, *Springer Mobile Networks and Applications* and *Wiley Concurrency and Computation: Practice and Experience.*

Rahim Khan (Member, IEEE) received the Ph.D. degrees in computer system engineering from the Ghulam Ishaq Khan Institute of Engineering Sciences and Technology, Swabi, Pakistan, in 2016.

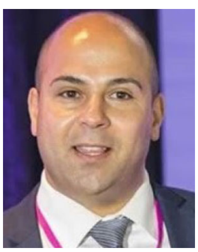
He is currently an Assistant Professor with the Computer Science Department, Abdul Wali Khan University Mardan, Mardan . His research interests include the wireless sensor networks deployment and routing protocols, outliers detection, congestion control, decision support system, vehicular ad-hoc networks, and similarity measures.

Spyridon Mastorakis (Member, IEEE) received the M.S. degree in computer science from the University of California, Los Angeles (UCLA), Los Angeles, CA, USA, in 2017, and a five-year diploma (equivalent to M.Eng.) in electrical and computer engineering from the National Technical University of Athens, Athens, Greece, in 2014, and the Ph.D. degree in computer science from UCLA in 2019.

He is currently an Assistant Professor in computer science with the University of Nebraska Omaha, Omaha, Nebraska. His research interests include network systems and protocols, internet architectures, IoT and edge computing, and security.

Varun G. Menon (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from Sathyabama University, India, in 2017.

He is currently an Associate Professor in computer science engineering with SCMS Group of Educational Institutions, Ernakulam, India. He has authored more than 45 research papers in peer reviewed and highly indexed International Journals and Conferences. His research interests include information science, scientometrics, digital library management, informatics of scientific databases, educational psychology, cyber psychology, hijacked and predatory journals, ad-hoc networks, wireless communication, opportunistic routing, wireless sensor networks, Internet of Things, fog computing and networking, underwater acoustic sensor networks, evaluation methods in education, online education tools, life skills training, training and development.



Mamoun Alazab (Senior Member, IEEE) received the Ph.D. degree in computer science from the School of Science, Information Technology and Engineering, Federation University of Australia, Ballarat, VIC, Australia, in 2012.

He is currently an Associate Professor with the College of Engineering, IT and Environment, Charles Darwin University, Casuarina, NT. He is a cyber security Researcher and Practitioner with industry and academic experience. He has more than 150 research papers in many international journals and conferences, such as the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS, IEEE TRANSACTIONS ON BIG DATA, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, *Computers and Security*, and *Future Generation Computing Systems*. His research interests include multidisciplinary that focuses on cyber security and digital forensics of computer systems with a focus on cybercrime detection and prevention.

Dr. Alazab delivered many invited and keynote speeches, 24 events in 2019 alone. He convened and chaired more than 50 conferences and workshops. He works closely with government and industry on many projects, including Northern Territory (NT) Department of Information and Corporate Services, IBM, Trend Micro, the Australian Federal Police, the Australian Communications and Media Authority, Westpac, United Nations Office on Drugs and Crime, and the Attorney General's Department. He is the Founding Chair of the IEEE NT Subsection.

Paul Watters (Senior Member, IEEE) received the Ph.D. degree in cyber security from Macquarie University, Sydney, NSW, Australia, in 2000.

He is currently an Adjunct Professor of Cybersecurity with La Trobe University, and Honorary Professor with Macquarie University. He is a Chartered IT Professional.

Dr. Watters is a fellow of the British Computer Society and a Member of the Australian Psychological Society. He is an Academic Dean at Australasian Academies Polytechnic, an ASX-listed education provider. He is also Australia's leading trusted cybersecurity advisor, thought leader, and founder of Cyberstronomy Pty Ltd.