PACMAN: Privacy-Preserving Authentication Scheme for Managing Cybertwin-based 6G Networking

Seyed Ahmad Soleymani, Shidrokh Goudarzi, Mohammad Hossein Anisi, Zeinab Movahedi, Anish Jindal, Nazri Kama

Abstract—Security and privacy of data-in-transit are critical issues in Industry 4.0 which are further amplified by the use of faster communication technologies such as 6G. Along with security issues, computation and communication costs, as well as data confidentiality, must be also accommodated. In this work, we design a cybertwin-based cloud-centric network architecture to improve the flexibility and scalability of 6G industrial networks. Cybertwin not only enables the deployment of advanced security solutions but also provides an always-on connection. However, the security of data-in-transit over wireless communication between users/things and cybertwin remains a concern. Hence, a privacy-preserving authentication scheme based on digital signature and authenticated key exchange protocol is designed to address the security concerns of data exchanged. Additionally, we conduct a security analysis that proves that the scheme resists several attacks in the industry 4.0 environment. Moreover, the evaluation performed confirmed the superiority of the proposed work comparing to the existing works.

Index Terms—Cybertwin, 6G, Industry 4.0, Authentication, Privacy.

1 Introduction

INdustry 4.0 is one of the benefits of the development of Wireless Sensor Networking (WSN) technologies in the industry. Through deploying and using WSNs in industries, optimizing the production line becomes possible with energy efficiency, fault prediction, better quality management, product planning, and resource prediction. Today, the development of smart devices and applications as well as advance in the network technology involved in various fields lead to the development of the digital industry, assisting industrial production with information and communication technologies. Industry 4.0, through Artificial Intelligence (AI) and next-generation communication and technology, can gain intelligent connections of end-users, data, processes, and things for making more relevant networked connections [1]. However, the vast array of sensor nodes/smart devices embedded in industry 4.0 applications has resulted in an explosive growth in the degree of interconnectivity and amount of data being processed.

The evolution of 6G networks can effectively mitigate some of these problems. Integration of 6G wireless network and industry 4.0 enables devices to communicate to a new level within intelligent environments, through connected smart sensors over the Internet. The 6G wireless network will extend the scale of industry 4.0 coverage by offering the fastest communication and connection density of massive bandwidth [2]. As mentioned in [3], the industry 4.0 revolution will be completely realized with 6G. It provides cost-effective and efficient Internet-based diagnostics, maintenance, operation, and direct machine connections by overcoming the boundaries and bridging the gap between the physical factory and the cyber computational environment. However, interfacing 6G-Industry 4.0 poses some challenges for security and privacy of data, trusted communication, computational complexity and cost in the aspects of data storage and data processing.

Besides, with the fast development of IoT and its applications, the ever-increasing Internet traffic and services bring unprecedented challenges, such as scalability, security, mobility, privacy and availability, which cannot be addressed by the current network architectures [4]. In the existing IP-based Internet architecture, demands of different devices and service dramatically increasing since IP address used for both identity and locator of the device attached to the network. This happen leads to the scalability problem. Moreover, network resource allocation and coordination among network service providers in order to ensure high Quality of Service (QoS) is difficult such that it leads to availability issue. In terms of network trustworthiness and security, the current IP-based Internet architecture relies on the safety of the end-to-end connections as well as user trustworthy. All such challenging issues in the present network architecture are vital and strictly impede the fast-growing services developments.

To meet the ever-increasing demands, handling the big data generated by IoT devices, and network resource sharing, cloud computing is an appealing strategy [5]. However, it could not be relied upon where a minor delay in data processing may lead to unfavorable outcomes and risky effects. Furthermore, its performance and scalability are still restricted owing to ignoring the network edge processing ability. Besides, the issue of mobility support is not usually considered for accommodating the increasing demands of services and tools. Edge computing integrated into industry 4.0 is one of the better solutions that can locally conduct many tasks rather than getting them processed either in the remote server/cloud or end devices. Edge computing introduces an extension of the cloud computing paradigm with the advantages of better quality of service, scalability, agility, decentralization, and efficiency. However, the

- *S. A. Soleymani is with the Institute for Communication Systems (ICS), University of Surrey, Guildford UK and Iran University of Science and Technology, Iran.E-mail: s.soleymani@surrey.ac.uk*
- *Sh. Goudarzi is with Centre of Artificial Intelligence, National University of Malaysia (UKM), Selangor 43600, Malaysia. E-mail: shidrokh@ukm.edu.my.*
- *M. H. Anisi and A. Jindal are with School of Computer Science and Electronic Engineering, University of Essex, Colchester CO4 3SQ, UK. E-mail: m.anisi@essex.ac.uk;a.jindal@essex.ac.uk.*
- *Z. Movahedi is with the Iran University of Science and Technology, Iran. Email: zmovahedi@iust.ac.ir;*
- *N. Kama is with the Universiti Teknologi Malaysia (UTM), Malaysia. Email: mdnazri@utm.my*

challenges on availability and mobility are not solved in cloud networking.

Given the existing challenges in presenting scalability, mobility, security, and availability for industry 4.0 network architecture designs, we employ the cybertwin-based cloud-centric network architecture. Cybertwin provides three functions such that the communication assistant function is the most fundamental function [6]. By using this function, it obtains the needed service from the network and then deliver the service to the users/things. This network architecture can address the mobility, scalability, and availability of industry 4.0 networks [7]. Cybertwin also deploys the advanced security solutions. Hence, it meets security since each data sending to the humans and or things should traverse the cybertwin. It also can fulfill user's privacy by hiding the the users' identity from the application service providers. Although, cybertwin satisfies security and privacy, however, due to the open-nature of wireless communication employed between cybertwin and humans/things in this network architecture, security and privacy of data transmission over the public channel still remains open concerns in this environment.

Motivated by the security shortcomings and challenges, we design a secure scheme that ensure data will be exchanged among involved entities in a secure way. To this end, we design a privacy-preserving authentication scheme for secure communication in heterogeneous systems. The scheme ensures that only authorized users are able to access data collected from the sensor nodes mounted in the industry 4.0 environment.

The main contributions of this study are as follows:

- We proposed a cloud-centric network based on cybertwin to provide scalability, mobility, and availability for 6G-Industry 4.0 network by accommodation the evolution from end-to-end connection to cloud-to-end connection. For the proposed network architecture, we developed an offloading strategy based on priority and computation time.
- We developed an authentication protocol with privacy-preserving based on digital signature and authenticated key exchange in order to generate and share the session key for dealing with illegitimate entities and ensure the integrity of data.
- We used the broadly accepted random oracle model in order to formally prove the security of our scheme. We also test the safety of the proposed scheme by using the Automated Validation of Internet Security Protocols and Applications (AVISPA).
- We simulated our scheme using the iFogSim simulator. The network throughput, end-to-end delay, and average authentication delay are used as network performance parameters. The detailed of obtained results indicate that our scheme is practical with acceptable communication efficiency.

The rest of paper is as follows: Sections 2 presents the related works. In Section 3, the relevant preliminaries are presented. In Section 4 our scheme is presented. In Section 5, the corresponding formal proof is given. In Section 6, the security analysis and performance evaluation are presented. Section 7 represents a practical perspective. The paper is concluded in Section 8.

2 Related Work

The main area of this study is the existing works on solving the authentication and privacy concerns on insecure communication in the industry 4.0 networks. In the following, we review state-of-the-art works in this area.

In [8], a temporal-credential-based scheme based on Elliptic Curve Cryptography (ECC) is developed for providing the intractability feature. This scheme is facing some issues related to function and security. For addressing the security issues in [8], a three-factor authentication scheme is designed in [9]. This scheme ensures all the security features for WSN in IoT network. For considering the fault tolerance in the biometric information extracted from user, error-correction codes, and fuzzy commitment scheme is adopted.

In [10], an ECC-based user authentication scheme is designed by for future applications of IoT. This scheme however needs higher costs of computation and communication in comparison with other non-ECC-based schemes. A secure light three-factor user authentication protocol for hierarchical IoT networks is presented in [11]. Password, smart card, and personal biometric information are three factors used in this scheme. In order to make a secure communication, they used cryptographic hash function and symmetric encryption/decryption method.

A user authentication scheme based on chaotic-map is designed in [12] applicable to the e-healthcare systems. The chaotic map-based operations have a lightweight nature in comparison with other public key-based cryptosystems such as, ECC and Rivest–Shamir–Adleman (RSA). This scheme also employs fuzzy extractor to verify user biometric. This scheme meets user anonymity. In [13], a remote user authentication scheme based on key establishment protocol is proposed. This protocol utilized for smart home environment. In this study, the focus is on the security of data transmitted between users and smart devices. To this purpose, a session key for secure communication between the user and smart device will be generated with the help of a gateway node.

As explained in [14], in the cybertwin-based edge computing architecture, the edge servers are more vulnerable to different attacks than cloud servers. Accordingly, they used the combination of blockchain and cybertwin to guarantee that the computing tasks of the edge nodes are completed accurately and appropriately returned to the end-user. However, they didn't consider security of communication between end-user and edge nodes and it remains still a security issue. In [6], a network architecture based on cybertwin is proposed. Authors described that user's privacy can be protected by cybertwin. In this network architecture, the end-user will be obtained services via the cybertwin and user's authentication will be verified by cybertwin. All user's behaviours will be logged by cybertwin. However, in this network, the lower layer is based on the IP layer and hence, security and privacy on communication between lower and upper layers still remain the main concern.

Considering the network architectures, the lack of scalable and flexible architecture, as well as always-on connection, is the main challenge in data-based industry 4.0 environments. Besides, the presence of active and passive adversaries in the network threatens the security and privacy of data exchanged between entities. Based on available knowledge, there is a lack of an efficient scheme that considers the security of data-in-transit for this network architecture. Given the big data generated in the large-scale network, computation and communication cost of security scheme also remains the most important challenges in industry 4.0.

3 Preliminaries

Here, the main entities participated in the proposed scheme are defined. Besides, we define threat models and security requirements and goals that we aim to achieve.

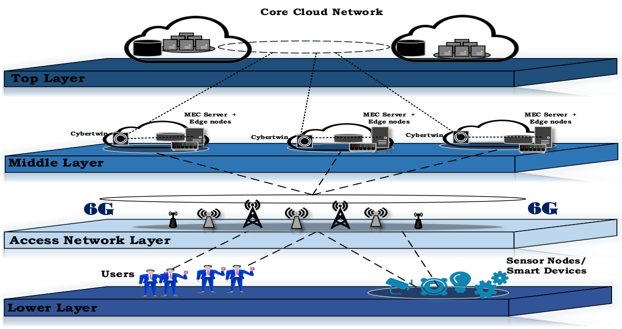


Figure 1: The cybertwin based cloud-centric network architecture for 6G-Industry 4.0.

3.1 System Model

In this study, we developed a cybertwin based cloud-centric network architecture for 6G-Industry 4.0 in where the core cloud network is located in top layer and Mobile Edge Computing (MEC) servers are deployed on the edge of the network in the middle layer (see Figure 1). The cybertwin as an intelligent service agent of smart devices and users/operators is located in the edge cloud [14]. It is assumed that each user is able to access multiple MEC servers and each MEC server has a queue of assigned tasks and can service only one user at the same time and handle sensitive tasks. In the lower layer, all data collected by things such as sensor nodes/smart devices will be transferred to its cybertwin hosting.

In this network architecture, the intensive tasks can perform locally on device and or offloaded the tasks to the MEC servers or core cloud servers. When the required data is available on the local device, there is no need to establish a connection with cybertwin. Otherwise, a user needs to establish a connection to its cybertwin hosting in order to access data and or services. The cybertwin gets services/data from MEC servers and core cloud and then offloads it to the best MEC server. Finally, it establishes a connection between user and MEC server. Therefore, an efficient strategy for offloading is required. Given the entities involved in the proposed network architecture, this strategy can be local offloading, MEC offloading, cloud offloading, and gateway offloading.

3.1.1 *Offloading Strategy*

In this work, our focus is more on accessing the data by users quickly and it is more important for real-time applications. To this purpose, the computation time (T^{com}_{task}), transmission delay (D^{tra}_{task}), and queuing delay (D^{que}_{task}) are taken into account as main factors for offloading.

$$\mathrm{offloading}(\mathrm{T^{c}_{task}}, \mathrm{D^{t}_{task}}, \mathrm{D^{q}_{task}})$$

In the local offloading, the computation time for performing a task is calculated by the following equation [15]

$$T^{c,loc}_{task} = \frac{\Gamma_{loc}}{F_{loc}} \tag{1}$$

where Γ_{loc} refers the number of CPU cycles needed to compute the task and F_{loc} is the local computing power of the local device. In this situation, it is assumed that transmission delay $D^{t}_{task} = 0$, and queuing delay $D^{q}_{task} = 0$. For the local processing, the total delay is $TD^{loc}_{task} = T^{c,loc}_{task}$.

In the MEC server offloading, a cybertwin selects the best MEC server in order to access the requested data. In this strategy, the computation time for performing a task is calculated by

$$T^{c,mec}_{task} = \frac{\Gamma_{mec}}{F_{mec}},\ D^{t,mec}_{task} = \frac{\chi_{ch}}{R_{ch}},\ D^{q,mec}_{task} = T^{mec}_{q}$$
$$where\ \ R_{ch} = \sum_{c_n=1}^{C} B_{ch} log_2(1+\mathrm{SNR_{ch}}) \tag{2}$$

in which χ_{ch} is the number of input data, Γ_{mec} is the number of CPU cycles needed to compute the task, F_{mec} refers to the local computing power of the MEC server, T^{mec}_{q} refers to the time that a task should be waiting in a queue to execute and complete the prior and high priority tasks since prioritized FIFO scheduling [16] is used in this work, R_{ch} indicates the total uplink transmission rate, B_{ch} is the bandwidth of sub-channel ch that is allocated for the task, $\mathrm{SNR_{ch}} = \frac{P_t}{N}$ refers to signal-to-noise ratio that is ratio of transmission power P_t to noise power N. In the MEC server, the total delay of offloading is $TD^{mec}_{task} = T^{c,mec}_{task} + D^{t,mec}_{task} + D^{q,mec}_{task}$.

Because of the limitation of MEC servers, they are unable to store all data in their storage server. Therefore, it is possible the requested data be unavailable in a MEC server. In this situation, the cybertwin can request to offload the task to the center cloud server through wireless network. The computation time for performing a task on cloud server is calculated by

$$T^{c,cld}_{task} = \frac{\Gamma_{cld}}{F_{cld}},\ D^{t,cld}_{task} = \frac{\chi_{ch}}{R_{ch}},\ D^{q,cld}_{task} = T^{cld}_{q} \tag{3}$$

where Γ_{cld} is the number of CPU cycles needed to compute the task on cloud server, F_{cld} refers to the local computing power of the cloud server, and T^{cld}_{que} refers to the time that a task should be waiting in the queue of the cloud for executing. The total delay of offloading in the cloud is $TD^{cld}_{task} = T^{c,cld}_{task} + D^{t,cld}_{task} + D^{q,cld}_{task}$.

3.1.2 *Problem Formulation*

As mentioned above, a task can perform locally and or can offload to a MEC server, cloud server, and or gateway for execution. We can give the total consumption as follows:

$$\Omega_{task} = \omega \times TD^{loc}_{task} + (1-\omega) \times TD^{off}_{task} \tag{4}$$

where $\omega = 1$ refers to the local execution, $\omega = 0$ means offloading the task to a destination and TD^{off}_{task} is the total computation task on the destination is calculated as follows:

$$TD^{off}_{task} = \alpha \times TD^{mec}_{task} + (1-\alpha) \times TD^{cld}_{task} \tag{5}$$

where $\alpha = 1$ indicates the task is performed on the MEC server while $\alpha = 0$ represents the task is executed on the cloud server.

In this study, the total time of execution task, transmission delay, and waiting time in the queue is taken into account as the optimization objective. The aim is to minimize this time. The optimization problem can be expressed as follows:

$$\begin{aligned} \mathrm{P1}:\ \min\sum_{i=1}^{N}\Omega_{task_i} &= \min\sum_{i=1}^{N}\omega \times TD^{loc}_{task_i} + \\ \min\sum_{i=1}^{N}(1-\omega) \times TD^{off}_{task_i} &= \min\sum_{i=1}^{N}\omega \times TD^{loc}_{task_i} + \\ \min\sum_{i=1}^{N}(1-\omega) \times \Big(\alpha \times TD^{mec}_{task_i} &+ (1-\alpha) \times TD^{cld}_{task_i}\Big) \end{aligned} \tag{6}$$

S.t.:

$$
\begin{aligned}
&\mathrm{C}_1 : \omega \times T^{c,loc}_{task_i} + (1-\omega) \times \left(\alpha T^{c,mec}_{task_i} + (1-\alpha) T^{c,cld}_{task_i}\right) \leq T^{c}_{max}\\
&\mathrm{C}_2 : \omega \times D^{t,loc}_{task_i} + (1-\omega) \times \left(\alpha D^{t,mec}_{task_i} + (1-\alpha) D^{t,cld}_{task_i}\right) \leq D^{t}_{max}\\
&\mathrm{C}_3 : \omega \times D^{q,loc}_{task_i} + (1-\omega) \times \left(\alpha D^{q,mec}_{task_i} + (1-\alpha) D^{q,cld}_{task_i}\right) \leq D^{q}_{max}\\
&\mathrm{C}_4 : \omega \in \{0,1\}\,, \quad \alpha \in \{0,1\}
\end{aligned}
\tag{7}
$$

where C_1, C_2, and C_3 respectively represent the maximum computation delay, transmission delay, and queue delay that cannot exceed T^{c}_{max}, D^{t}_{max}, D^{q}_{max}. And, C_4 reflects the computing task offloading decision, which determines whether the tasks are offloaded by MEC servers/cloud.

This network architecture supports users with mobility. When a user moves to the new location, it needs to establishes connection with its cybertwin through new access point. In this network, connection between users and cybertwin and in addition between gateway and cybertwin is under 6G communication standard where it provides high data rate communication system.

3.2 Security Requirements

In industry 4.0, because of the open-access technology used for communication between cybertwin (CT), gateway (GW) and user (U), attackers can obtain and tamper the data by eavesdropping on the communication networks.

To tackle this concern, an efficient privacy-preserving authentication scheme can be helpful. This security scheme should be able to fulfill the key security requirements. In this study, the most critical requirements are summarized below:

- **Data/Message Integrity:** The authorized entities should be able to verify the integrity of the signed data/message.
- **Privacy-preserving:** A third party should be unable to extract the real identity and private information from the user's pseudo-identity and the real identity of authorized users remain anonymous.
- **Data Confidentiality:** An adversary should be unable to extract any information from the communicated data.

3.3 Threat Model

In this study, the Dolev-Yao (DY) threat model [17] is used to analysis and prove security of the proposed scheme. An adversary $\mathbf{\Lambda}$ is able to overhear and manipulate the messages exchanged among two entities over an insecure channel. Besides, $\mathbf{\Lambda}$ can compromise the mobile device by using sophisticated analysis attacks and extract the secret data of the user.

3.4 Fuzzy Extractor

The fuzzy extractor is a useful mechanism that uses biometric information for user authentication. In this method, to deal with physical attacks, the noisy data extracted from the biometric data of the user will be used to generate the cryptographic keys [18]. A $\{M, m_e, l, \tau, \epsilon\}$-fuzzy extractor is made up by two functions *Gen* and *Rep* as probabilistic generation and deterministic reproduction, respectively. *Gen* outputs (R_U, P_U) on input biometric data $BIO_U \in M$ where $R_U \in \{0,1\}^l$ is a secret string and P_U is a auxiliary string such that for any distribution W on M of min-entropy m_e the statistical distance $SD\left((R_U, P_U), (U_l, P_U)\right) < \epsilon$. Here, U_l is the uniform distribution string with length l. And, *Rep* outputs and recovers the secret string R_U given the $BIO^{'}_U$ and P_U such that $Dis\left(BIO_U, BIO^{'}_U\right) < \tau$. Here, $BIO^{'}_U$ is biometric information collected from user U such that distance between $BIO^{'}_U$ and BIO_U is low with high probability $Pr\left[Dis\left(BIO_U, BIO^{'}_U\right) < \tau\right] \geq 1 - \varepsilon_{fn}$, where ε_{fn} is "false negative" probability. In contrast, the distance between biometric data BIO_{U_1} and BIO_{U_2} collected from U_1 and U_2 is high with high probability $Pr\left[Dis\left(BIO_{U_1}, BIO_{U_2}\right) < \tau^{'}\right] \geq 1 - \varepsilon_{fp}$, such that $\tau^{'} > \tau$ and ε_{fp} means "false positive."

4 Our Scheme: A privacy-preserving authentication scheme

The data collected by sensor nodes and/or smart devices and stored in the MEC storage servers should be transferred securely to the users. To this end, we employed the symmetric encryption algorithm since it is quite fast and efficient to secure communication between user and cybertwin. However, the secret key distribution is one of the main concerns in symmetric algorithms. In this work, we designed a digital signature to share confidential the session key generated by cybertwin. We proved that the entities utilized in the proposed framework are able to communicate securely. Here, we explain our scheme in details.

4.1 Phase I - Initialization Phase

In this phase, Trusted Authority (TA) generates the system parameters and then release it to all legal entities in the network. Let two primes p, q; group G of order q; and the distinct generator $P \in G$. It selects an integer $s \in Z^{*}_{q}$ as the master private key with at least 160 bits at random. TA calculates the appropriate public key $P_{pub} = s.P$ by using the master private key. It also selects a secure one-way hash function $h : \{0,1\}^{*} \rightarrow Z^{*}_{q}$ and sets $SysPara = \{p, q, E_q(a,b), G, P, P_{pub}, h\}$ as parameters of the system in order to publish to the core clouds, cybertwin, MEC servers, users and gateway/smart hubs wherein $E_p\left(a,b\right) : y^2 = x^3 + ax + b \ \ mod \ \ p$ is a non-singular elliptic curve with $\left(4a^3 + 27b^2\right) mod \ \ q \neq 0$.

4.2 Phase II - Registration Phase

Here, the registration of cybertwin and user is accomplished by TA.

Cybertwin: Let $\mathcal{C}_{CT} = \{CT_1, CT_2, \cdots, CT_k\}$ as a set of cybertwins contributed to the network. Each CT_i has a real identity ID_{CT_i}, private key $SK_{CT_i} \in Z^{*}_{q}$, public key $PK_{CT_i} = SK_{CT_i}.P$ and a master secret key X_{CT_i}.

User: Let $\mathcal{U}_U = \{U_1, U_2, \cdots, U_n\}$ be authorized users in the network. TA has a database that contains personal details of users in the $\mathcal{U}_U$. Each user in this list i.e. U_i has a private key $SK_{U_i} \in Z^{*}_{q}$, public key $PK_{U_i} = SK_{U_i}.P$ is known by TA. For each user, TA selects ID_{U_i} and PWD_{U_i} as real identity and password, respectively and finally sends $Y_i = \{ID_{U_i}, PWD_{U_i}, s\}$ to the U_i in a secure manner. To this end, TA signs $SGN(Y_i)$ and sends the encrypted message $Z_i = Enc_{PK_{U_i}}\{Y_i, SGN_{SK_{TA}}(Y_i)\}$ to the user. Upon receiving Z_i, it will be decrypted by U_i in order to obtain $\{ID_{U_i}, PWD_{U_i}, s\}$. Besides, PK_{TA} will be used to verify the signature. By using fuzzy extractor and input biometric data BIO_U, each user U extracts R_U and P_U as its biometric information stored in the mobile device. Then, U randomly selects a number r_U, and calculates $HPW_U = h(PWD_U \parallel r_U)$. Finally, user submits the registration request (ID_U, HPW_U, R_U) to its cybetwin host through a secure way. Once receiving a request for registration from the user U, its cybertwin checks whether ID_U is in the database. If exist, the user needs to choose a new identity. Otherwise, cybertwin calculates $B_1 = h(ID_U \parallel HPW_U \parallel R_U)$, $B_2 = h(ID_U \parallel X_{CT})$ where X_{CT} is master secret key selected by cybertwin, and $B_3 = h(HPW_U \parallel R_U) \oplus B_2$. Finally, the cybertwin sends the data (B_1, B_3, X) to U via a secure way. Upon obtaining the parameters, U stores $(P_U, r_U, B_1, B_3, X, Gen(.), Rep(.))$ into the mobile device.

4.3 Phase III - Authentication Phase

In the designed network architecture, the communication between end-users/things and cybertwin (U-CT) is still based on mobile IP. Because of the open nature of U-CT wireless communication, we focus on the security of this communication and explain the authentication in the following.

U-CT Communication: In this work, the U-CT communication is via a symmetric encryption method since it is quite fast and efficient. To establish a secure session communication between U and CT, it is essential to create a session/secret key SEK_{U-CT}. Since the cybertwin is a fully-trusted entity, it is responsible to generate the session key and share with user.

In order to establish this communication, a user has to send a login request to its cybertwin host. Along with this request, the user sends the gateway identity ID_{GW} that needs it's data. Once the cybertwin received this request, it checks user authentication first and then generates a session key SEK_{U-CT} and share with the authorized user. Upon receiving this key, user can start communication with its cybertwin host and other cybertwins as well as MEC servers using a symmetric encryption algorithm such as Advanced Encryption Standard (AES) via a secure manner. This is mainly because the generated session key not only will be sent to the user but also will be shared with all cybertwin hosts, MEC servers, and core cloud servers.

To this purpose and in order user authentication, the user U imprints BIO'_U as its biometric information by using a fuzzy extractor and identity ID_U and password PWD_U as inputs. It calculates $B'_1 = h(ID_U \parallel h(PWD_U \parallel r_U) \parallel R_U)$ where $R_U = Rep(BIO'_U, P_U)$. Then, it checks $B'_1 \overset{?}{=} B_1$. If it does not hold, the mobile device rejects the login request. This is because, at least one factor of biometrics R_U, identity ID_U, and password PWD_U is not valid. Otherwise, if it holds, U randomly selects a number $x_u \in Z^*_q$, and calculates $B_2 = B_3 \oplus h\left(h\left(PWD_U \parallel r_U\right) \parallel R_U\right)$, $D_1 = x_u.P$, $D_2 = x_u.PK_{CT}$, $PID_U = ID_U \oplus h(D_2)$, and $D_3 = h\left(B_2 \parallel D_2\right)$. Finally, the login request $M_1 = \{D_1, D_3, T_1\}$ will be signed by user and submit to its cybertwin host where T_1 is the current timestamp. In order to sign the M_1, user by its mobile device computes the corresponding signature by Equation 8. Then, user sends $\{PID_U, M_1, \sigma_u\}$ to its cybertwin host.

$$\sigma_u = SK_U + s.h\left(PID_U \parallel M_1\right) \tag{8}$$

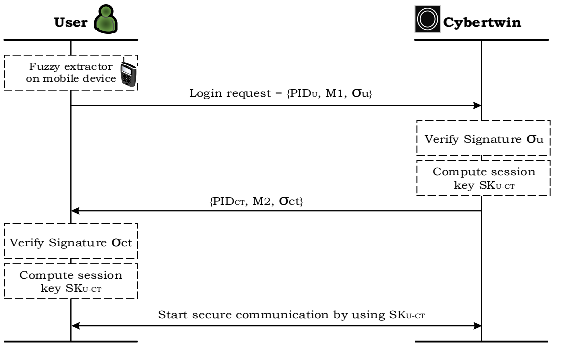

User
Cybertwin
Fuzzy extractor on mobile device
Login request = {PIDU, M1, σu}
Verify Signature σu
Compute session key SKU-CT
{PIDCT, M2, σct}
Verify Signature σct
Compute session key SKU-CT
Start secure communication by using SKU-CT

Figure 2: Process of authentication and session key generation between user and Cybertwin

Upon receiving the login request, cybertwin needs to verify the signature. This verification ensures that the user is not attempting to disseminate false messages and or impersonate other authorized and legitimate users. It first checks whether timestamp T_1 is fresh. If not, it rejects the request. Otherwise, it verifies whether

$$\sigma_u.P = PK_U + P_{pub}.h\left(PID_U \parallel M_1\right) \tag{9}$$

holds or not. If so, cybertwin checks whether $ID'_U = PID_U \oplus h(D'_2)$ is in the database where $D'_2 = SK_{CT}.D_1$. If yes, cybertwin calculates $B'_2 = h(ID'_U \parallel X_{CT})$, $D'_3 = h(B'_2 \parallel D'_2)$, and checks $D'_3 \overset{?}{=} D_3$. The request is terminated by the cybertwin if $D'_3 \neq D_3$. Otherwise, the cybertwin calculates $D_4 = x_c.P$, $SEK_{U-CT} = h(D_1 \parallel D_4 \parallel x_c.D_1)$, $D_5 = h(ID'_U \parallel D_1 \parallel D_4 \parallel B'_2)$, and then submits the message $M_2 = \{D_4, D_5, T_2\}$ to U where T_2 is the current timestamp. Before submission, cybertwin signs the message M_2. To this end, cybertwin compute the signature by using Equation 10. Then, cybertwin sends $\{ID_{CT}, M_2, \sigma_{ct}\}$ to user.

$$\sigma_{ct} = SK_{CT} + s.h\left(ID_{CT} \parallel M_2\right) \tag{10}$$

When getting the message M_2, user has to verify the signature of the message. It firstly checks whether timestamp T_2 is fresh. If not, it rejects the request. Otherwise, it verifies whether

$$\sigma_{ct}.P = PK_{CT} + P_{pub}.h\left(ID_{CT} \parallel M_2\right) \tag{11}$$

hold or not. If it is established, user calculates $D'_5 = h(ID_U \parallel D_1 \parallel D_4 \parallel B_2)$, and checks $D'_5 \overset{?}{=} D_5$. The session is terminated if it does not hold. Otherwise, the cybertwin is authenticated by U. Then, the mobile device calculates $SEK'_{U-CT} = h(D_1 \parallel D_4 \parallel x_u.D_4)$ and start secure communication with its cybertwin till the session key is valid. If the user moves to a new position, it is required the user connects to its cybertwin host through a new access point. During the movement, as long as the session key is valid, all communication is through symmetric encryption. Once the session key is expired, it needs to perform the above procedure for generating a new session key. Figure 2 shows the process of authentication between end-user and its cybertwin host.

5 Formal Security Analysis and Verification

Here, with the random oracle model [19], we first prove that our scheme is secure. Next, we test the safety of our scheme against the passive/active adversaries by using AVISPA.

Definition 1: *The Discrete Logarithm Problem (DLP) is as follows. Consider two random number $P, Q \in G$ where $Q = x.P$ and $x \in Z^*_q$. Given the DLP, computing x from Q is hard.*

Theorem 1: *scheme is secure under random oracle for industry 4.0 environment network.*

Proof: Consider a security model is established by $\mathcal{CH}$ and $\mathbf{\Lambda}$ as challenger and adversary, respectively. $\mathbf{\Lambda}$ can forge $\{PID_i, M_i, \sigma_i\}$. Let the game between $\mathcal{CH}$ and $\mathbf{\Lambda}$ can solve DLP by running $\mathbf{\Lambda}$ with a non-negligible probability. It is supposed that $\mathcal{CH}$ keeps $List_{H_1}$, and $List_{H_2}$ as hash lists which are initialized to empty.

Setup: $\mathcal{CH}$ randomly chooses s and compute $P_{pub} = s.P$ as public key. Besides, $\mathcal{CH}$ sends $params = \{p, q, P, P_{pub}, H_1, H_2\}$ as systeme parameters to $\mathbf{\Lambda}$.

H_1**-Oracle**: $\mathcal{CH}$ keeps $List_{H_1}$ contains the tuples $\langle M_i, \sigma \rangle$. By performing the H_1 query with message M, created by $\mathbf{\Lambda}$, $\mathcal{CH}$ checks whether the tuple $\langle M, \sigma \rangle$ exists in the $List_{H_1}$. If so, $\mathcal{CH}$ returns $\sigma = H_1(M_i)$ to $\mathbf{\Lambda}$; otherwise, $\mathcal{CH}$ randomly chooses $\sigma \in Z_q^*$ and adds $\langle M_i, \sigma \rangle$ into the $List_{H_1}$. Finally, $\mathcal{CH}$ sends $\sigma = H_1(M_i)$ to $\mathbf{\Lambda}$.

H_2**-Oracle**: $\mathcal{CH}$ keeps a list $(List_{H_2})$ with the form of $\langle PID_i, M_i, \sigma \rangle$. By performing a H_2 query by $\mathbf{\Lambda}$ with the message $\langle PID_i, M_i, \sigma \rangle$, $\mathcal{CH}$ checks whether the tuple $\langle PID_i, M, \sigma \rangle$ is in the $List_{H_2}$. If exist, $\mathcal{CH}$ sends $\sigma = H_2(PID_i, M_i)$ to $\mathbf{\Lambda}$. If not exist, $\mathcal{CH}$ randomly selects $\sigma \in Z_q^*$ and adds $\{PID_i, M_i, \sigma\}$ into the $List_{H_2}$. Finally, $\mathcal{CH}$ sends $\sigma = H_2(PID_i, M_i)$ to $\mathbf{\Lambda}$.

Sign-Oracle: Upon receiving a query created by $\mathbf{\Lambda}$ with the message M_i, $\mathcal{CH}$ generates two random numbers α_i,$\sigma_i \in Z_q^*$ and chooses two random point PID_i and PK_i. Then, $\mathcal{CH}$ adds $\langle PID_i, M_i, \alpha_i \rangle$ into the $List_{H_2}$. Next, $\mathcal{CH}$ sends $\langle PID_i, M_i, \tau_i \rangle$ to $\mathbf{\Lambda}$. It is easy to verify the equation $\sigma_i.P = PK_i + P_{pub}.h(PID_i \parallel M_i)$ is established. Therefore, the generated signatures by $\mathcal{CH}$ from signatures generated by authorized users are indistinguishable. Lastly, $\mathbf{\Lambda}$ gives a message $\langle PID_i, M_i, \sigma_i \rangle$ and $\mathcal{CH}$ checks whether $\sigma_i.P = PK_i + P_{pub}.h(PID_i \parallel M_i)$ is established. If not, the process will be aborted by $\mathcal{CH}$.

$\mathbf{\Lambda}$ generates a valid message $\left\langle PID_i, M_i, \sigma_i^{'} \right\rangle$ by using Forking Lemma [19]. In the valid messages $\langle PID_i, M_i, \sigma_i \rangle$ and $\left\langle PID_i, M_i, \sigma_i^{'} \right\rangle$, the signatures $\sigma_i = SK_i + s.h(PID_i \parallel M_i)$ and $\sigma_i^{'} = SK_i + s.h^{'}(PID_i \parallel M_i)$ where $h \neq h^{'}$ are produced by $\mathcal{CH}$ within polynomial running time. Given σ_i and $\sigma_i^{'}$, $\mathcal{CH}$ obtains $x = \left(\sigma_i - \sigma_i^{'}/h - h^{'}\right) mod\ q$ as the answer of the DLP.

Since solving the DLP is contradict to the hardness of DLP, hence, our scheme is secure against the alternatively chosen message attack in the random oracle model. As a result, our scheme provides message authentication for the designed network architecture.

Theorem 2: *(Message Integrity) signature of the message guarantees the message integrity.*

Proof: As explained in Theorem 1, our scheme is secure against a chosen message attack in the random oracle model. Therefore, an attacker is unable to forge valid signatures.

Theorem 3: *(Privacy-Preserving) an adversary is unable to extract the real identity of user from its pseudonym.*

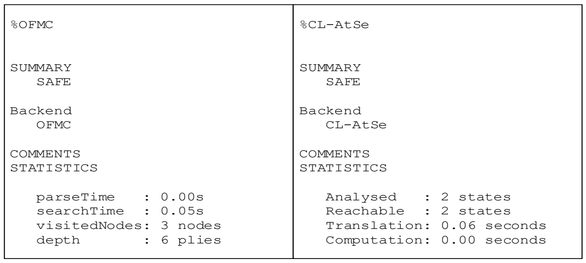
Proof: U_i transmits message $\{PID_U, M_i, \sigma_i\}$ to its cybertwin host, where $PID_U = ID_U \oplus h(x_u.PK_{CT})$. The real identity ID_U is perfectly concealed since PID_U is an unknown identity with a random number x_u. Based on the DLP, it is hard to compute x_u through PID_U and PK_{CT}. Hence, the adversary is unable to obtain ID_U. As a result, our scheme fulfils privacy-preserving.

Theorem 4: *(Data Confidentiality) all data are confidential against an adversary.*

Proof: All data-in-transit for a session between user U and its cybertwin CT are encrypted using the established session key SEK_{U-CT}. This provides end-to-end encryption whereby an attacker is listening to the traffics will only be able to capture the encrypted data. As long as a well-established and secure symmetric encryption scheme (i. e. AES) is used, it is infeasible for an adversary to learn any information from the encrypted data.

5.1 Security Verification

AVISPA, as a popular tool, is used to examine the security protocol versus active or passive adversaries. The security protocol within the formal manner can be verified by using AVISPA. We have modelled our scheme utilizing the AVISPA via High-Level Security Protocol Language (HLPSL) and the user's role specifications, gateway and cybertwin. Then, we simulated the presented outline utilizing the Security Protocol ANimator (SPAN) and the simulation results are summarized in Figures 3 under two extensively-utilized back-ends integrated into AVISPA namely Constraint Logic-based Attack Searcher (CL-AtSe) and On-the-Fly Model-Checker (OFMC).



```
%OFMC                               %CL-AtSe


SUMMARY                             SUMMARY
   SAFE                                SAFE

Backend                             Backend
   OFMC                                CL-AtSe

COMMENTS                            COMMENTS
STATISTICS                          STATISTICS

   parseTime   : 0.00s                 Analysed   : 2 states
   searchTime  : 0.05s                 Reachable  : 2 states
   visitedNodes: 3 nodes               Translation: 0.06 seconds
   depth       : 6 plies               Computation: 0.00 seconds
```

Figure 3: The results of OFMC and CL-AtSe back-ends.

Table 1: Experimental Specifications.

Operations	Symbol	Operation time
Scalar-point multiplication	T_{sm}	0.013 ms
One-way hash function	T_h	0.035 ms
Message authentication code	T_{mac}	0.074 ms
ECC point multiplication	T_{ecc}	0.430 ms
Encryption operation	T_{enc}	0.043 ms
Decryption operation	T_{dec}	0.059 ms
Bitwise XOR operation	T_{xor}	0.009 ms

Table 2: Performance Comparisons.

Ref.	Computation Cost	Commu. Cost
[20]	$19T_h + 8T_{xor} + 6T_{sm}$	340 Bytes
[21]	$30T_h + 16T_{xor}$	482 Bytes
[22]	$31T_h + 20T_{xor} + 4T_{sm}$	232 Bytes
[23]	$14T_h + 8T_{xor}$	340 Bytes
Our Scheme	$14T_h + 3T_{xor} + 7T_{sm}$	128 Bytes

Table 3: Experiment Parameters.

Parameter	Value
Channel bandwidth	4 MHZ
Number of channels	10
Size of task	1 - 4 MB
Range of operands for task	500–2000 Megacycle
CPU cycle	0.1 - 1 GHZ
MEC server clock frequency	10 GHZ
Cloud server clock frequency	100 GHZ

6 Performance Analysis

Here, we assess the performance of our scheme by making a comparison with [20], [21], [22], and [23] by considering the computation cost and communication cost.

Computation Cost: We measure the operation time of cryptographic operations by executing the benchmark on Linux host using Intel Core i7-980X processor laptop with CPU speed 3.3 GHz as testbed. We also measure the execution time of operation on To this end, we use the JPBC library Pbc-05.14, and the JCE library. Table 1 represents the experiment specifications, including the computational specifications.

Communication Cost: For the convenience, we supposed the length of gateway identity ID_{GW}, cybertwin ID_{CT}, output of hash function $h(.)$, random number $x \in Z_q^*$ are 160 bits, whereas the length of user identity ID_U, timestamps, and size of each element $P \in G$ are 80 bits, 32 bits, and 320 bits, respectively [24], [25]. The block size of the cryptography of AES, as the symmetric encryption algorithm applied in our scheme, is equal to 128 bits [26]. Table 2 represents the performance of our scheme and other comparable schemes in terms of computation and communication cost.

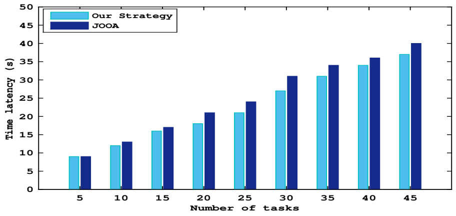


Figure 4: Time latency

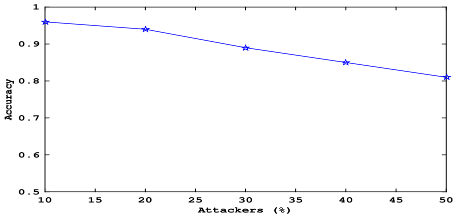


Figure 5: Overall accuracy

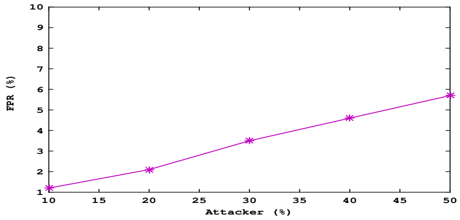


Figure 6: FPR

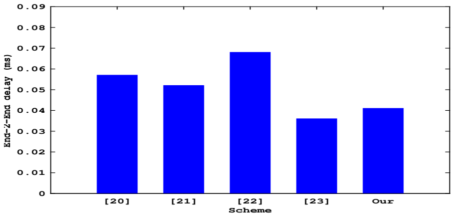


Figure 7: End-to-End delay

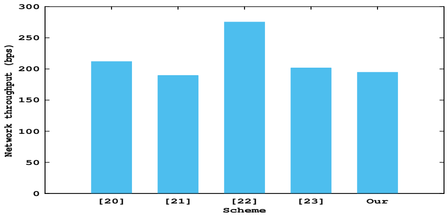


Figure 8: Network throughput

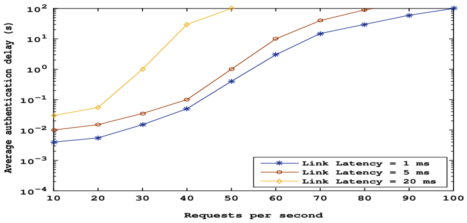


Figure 9: Authentication delay

7 Practical Perspective

We simulate the integrated architecture using iFogSim [27]. It provides a full-stack environment for modelling and simulation in the edge and fog computing environment [28]. iFogSim is used to model the interactions across all layers of the IoT architecture. In this work, a real-life scenario with 1 gateway, 5 MEC servers, and 2 cloud servers is simulated. The simulation takes average of 30 minutes on a Linux host using Intel Core i7-980X, 3.33GHz.

7.1 Offloading Evaluation

Here, we evaluate our strategy for task offloading by making a comparison with strategy that used in [29] named ”JOOA” by considering time latency under different number of tasks. To this end, inspired by the work in [29], we set some parameters aiming to reflect a scenario as much realistic as possible (see Table 3). We measure the time latency versus different numbers of intensive tasks for our strategy and JOOA.

Figure 4 clearly shows time latency is increasing as the number of tasks increases. As we can see in this figure, the time latency for our strategy and JOOA are almost the same but when the number of tasks is increasing, the difference between these values increases and it is lower for our strategy. Because of the importance of real-time tasks in industry 4.0 network, this comparison proves that our strategy is more efficient and effective.

7.2 Authentication Scheme Evaluation

In the Industry 4.0 network environment, especially in real-time applications, accessing the required data/services securely and efficiently with the least possible delay has a vital role in the system performance. In this work, we first evaluate the accuracy and False Positive Ratio (FPR) of our scheme under the DY threat model. Then, we use three indexes to see the practicality of communication: End-to-End Delay (E2ED), Network THRoughput (NTHR), and average authentication delay.

Accuracy: Here, the overall accuracy is considered as a percentage of the total number of correct outcomes and results. It is measured by the standard formula as follows [25]:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \tag{12}$$

where TP, TN, FP and FN refer to the number of true positive, true negative, false positive and false negative, respectively. As shown in Figure 5, the average accuracy of our scheme is 89% under the different percentages of attackers who participated in the network.

FPR: In this work, FPR is used to prove the validity of our scheme to detect forged messages. It is measured by the standard formula as follows [25]:

$$FPR = \frac{FP}{FP + TN} \tag{13}$$

where FP refers to the number of forged messages incorrectly detected as valid messages and TN is the number of forged messages correctly detected by our scheme. As shown in Figure 6, the average of FPR is about 4% with the different percentages of attackers that inject forged messages.

End-to-End Delay: It is a network performance parameter that is defined as the time taken for a packet to be transmitted between the sender and the receiver across a network. It is formulated as

$$E2ED = \frac{\sum_{i=1}^{N} (T_{r_i} - T_{s_i})}{N} \tag{14}$$

where T_{r_i} and T_{s_i} respectively refer to receiving and sending time of packet i and N is the total number of packets.

Figure 7 shows that E2ED values for our scheme, [20], [21], [22], and [23], during the authentication process, are respectively $0.041ms$, $0.057ms$, $0.052ms$, and $0.036ms$. As we can see, E2ED for [23] is less than our scheme, [20], [21] and [22]. This because the size of messages for [23] is less than our scheme and other comparable schemes.

Network Throughput: It is also an important network performance parameter which is defined as the number of bits transmitted per unit time, and it is formulated as

$$NTHR = \frac{N_r \times |Pkt|}{T_d} \tag{15}$$

where N_r is the total number of received packet, $|Pkt|$ refers to the size of each packet and T_d is total time.

Figure 8 shows that the value of throughput for our scheme is less than [20], [22], and [23] because our scheme uses less-sized messages during the authentication phases. The throughput value for [21] is less than our scheme, however, our scheme provides better security and more functionality features.

Average Authentication Delay: We use this parameter to show the impact of 6G, 5G and 4G as wireless communication technologies on authentication process. In the 6G-Industry 4.0, the typical value of link latency is $1ms$, whereas it is $5ms$ in 5G-Industry 4.0 network. With this assumption, we evaluate the average authentication delay under different rates of request (per second) and different time for authentication request service. We also explore the average authentication delay with link latency= $20ms$ which is a typical value in 4G systems. As we can see in Figure 9, the average delay experienced by an authentication request varies with the rate of requests for link latency= $5ms$ and $20ms$.

8 Conclusion

In this work, we have designed a cybertwin based cloud-centric network architecture for 6G-Industry 4.0 network to provide scalability, mobility, security and availability. Because of the vital role of tasks and data offloading, an efficient offloading strategy was proposed to support the network architecture. Besides, given the open-nature of wireless communication between end-users/things and cybertwin, we have developed a authentication scheme based on digital signature and authenticated key exchange with privacy-preserving. This scheme ensures the integrity of data-in-transit. The formal proof analysis has proved that the proposed scheme is secure and robust against DY threat model. Furthermore, the comparison with the related work proves the effectiveness of the work in terms of security and performance.

References

[1] D. Wang, D. Chen, B. Song, N. Guizani, X. Yu, and X. Du, "From IoT to 5G I-IoT: The next generation IoT-based intelligent algorithms and 5G technologies," *IEEE Communications Magazine*, vol. 56, no. 10, pp. 114–120, 2018.

[2] B. Ji, Y. Wang, K. Song, C. Li, H. Wen, V. G. Menon, and S. Mumtaz, "A survey of computational intelligence for 6G: Key technologies, applications and trends," *IEEE Transactions on Industrial Informatics*, 2021.

[3] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G networks: Use cases and technologies," *IEEE Communications Magazine*, vol. 58, no. 3, pp. 55–61, 2020.

[4] X. Ren, G. S. Aujla, A. Jindal, R. S. Batth, and P. Zhang, "Adaptive recovery mechanism for sdn controllers in edge-cloud supported fintech applications," *IEEE Internet of Things Journal*, 2021.

[5] S. Garg, A. Singh, K. Kaur, G. S. Aujla, S. Batra, N. Kumar, and M. S. Obaidat, "Edge computing-based security framework for big data analytics in vanets," *IEEE Network*, vol. 33, no. 2, pp. 72–81, 2019.

[6] Q. Yu, J. Ren, H. Zhou, and W. Zhang, "A cybertwin based network architecture for 6G," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*. IEEE, 2020, pp. 1–5.

[7] Q. Yu, J. Ren, Y. Fu, Y. Li, and W. Zhang, "Cybertwin: An origin of next generation network architecture," *IEEE Wireless Communications*, vol. 26, no. 6, pp. 111–117, 2019.

[8] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 76, pp. 37–48, 2016.

[9] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments," *Journal of Network and Computer Applications*, vol. 103, pp. 194–204, 2018.

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

[11] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 269–282, 2017.

[12] 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 of Things Journal*, vol. 5, no. 4, pp. 2884–2895, 2017.

[13] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 2, pp. 391–406, 2017.

[14] Z. Chen, W. Hou, H. Wen, W. Lei, S. Wu, and H. Lin, "Multi-dimensional resource management system based on blockchain and cybertwin," in *The 2nd International Conference on Computing and Data Science*, 2021, pp. 1–5.

[15] W. Han, W. Hou, H. Wen, W. Lei, X. Xu, and H. Lin, "Reinforcement learning-based multidimensional resource management in edge cloud regions," in *The 2nd International Conference on Computing and Data Science*, 2021, pp. 1–5.

[16] V. Sdralia, C. Smythe, P. Tzerefos, and S. Cvetkovic, "Performance characterisation of the mcns docsis 1.0 catv protocol with prioritised first come first served scheduling," *IEEE Transactions on broadcasting*, vol. 45, no. 2, pp. 196–205, 1999.

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

[18] D. Choi, S.-H. Seo, Y.-S. Oh, and Y. Kang, "Two-factor fuzzy commitment for unmanned IoT devices security," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 335–348, 2018.

[19] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of cryptology*, vol. 13, no. 3, pp. 361–396, 2000.

[20] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ECC-based provable secure authentication protocol with privacy preserving for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3599–3609, 2017.

[21] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. Rodrigues, "Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4900–4913, 2018.

[22] J. Srinivas, A. K. Das, M. Wazid, and N. Kumar, "Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial internet of things," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 6, pp. 1133–1146, 2018.

[23] G. S. Poh, P. Gope, and J. Ning, "Privhome: Privacy-preserving authenticated communication in smart home environment," *IEEE Transactions on Dependable and Secure Computing*, 2019.

[24] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, and K.-K. R. Choo, "A robust and energy efficient authentication protocol for industrial internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1606–1615, 2017.

[25] S. A. Soleymani, S. Goudarzi, M. H. Anisi, M. Zareei, A. H. Abdullah, and N. Kama, "A security and privacy scheme based on node and message authentication and trust in fog-enabled vanet," *Vehicular Communications*, vol. 29, p. 100335, 2021.

[26] 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.

[27] H. Gupta, A. Vahid Dastjerdi, S. K. Ghosh, and R. Buyya, "iFogSim: A toolkit for modeling and simulation of resource management techniques in the internet of things, edge and fog computing environments," *Software: Practice and Experience*, vol. 47, no. 9, pp. 1275–1296, 2017.

[28] M. Chernyshev, Z. Baig, O. Bello, and S. Zeadally, "Internet of things (IoT): Research, simulators, and testbeds," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1637–1647, 2017.

[29] T. Yang, H. Feng, S. Gao, Z. Jiang, M. Qin, N. Cheng, and L. Bai, "Two-stage offloading optimization for energy–latency tradeoff with mobile edge computing in maritime internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 5954–5963, 2019.

Seyed Ahmad Soleymani is a research fellow at the Institute for Communication Systems (ICS), University of Surrey, Guildford UK. He received his Ph.D. degree in computer science from faculty of engineering, Universiti Teknologi Malaysia (UTM). He received his M.S degree from the Department of Computer Engineering, Islamic Azad University, Iran and B.S. degree from the Department of Computer Engineering, Sadjad University, Iran. His research interests are in the area of Vehicular Ad Hoc Network (VANET), Internet of Things (IoT), Industrial Internet of Things (IIoT), and Intelligent Algorithms (IAs).

Shidrokh Goudarzi received her Ph.D. degree in communication system and wireless network from Malaysia-Japan International Institute of Technology (MJIIT), Universiti Teknologi Malaysia (UTM). In 2014, She received three-year full scholarship to study Ph.D. at UTM. Then, She joined the Department of Advanced Informatics School at UTM as a Postdoctoral Fellow from 2018 to 2019. Currently, she is a senior lecturer at Universiti Kebangsaan Malaysia (UKM). She also serves as reviewer for Canadian Journal of Electrical and Computer Engineering, KSII Transactions on Internet and Information Systems Journal,Journal of Engineering and Technological Sciences, Mathematical Problems in Engineering and IEEE Access. Her research interests are in wireless networks, artificial intelligence, machine learning, next generation networks, Internet of Things (Iot) and Mobile/distributed/Cloud Computing.

Mohammad Hossein Anisi (M'14-SM'19) is currently an Associate Professor with the School of Computer Science and Electronic Engineering, University of Essex, U.K. and Head of Internet of Everything (IoE) Laboratory. Prior to that, he worked as a Senior Research Associate with the University of East Anglia, U.K. and Senior Lecturer with the University of Malaya, Malaysia, where he received the "Excellent Service Award" for his achievements. He has published more than 100 articles in high-quality journals and several conference papers. His research interests include IoT, WSN, Green and Energy-efficient Communication and Vehicular Networks. He has received several international and national funding awards for his fundamental and practical research as PI and Co-I. He is an Associate Editor of several journals and has been lead organizer of special sessions and workshops at IEEE conferences such as ICC, CAMAD, PIMRC, and VTC.

Zeinab Movahedi received the M.Sc. and Ph.D. degrees in computer networks and telecommunications from the University of Pierre and Marie Curie (Paris 6), Laboratoire d'Informatique de Paris 6 (LIP6), Paris, France, in 2007 and 2011, respectively. She is currently an Assistant Professor at IUST. Her research interests include green communication, mobile cloud computing, software-defined networks, autonomic networking, wireless networks, network security, performance evaluation, and quality-of-service support.

Anish Jindal received his Ph.D. degree in Computer Science and Engineering Department from Thapar University, Patiala, India in 2018. He is the recipient of Outstanding Ph.D. Dissertation Award, 2019 from IEEE Technical Committee on Scalable Computing (TCSC) and IEEE Communication Society's Outstanding Young Researcher Award for the Europe, Middle East, and Africa (EMEA) Region (2019). He is working as a Lecturer in School of Computer Science and Electronic Engineering, University of Essex, UK. Prior to this, he was working as a Senior Research Associate in the School of Computing and Communications, Lancaster University, UK. He has published in top cited journals such as IEEE TII, IEEE TIE, IEEE TVT, IEEE TSC, IEEE JSAC, IEEE Communication Magazine, IEEE Network, Future Generation Computer Systems, and Computer Networks. He has served as TPC member, publicity chair and session chair of various reputed conferences and workshops including IEEE Globecom, IEEE WoWMoM, and IEEE ICC.

Nazri Kama is a professor at Universiti Teknologi Malaysia (UTM) specializing in system software engineering. In 2011, he received a doctorate in software engineering from the University of Western Australia in Australia. His research interest covers from system software engineering, requirements engineering, software design, electric vehicle charging technology, and electric vehicle networks.