IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 24 July 2022, accepted 1 August 2022, date of publication 16 August 2022, date of current version 9 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3198642

RESEARCH ARTICLE

Designing an Enhanced User Authenticated Key Management Scheme for 6G-Based Industrial Applications

IJAZ DARMAN[1], MUSARIA KARIM MAHMOOD[2], SHEHZAD ASHRAF CHAUDHRY[3,4], SAJJAD AHMAD KHAN[5], AND HUHNKUK LIM[5], (Member, IEEE)

[1]Department of Electrical and Electronics Engineering, Istanbul Gelisim University (IGU), 34310 Istanbul, Turkey
[2]Department of Energy Systems Engineering, Yildirm Beyazit University, 06760 Ankara, Turkey
[3]Department of Computer Engineering, Faculty of Engineering and Architecture, Nisantasi University, 34398 Istanbul, Turkey
[4]Department of Computer Science and Information Technology, College of Engineering, Abu Dhabi University, Abu Dhabi, United Arab Emirates
[5]Department of Computer Engineering, Hoseo University, Asan-si 31499, South Korea

Corresponding author: Huhnkuk Lim (slow63347@gmail.com; rooky13@hanmail.net)

This work was supported by the Korean Government (Ministry of Science and ICT) through the National Research Foundation of Korea (NRF) under Grant 2021R1A2C1010481.

ABSTRACT In the Sixth Generation (6G) mobile system, the importance of security increases even more in the communication system. One of the potential technologies of 6G is the Network in a Box (NIB). The 6G-enabled NIB is a multi-generational, easily and quickly installable technology used for communication. It is based on both hardware and software. The main features of a 6G-enabled NIB include low latency and a high level of flexibility. In addition, it provides connectivity services to the applications used in unusual situations such as battlefields or natural disasters in the industry. However, most of the applications used in the 6G-enabled NIB are not appropriately secured. There are chances of several active and passive attacks due to the insecure channel. Therefore, a novel remote user authentication and key management scheme is presented in this paper. This scheme is the modified and improved version of UAKMS-NIB and is renamed as the improved User Authentication and Management Scheme to secure the 6G-enabled NIB (iUAKMS-NIB) that can be used in industrial applications. Hence, the proposed scheme provides the best security solution against the possible attacks on the 6G communication system. The analytical results show that the proposed scheme performs better compared to the existing schemes.

INDEX TERMS Sixth generation (6G), Internet of Thing (IoT), network in a box (NIB), security.

I. INTRODUCTION

The 21st century is the era of modern technologies and communication, with the organization of Security Group (SG) frameworks. On the other hand, the Sixth Generation (6G) architecture is under development and expected to launch in 2030. In 6G mobile networks, the trend toward cloud and edge native infrastructures is projected to continue and require a complete 6G network security architecture design [1]. A new term, ''Network In a Box'' (NIB), is a new concept refers to a unique networking assembly that may supply essential services to its neighbors and mobile objects. NIB is able to give customers in crisis with phone, SMS, and Internet access [1], [2]. The primary characteristics of NIB are the high resilience, robustness, and dependability of the underlying network configuration. Therefore, NIB must be a lightweight, highly portable, mobility-aware, privacy-protecting tool. Due to the presence of latency, non-cognitive behavior, and three-dimensional connectivity [3], legacy communication technologies such as 2G, 3G, 4G, and 5G may not be efficient enough to exploit massive connection-aware network service provisioning. Hence, it provides dynamic solutions for 6G mobile network as well gained enormous popularity nowadays. This multi-generational, 6G-enabled NIB can be carried in a bag [4]. Hence, the 6G-enabled NIB is a collection of hardware and

The associate editor coordinating the review of this manuscript and approving it for publication was Barbara Masini.

software components for mobile communication that are simple to set up and maintain. The fundamental concept behind the use of NIB is to provide communication services in catastrophe scenarios such as earthquakes, fires in industries, battlefields, floods, emergency situations, and many more. In addition, the concept of NIB relies on merging all sorts of software and hardware modules that are required by mobile networks inside a single bag that contains a small number of physical devices [5]. Due to its high degree of customization and increased dependability, this highly adaptable 6G-enabled NIB can provide communication services for a wide variety of applications. It is crucial to emphasize that emergency and tactical networks are designed to be adaptable and flexible due to the fact that their deployment is not well known. They are classified as ''Mobile Ad-hoc Networks (MANETs)'' in this category. Furthermore, the NIB is a portable entity by nature. As a result, it may be used in disaster management situations especially for fire control in industries [6].

Recently, specifications for disaster and mobile networking systems have been improved to allow the systems to operate with fewer physical devices while still accomplishing the primary purpose of enhancing serviceability. Many network providers have also adopted this approach in order to build these networks, which may be set up with just a small number of physical devices or even just a single device. As a result, the development of NIB is a new network communication technology that meets the requirements of future-generation mobile networks, such as the use of industrial mobile communication networks. As a general rule, the 6G-enabled NIB may be ''configured to operate alone or in combination with existing legacy network elements or NIBs.'' In addition, it is designed to enable access to all wireless networks in a compact, portable device for corporate, industrial, private, public, military, and security applications [1], [7], [8].

6G-based ''Evolved Packet Core (EPC),'' ''tower with antenna,'' ''user with a mobile device,'' ''IP Multimedia Subsystem (IMS),'' ''content server,'' ''smart industrial devices,'' and ''Trusted Authority (TA)'' are just a few of the components that make up the 6G-enabled NIB and can be used in industrial applications. These parts help people communicate with each other and get to important services, like web-based information, video streaming, or information from smart industrial equipment [5], [7], [9]. For the purpose of monitoring and controlling industrial equipment, intelligent industrial tools such as Programmable Logic Controllers (PLC), Distributed Control Systems (DCS), and SCADA, etc., are being used [10]. The 6G wireless communication technology makes it possible for different parts and devices to exchange the data between them.

A. MOTIVATION

The 6G-enabled NIB can be deployed in critical conditions to provide secure communication and public safety during natural disasters. The internet providers use Mobile Broadband (MBB) services to access the application server via the Internet. In the RAN architecture, mobile operators employ eNB and a collection of SGW, PGW, and MME in order to provide public services [11]. Consequently, the LTE-based public service strategy might be implemented inside the 6G-enabled NIB with the appropriate adjustments to 6G-oriented service protocols.

There are several benefits of using a 6G-enabled NIB compared to previous wireless communication technologies. However, there are some network security concerns regarding the forthcoming 6G-based mobile networks (i.e., NIB). It occurs as a result of the fact that security measures are not completely implemented in modern mobile networks, such as 6G. According to study results, there is a newly discovered capacity for third-person attacks in terahertz 6G networks that could be exploited. It is critical to stress that the 6G-enabled NIB implemented for commercial implementation have different security and privacy concerns, such as exposed to many cyber-attacks. It is possible to conduct various attacks on a 6G-enabled NIB targeting industrial applications known to have critical security implications. These attacks include replaying, third-person, cloning, unauthorized access to data, unauthorized key exchange calculation, and attacks from the stolen devices. As a result, it is needed to develop security rules for a ''6G-enabled NIB used for industrial purposes.''

In order to access the real-time data, a registered user must also authenticate with the smart industrial equipment used to receive the information. Disaster management (earthquakes and tsunamis), for example, is one of the important applications of NIB, where a user has to be able to receive real-time information directly from smart-industrial equipment installed in the 6G-based network. To alleviate these problems, authentication and key establishment with an authorized user and accessible smart industrial equipment must occur through a critical intermediate node known as the content server [12]. The content server is positioned between the two parties. Thus, we should develop a new and comprehensive user authentication protocol system that allows mutual authenticated key configuration between users and intelligent industrial equipment through a content server.

B. PROBLEM STATEMENT

The implementation of NIB and portable networks seem to be very crucial for the future industrial revolution. Logistics, factory-floor robots and warehouse management may demand very dense deployments of mobile-aware, adaptable services. Such use cases must be allowed by the 6G-enabled NIB to facilitate low latency in order to optimize the performance. In the past, disaster management lacked networking plans and failed to provide better communication. Therefore, the 6G-enabled NIB is expected to play an effective role in this regard. Furthermore, the 6G-enabled NIB will enable self-healing and self-organizing networking infrastructures to ensure seamless communication between the victim and rescuer during any natural or artificial disaster. However, most of the applications used in the 6G-enabled NIB will not be appropriately secured. There are chances of several active and

passive attacks due to the insecure channel. An authentication scheme (UAKMS-NIB) is presented in the Wazid *et al.*'s article [13]. However, there is a missing step to exchange the authentication key between the content server and smart devices. The smart device sends the key directly to the user without having any information about the authentication key. Therefore, it is not possible to communicate without exchanging authentication key information.

C. CONTRIBUTIONS

In order to counter the incorrectness mentioned above, we propose an improved scheme based on an elliptic curve, which provides user authentication and better security.

The significant contributions of this paper are as follows:

1) An improved User Authentication and Management Scheme for secure communication in 6G-enabled NIBs (iUAKMS-NIB) is proposed in this paper. The proposed scheme validates the authentication process between a user and the smart-industrial equipment through a verification key.
2) This paper provides different analyses to ensure security and verify authentication between a user and smart-industrial equipment. An experiment is conducted by using a Raspberry-Pi, iPhone Xs Max, and a Dell Ultrabook 8757P. It is demonstrated that the iUAKMS-NIB is resilient against various possible attacks required in a 6G-enabled NIB environment.
3) The testbed studies on different authentication key schemes are carried out by using the widely accepted ''Burrows Abadi and Needham Logic (BAN-Logic)'' [14] in both the server and user environments, and the results are presented in Section VIII.
4) Finally, a comparative analysis of computation and communication costs is presented and discussed. The results show that the improved iUAKMS-NIB scheme validates authentication and exchanges a verified key between a user and smart-industrial equipment through the content server during user authentication.

D. PAPER ORGANIZATION

The remainder of the paper is organized as follows: Section II provides an overview of existing work. Section III explains the System Model, consisting of the Network Model and Threat Models. Section IV explains the Wazid *et al*. scheme and its pitfalls in Section V. The proposed scheme is presented in Section VI. The Performance analysis, such as Computational Cost and Communication Cost, is performed in Section VII. Section VIII contains the results of the experiment performed using BAN Logic, and the conclusion is given in Section IX.

II. RELATED WORK

In recent years, sufficient research has been conducted in order to provide data privacy and protection during network communication and has presented their potential ideas. The authors in [15] provide a privacy-enhanced data aggregation technique that employs Homomorphic encryption and fog computing to aid aggregation servers in executing data collection with a privacy guarantee. By offering a reputation assessment system for data aggregation users and data sensing users, the authors in [16] presented a solution to data aggregation that ensures data privacy during the aggregate process. Data trustworthiness is used in data aggregation in order to strengthen the reputations of sensing and aggregation users while limiting the likelihood of privacy concerns. In [19] and [20], the researchers described a number of truth-finding methods that can be used to get reliable information without putting user privacy at risk. The authors of [19] proposed a privacy-aware data transmission approach that employs deep reinforcement learning technology to dynamically select and optimize the transmission path while avoiding privacy violations during transmission. In addition, the authors in [20] combine the multimedia data aggregation coding with k-anonymous procedures to produce k-anonymity. In [21], the researchers encrypt sensitive data during data aggregation using the partly Homomorphic encryption encryption approach. While the authors in [22] use Contract Theory to provide participator's users with a variety of contracts with varying privacy settings, This is done to strike a compromise between the accuracy of the fusion center as a whole and the privacy of each user's information.

The authors in [23] presented a model for spatial crowd-sourcing that provides security and privacy. The scheme uses attribute based encryption and symmetric key encryption to protect the security of spatial tasks. However, confidentiality and the validity of responses cannot be guaranteed. The authors in [24] offered a privacy-preserving technique with distinctive privacy to protect data and ensure data availability. In [25], the authors implemented several controls to manage data in the production automation systems to ensure the confidentiality and integrity of data, which will slow down an attacker. This strategy, however, requires a great deal of physical equipment and results in network complexity.

On the other hand, the authors in [26] provided various use cases that inspired the creation of the NIB idea. The common aspects of NIB implementations, as well as other ideas, were addressed. Some of the potential study avenues that may be pursued were also mentioned. In [27], the authors presented a variety of approaches for improving the robustness of Long-Term Evolution (LTE) networks that are used for military and public safety operations. It is possible that these approaches will be enabled via the 3GPP LTE standards and that they will also be deployed as software enhancements for existing systems. A management approach developed in [28], which enabled numerous operators (for example, multiple Servicing/Packet Gateways (S/P GWs) in order to operate dynamically through multiple Sm-GWs in a large number of tiny cells. The Software-Defined Networking (SDN) based Smart gateways (Sm-GWs) were responsible for coordinating

the adaptive distribution of uplink transmission bit rates to evolved Node Bass-stations (eNBs) depending on needs.

The authors in [27] presented a variety of approaches for improving the robustness of Long-Term Evolution (LTE) networks that are used for military and public safety operations. It is possible that these approaches will be enabled via the 3GPP LTE standards and that they will also be deployed as software enhancements for existing systems. A management approach developed in [28], which enabled numerous operators (for example, multiple Servicing/Packet Gateways (S/P GWs) in order to operate dynamically through multiple Sm-GWs in a large number of tiny cells. The Software-Defined Networking (SDN) based Smart gateways (Sm-GWs) were responsible for coordinating the adaptive distribution of uplink transmission bit rates to evolved NodeBS (eNB) depending on needs.

In [29], the authors addressed the major technical developments that could drive the 6G mobile network. For example, ''cognitive spectrum sharing techniques for new spectrum bands,'' ''integration of localization and sensing capabilities'' into the definition of a system, ''achievement of extreme performance requirements in terms of latency and reliability,'' new network architecture paradigms that include ''sub-networks'' and ''RAN-Core convergence'', and advanced security and privacy techniques are all being explained.

On the other hand, the authors in [30] identified certain probable requirements and provided an overview of the most recent research on viable ways for developing 6G, which has garnered substantial interest. In addition, the major technological issues related with 6G, as well as possible solutions, were examined at length. The authors in [31] provided an overview of key technologies that will serve as pillars for the evolution of wireless communication beyond 5G, including ''micro-services-oriented core networks,'' ''native IP-based user planes,'' ''network analytics,'' and ''support for low latency-high reliability.'' They focused on ''micro-service-oriented core networks,'' ''native IP-based user planes,'' ''network analytics,'' and ''support for low latency-high reliability.'' It was also examined what problems remain in terms of technical and business requirements, such as building ''softwarization footprints,'' ''security and trust,'' and ''distributed architectures and services'' in the direction of 6G deployments, and how to overcome the problems.

III. SYSTEM MODELS

The proposed scheme i.e., iUAKMS-NIB is explained by using the following two models. The overall network model is given in the Fig. 1.

A. NETWORK MODEL

Fig. 1 depicts the network model of the ''6G-enabled NIB'' that has been implemented for industrial applications. NIB provides the connections and enables the various sorts of entities to communicate with each other. It is used to provide integrated voice and data services via mobile communication networks such as 3G and 4G, and beyond mobile networks. The EPC incorporates critical components such as the Packet Data Network Gateway (P-GW), the Serving Gateway (S-GW), the Mobility Management Entity (MME), and the Home Subscriber Server (HSS). The mobile device serves as a connection point between external networks. It serves as the point of entry for data flow for a mobile device's user. The user's mobile device may be linked to several P-GWs at the same time in order to get access to multiple P-GWs. Furthermore, S-GW is responsible for the routing and forwarding of user data packets. It is also in charge of inter-eNB handovers and the provision of mobility between long-term evolution (LTE) and other kinds of networks (for example, between 2G/3G and P-GW), among other functions. An eNB is a kind of base station that is responsible for controlling the mobile phones in a group of cells. The serving eNB is the base station that connects with a user's mobile device and is referred to as the serving eNB. ''Idle mode user's mobile device tracking,'' ''paging procedure (i.e., re-transmissions),'' ''bearer activation and deactivation process,'' ''S-GW selection for a user's mobile device at the initial attach,'' ''intra-handover with Core Network,'' and ''user's mobile device authentication with HSS'' are just a few of the tasks that the MME is responsible for in the NIB. The MME server also manages ciphering and integrity protection for Non-Access Stratum (NAS) signaling, as well as security key administration. HSS is also a critical component of the NIB system. It is a master user database that is only kept on a single node in the cluster. (i.e., device). Communications service providers may manage consumers in real time and at a reasonable cost as a result of this technology. Information about subscribers (i.e., users) is stored in the HSS database in order to assist with authorisation, as well as specifics about devices, as well as the user's location and other associated service information, among other things. It also establishes a connection between the user's request and the IP Multimedia Subsystem (IMS). In an integrated network of telecommunications carriers, an IMS is a critical component that makes it possible to use IP (Internet Protocol) for various types of packet transmission in wired or wireless communication, including telephony, fax, e-mail, Internet access, web services, and voice over IP (VoIP), and so on. The content server, which serves as a link between the users and the smart industrial equipment, is also an essential node in the network.

A smart industrial device network has been built on this network for the purpose of monitoring and controlling industrial machinery. Each intelligent industrial gadget has a certain goal in mind that it strives to achieve. Users of an industrial facility may sometimes be interested in gaining access to real-time data collected by smart industrial equipment. Users and smart industrial equipment must go through the procedures of authentication and key setup methods in order to be able to share information in a safe manner with one another.

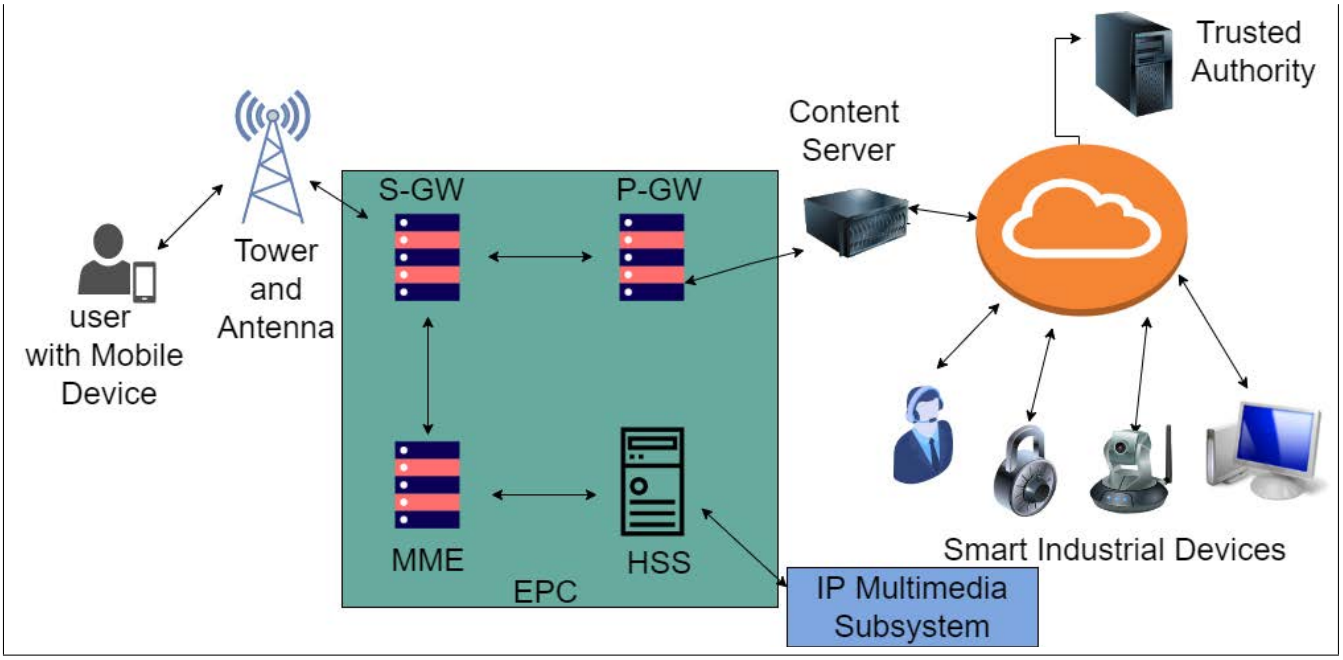

FIGURE 1. The network model for 6G-enabled NIB.

B. THREAT MODEL

During the development of iUAKMS-NIB, we followed to the well-known "Dolev-Yao threat model" [32], which is also known as the DY model. The communicative entities (parties) speak with one another over an open channel as a result. Individuals who interact with the end-point entities (such as users and smart industrial equipment) are not often regarded as trustworthy. The trustworthy authorities of the "6G-enabled NIB deployed for commercial applications" is, on the other hand, regarded to be the completely trusted node. In any event, the TA should not be infiltrated since it is responsible for the registration of network entities (including users, content servers, and smart industrial devices). If the TA is hacked, the security of the whole network would be jeopardized. Aside from that, the content server might be regarded as a semi-trusted entity in the network. Furthermore, it is believed that the memory unit of the user's Mobile Device (MD) is not provided with tamper-resistant capabilities to prevent unauthorized access. By using power analysis techniques, a hacker may hijack a user's mobile device and retrieve all of the sensitive information that has been saved on it from the device's memory [33], [34].

A model known as the "CK-adversary model" [35], which is now de-facto standard in the design of key exchange systems [36], [37], [38], [39], [40], is also taken into consideration in iUAKMS-NIB. According to this model, A may tamper with messages in the same way as he or she can in the DY model, but he or she can also compromise session keys, private keys, and other session states via session hijacking attacks in addition to tampering with messages.

IV. THE UAKMS-NIB SCHEME OF WAZID *ET AL.*

This section explains the Wazid *et al.*'s scheme named as UAKMS-NIB. Different stages used in UAKMS-NIB schemes are discussed in details.

A. REGISTRATION PHASE

This phase is executed by a *TA* and for this *TA* select an elliptic cure $E_p(x_x, x_y) : y^2 = x^3 + x_x + x_y(modp)$ and a base point P over $GF(p)$. The *TA* then selects a oneway hash function $h(\cdot)$.

1) SMART INDUSTRIAL DEVICE REGISTRATION

The *TA* registers SD_z (Smart Industrial Device) through execution of following steps:

RD-1: The *TA* selects it's own secret key d_{TA} and the identity, secret key and public key tuple $\{ID_z, d_z, Q_z = d_z \cdot P\}$ for SD_z along with pseudo identity $RD_z = h(ID_z \| d_{TA})$. The *TA* then using the timestamp RTS_z, computes $TC_z = h(d_z \| ID_z \| RTS_z \| d_{TA}$.

RD-2: The information obtained from RD-1, such that $RD_z, TC_z, Q_z, d_z, h(\cdot), E_p(a, b), P$ is stored in the memory of SD_z. It is noted that Q_z is announced widely to the other entities. In addition, RD_z can be sent to CS_y by *TA* in a secure way.

2) CONTENT SERVER REGISTRATION

The content server CS_y is registered during this phase. This task is executed by *TA* in the following steps.

RCS-1: In order to calculate the pseudo-identity of CS_y as $RD_y = h(ID_y \| d_{TA})$, public key $Q_y = d_y \cdot P$, the *TA* picks a unique identity ID_{CSj} and a random secret key

TABLE 1. The symbols and notation used in iUAKMS-NIB.

Symbol	Explanation
A	An adversary
U_x, D_x	x^{th} user and his/her mobile device, respectively
ID_x, RD_x	x's identity and pseudo identity, respectively
PW'_x, BO_x	x's password and biometric, respectively
TA, ID_{TA}	Trusted authority and its identity, respectively
RD_{TA}	TA's pseudo identity
CS_y,ID_y	y^{th} content server and its identity, respectively
RD_y	Pseudo identity of CS_y
SD_z, ID_z	y^{th} smart industrial device & its identity, respectively
RD_z	Pseudo identity of SD_z
d_x, d_y	160-bit secret keys of U_x and CS_y respectively
d_z, d_{TA}	Secret keys of SD_z and TA, respectively
X	1024-bit long-term random secret of U_x
r_x, r_y	160-bit random secrets of U_x and CS_y, respectively
r_z	160-bit random secret of SD_z
T_s	Various current timestamps
ΔT	Maximum transmission delay
$Gen(\cdot)$	Generation process in fuzzy extractor
$Rep(\cdot)$	Reproduction process in fuzzy extractor
α'_x	Biometric secret key of U_x for BO_i
τ_x	Public reproduction parameter of U_x for BO_x
t	Error tolerance threshold required by fuzzy extractor
$h(\cdot)$	Collision-resistant cryptographic one-way hash function
SK_x, SD_z	Session key between U_x and SD_x
$\|\|$, $\oplus$	Concatenation & bitwise XOR operations, respectively
d_e	Private key of entity E
Q_e	Public key of entity E, where $Q_e = d_e \cdot P$, where P is an elliptic curve point.

d_y for CS_y. Meanwhile, it also generates it own pseudo random identity $RD_{TA} = h(ID_{TA}\|d_{TA})$.

RCS-2: The related content server and user information RD_y, RD_x, TID_x, RD_{TA}, RD_z, Q_y, d_y, $h(\cdot)$, $E_p(a, b)$, P is stored on a database created over a temper resistant memory pf the *TA*. Here, $\{RD_x, TID_x\}$ are registered user (U_x) related parameters. The public key Q_y of the content server is publicly available to all intended entities.

3) USER REGISTRATION

This phase furnishes the user registration.The registration curious user U_x and *TA* mutually communicate over a secure channel through execution of following steps to accomplish this phase:

RU-1: The U_x selects identity-password pair $\{ID_x, PW'_x\}$ in addition to a secret and random long term key $x \epsilon Z_p^*$, and then it computes $RPW'_x = h(PW'_x\|x)$. Now, U_x transmits $\{ID_x, RPW'_x\}$ to *TA*.

RU-2: On receiving $\{ID_x, RPW'_x\}$, the *TA* computes pseudo and temporary identity pair $\{RD_x = h(ID_x\|d_{TA}), TID_x\}$, in addition to a secret and random key $d_x \epsilon Z_p^*$. After then, the *TA* computes $Q_x = d_x \cdot P$, the public key for the U_x and the temporary parameters The *TA* computes temporal credential of U_x as $TC_x = h(ID_x\|RPW'_x\|d_x\|d_{TA}\|RTS_x)$ and $\alpha'_x = h(RPW'_x\|RD_x) \oplus d_x$ (also termed as temporal credentials) for U_x. The *TA* now sends the tuple containing $\{RD_x, TID_x, RD_{TA}, TC_x, \alpha'_x, Q_x, h(\cdot), E_p(a, b), P\}$ to U_x. The *TA* places Q_x over a public space and any intended identity has access to the Q_x.

RU-3: On receiving $\{RD_x, TID_x, RD_{TA}, TC_x, \alpha'_x, Q_x, h(\cdot), E_p(a, b), P\}$, The U_x pins BO_x and the D_x computes $(\alpha'_x, \tau_x) = GenB(BO_x)$, where BO_x, α'_x and τ_x are the U_x's biometrics information, BO_x related secret key and re-production parameter, respectively. Moreover, the "$GenB(\cdot)/RepB(\cdot)$ are generation and re-production functions of the fuzzy-extractor related to the biometrics. Now the U_x further computes $d_x = h(RPW'_x\|RD_x) \oplus \alpha'_{U_x}$, $TC_x = h(TC_x\|x\|\alpha'_x)$, $x^* = x \oplus h(ID_x\|PW'_x\alpha'_x)$, $RD^*_x = RD_x \oplus h(PW'_x\|\alpha'_x)$, $TID^*_x = TID_x \oplus h(ID_x\|PW'_x)$, $RD^*_{TA} = RD_{TA} \oplus h(ID_x\|RPW'_x\|\alpha'_x)$, $TC^*_x = TC_x \oplus h(ID_x\|RPW'_x\|\alpha'_x$, $d^*_x = d_x \oplus h(ID_x\|\alpha'_x)$ and $LV = h(ID_x\|RPW'_x\|TC_x\|d_x\|\alpha'_x)$. The U_x then updates the D_x with the tuple RID^*_x, TID^*_x, RD^*_{TA}, TC^*_x, d^*_x,Q_x, τ_x, LVx^*, $h(\cdot)$, $Gen(\cdot)$, $Rep(\cdot)$, t, $E_p(a, b)$, P

RU-4: The *TA* on successful registration of a user U_x communicates RD_x, TID_x to CS_y and it removes the tuple RD_x, TID_x, RD_y, RD_z, d_x, d_y, d_z, TC_x, TC_z, α'_x, RPW'_x from *TA*'s own memory.

B. USER LOGIN AND AUTHENTICATION PHASE

A registered user U_x initiates this step to get NIB services and for this the U_x performs following login and authentication steps:

ULA-1: The U_x submits the tuple $\{ID_x, PW'_x, BO'_x\}$ consisting of it's identity, password and biometrics. The D_x checks the relation of BO'_x with the user-biometrics imprinted during registration phase and in case if both biometrics match each other the D_x computes $\alpha'_x = RepB(BO'_x, \tau_x)$. Now, the user side computes $x = x \oplus h(ID_x\|PW'_x\alpha'_x)$, $RPW'_x = h(PW'_x\|x)$, $RD_x = RD_x \oplus h(PW'_x\|\alpha'_x)$, $TID_x = TID_x \oplus h(ID_x\|PW'_x)$, $RD_{TA} = RD_{TA} \oplus h(ID_x\|RPW'_x\|\alpha'_x)$, $TC_x = TC_x \oplus h(ID_x\|RPW'_x\|\alpha'_x)$, and $\alpha' d_x = d_x \oplus h(ID_x\|\alpha'_x)$. Now D_x confirms the authenticity of U_x if $LV \stackrel{?}{=} h(ID_x)\|RPW'_x\|TC_x\|d_x\|\alpha'_x)$ holds and furthers the process by generating the timestamp and random number pair $\{T_1, r_x\}$. The user device now computes $M_1 = h(r_x\|T_1) \oplus (RD_{TA}\|RD_x\|d_x \cdot Q_y\|T_1)$, $MM_1 = h(h(r_x\|T_1)\|TC_x\|T_1\|RD_x\|RD_{TA}) \oplus h(h(r_x\|T_1)\|RD_{TA}\|T_1)$, $M_x = h(RD_x)\|RD_{TA})$, $M_2 = M_x \cdot P$, $M_3 = M_x + h(r_x\|T_1) \cdot d_x$ and selects the smart device with RD_z as it's pseudo identity. U_x completes this step by sending $M_{sg1} = \{TID_x, RD_z, M_1, MM_1, M_2, M_3, T_1\}$ to CS_y via open channel.

ULA-2: After successful login and receiving of $M_{sg1} = \{TID_x, RD_z, M_1, MM_1, M_2, M_3, T_1\}$, the CS_y after confirming the timestamp (T_1) freshness extracts RD_x relevant to the received TID_x. The CS_y then computes $h(r_x\|T_1) = M_1 \oplus h(RD_{TA}\|RD_x\|d_y \cdot Q_x\|T_1)$ and $M_x = h(RD_x\|RD_{TA})$. The CS_y confirms the genuineness of the U_x if $M_3 \cdot P \stackrel{?}{=} M_2 +$

$h(r_x\|T_1)\cdot Q_x$. The CS_y after confirming genuineness generates timestamp and random number pair $\{T_2, r_y\}$ and computes $M_4 = h(r_y\|T_2\|RD_y) \oplus h(RD_z\|d_y \cdot Q_z\|T_2)$, $MM_2 = MM_1 \oplus h(h(r_x\|T_1)\|RD_{TA}\|T_1) \oplus h(h(r_y\|T_2\|RD_y)\|T_2\|RD_z)$, $M_y = h(RD_z\|T_2)$, $M_5 = M_z \cdot P$ and $M_6 = M_y + h(r_y\|T_2\|RD_y)\cdot d_y$. The CS_y then generates TID_x^{new}, and computes $M_T = TID_x^{new} \oplus h(h(r_x\|T_1)\|RD_{TA}\|T_2)$, where TID_x^{new} is the new temporary identity for U_x. Now, the CS_y sends $M_{sg2} = \{RD_z, M_4, MM_2, M_5, M_6, M_T, T_1, T_2\}$ to SD_z.

ULA-3: On receiving $M_{sg2} = \{RD_z, M_4, MM_2, M_5, M_6, M_T, T_1, T_2\}$, the SD_z after confirming the timestamp (T_2) freshness, computes $h(r_y\|T_2\|RD_y) = M_4 \oplus h(RD_z\|d_z \cdot Q_y\|T_2)$, $h(h(r_x\|T_1)\|TC_x\|T_1\|RD_x\|RD_{TA}) = MM_2 \oplus h(h(r_x\|T_1)\|RD_{TA}\|T_1) \oplus h(h(r_x\|T_1)\|RD_{TA}\|T_1) \oplus h(h(r_y\|T_2\|RD_y)\|T_2\|RD_z)$, $M_y = h(RD_z\|T_2)$ and checks $M_6 \cdot P \stackrel{?}{=} M_5 + h(r_y\|T_2\|RD_y)\cdot Q_y$. The SD_z further computes $X_s = h(h(r_x\|T_1)\|TC_x\|T_1\|RD_x\|RD_{TA})$, if the previous condition holds. The SD_z furthers the process by generating the timestamp and random number pair $\{T_3, r_z\}$ and computes $M_7 = h(r_z\|T_3) \oplus h(T_1\|T_3\|d_z \cdot Q_x)$, $M_x = h(RD_z\|TC_z) \oplus h(h(r_z\|T_3)\|T_1)$, $M_z = h(h(RD_z\|TC_z)\|T_1\|T_3)$, $M_8 = M_z \cdot P$, and the session key $SK_{SD_z,U_x} = h(X_s\|h(r_z\|T_3)\|T_1\|T_2\|T_3\|M_z)$. The SD_z now generates signatures $M_9 = M_z + h(SK_z, U_x\|M_T\|T_1\|T_3)\cdot d_z$ and sends $M_{sg3} = \{M_7, M_x, M_8, M_9, M_T, T_3, T_2\}$ to U_x.

ULA-4: On receiving $M_{sg3} = \{M_7, M_x, M_8, M_9, M_T, T_3, T_2\}$, the U_x after confirming the timestamp (T_3) freshness, computes $h(r_z\|T_3) = M_7 \oplus h(T_1\|T_3\|Q_z \cdot d_x)$, $h(RD_z\|TC_z) = Mx \oplus h(h(r_z\|T_3)\|T_1)$, $M_z = h(h(RD_z\|TC_z)\|T_1\|T_3)$ and session key $SK_{U_x,SD_z} = h(h(h(r_x\|T_1)\|TC_x\|T_1\|RD_x\|RD_{TA})\|h(r_z\|T_3)\|T_1\|T_2\|T_3\|M_z)$. Now, U_x verifies the genuineness of the SD_z by verifying the equality $M_9 \cdot P \stackrel{?}{=} M_8 + h(SK_{U_x,SD_z}\|M_T\|T_1\|T_3)\cdot Q_z$ and on successful verification, the U_x computes $TID_x^{new} = M_T \oplus h(h(r_x\|T_1)\|RD_{TA}\|T_2)$ and replaces TID_x by TID_x^{new}.

V. PITFALLS OF WAZID *ET AL.*'s SCHEME

In this section, we prove that the Wazid *et al.*'s scheme, given in Fig. 2, can not provide authentication among a user and a smart device. Moreover, it is also shown that their scheme entails identity de-synchronization issues.

A. INCORRECTNESS

The authentication phase of Wazid *et al.*'s scheme is incorrect and it cannot be completed. As a severe consequence, the user and the smart industrial device may not share the key at all. Precisely, a user initiates a request by computing and sending $M_{sg1} = \{TID_x, RD_z, M_1, MM_1, M_2, M_3, T_1\}$ to CS_y and the CS_y further processes the request and after verifying the legitimacy of the the user say U_x, direct message $M_{sg2} = \{RD_z, M_4, MM_2, M_5, M_6, M_T, T_1, T_2\}$ to SD_z. The SD_z processes the message and verifies the legitimacy of CS_y, After then SD_z computes and sends $M_{sg3} = \{M_7, M_x, M_8, M_9, M_T T_3, T_2\}$ to U_x. In this whole process the SD_z does not verify the legitimacy of the user U_x rather SD_z does not know the real or pseudo identity of the user U_x and the message M_{sg2} received from CS_y also does not contain any tangible information regarding the identity of U_x. Therefore, the step to send M_{sg3} from the SD_z to U_x is out of question. Hence, the scheme Wazid *et al.* is incorrect and due to this incorrectness, the said scheme fails to complete a round of authentication process.

B. IDENTITY DE-SYNCHRONIZATION

The provision of anonymity and user privacy in the scheme of Wazid *et al.* is achieved through temporary identity generated by the CS_y during registration phase and this temporary identity is updated during each login and authentication round, described as follows: The user U_x sends temporary identity TID_x as part of message M_{sg1}. The CS_y upon reception of M_{sg1} extracts RD_x corresponding to TID_x and then after processing the message generates new temporary identity TID_x^{new}, hides it in $M_T = TID_x^{new} \oplus h(h(r_x\|T_1)\|RD_{TA}\|T_2)$ and sends it to SD_z along with other parameters included in M_{sg2}. This M_T is sent through M_{sg3} from SD_z to U_x. Finally, the U_x after processing the message updates TID_x by TID_x^{new}. Now, if any of the message M_{sg2} or M_{sg3} is blocked by an attacker controlling the public communication channel as per CK attack model adopted in this paper, the U_x would not be able to update its temporary TID_x, whereas, the CS_y has already updated TID_x by TID_x^{new}, after receiving M_{sg1}. Now, both entities U_x and CS_y are having mismatched identities. Hence, identity de-synchronization has occurred, and for the next login by U_x will fail.

VI. PROPOSED SCHEME

This section explains the details of our proposed and improved scheme iUAKMS-NIB, shown in Fig. 3.

A. REGISTRATION PHASE

This phase uses a fully TA that selects a "non-singular elliptic curve $E_p(a, b)$ and forms "$y2 = x3 + ax + b(modp)$ over a Galois (finite) field $GF(p)$, where p is a large prime," such that the "Elliptic Curve Discrete Logarithm Problem (ECDLP)" becomes intractable, with "a base point P in $E_p(a, b)$, whose order is as big as p.

Furthermore, the *TA* selects a collision-resistant one-way cryptographic hash algorithm $h(\cdot)$ along with a private key d_{TA} of the trusted authority.

1) SMART INDUSTRIAL DEVICE REGISTRATION

The following steps are performed by *TA* for registration of the deployment of a smart industrial device.

PRS-1: First of all, a unique identity ID_z and a random secret key $d_z \epsilon Z_p^*$ for smart device SD_z, is chosen by the TA. For SD_z, *TA* calculates the pseudo identity of SD_z as $RD_z = h(ID_z\|d_{TA})$, the public key of d_z as

FIGURE 2. The existing scheme presented by Wazid *et al.* [13].

$Q_z = d_z \cdot P$ and the temporal credential as $TC_z = h(d_z \| ID_z \| RTS_z \| d_{TA})$, where RTS_z is the registration timestamp of SD_z.

PRS-2: The information obtained from RSD-1, such that $RD_z, TC_z, Q_z, d_z, h(\cdot), E_p(a,b), P$ is stored in the memory of SD_z before the development of SD_z. It is noted that Q_z is announced widely to the other network entities. In addition, RI d_z can be sent to CS_y by *TA* in a secure way.

2) CONTENT SERVER REGISTRATION

The content server CS_y is registered during this phase. This task is executed by TA in the following steps.

PRC-1: The TA chooses a unique identity ID_y and a secret key $d_y = h(ID_y || d_{TA})$ for CS_y to compute the pseudo identity of CS_y as $RD_y = h(ID_y \| d_{TA})$, public key $Q_y = d_y \cdot P$ and its own pseudo-random identity $RD_{TA} = h(ID_{TA} \| d_{TA})$.

PRC-2: The credentials RD_y, RD_x, TID_x, RD_{TA}, RD_z, Q_y, d_y, $h(\cdot)$, $E_p(a,b)$, P are then stored in CS_y is secure/tamper-resistant database by the *TA*.

Note that RD_x and TID_x related to a registered user U_x are generated in the below section during the user registration phase. In addition, Q_y is published publicly to other network entities.

3) USER REGISTRATION

In this phase, the registration of a user U_x is performed by the TA through a secure channel (e.g., in person) using the following steps.

FIGURE 3. **Proposed Scheme (iUAKMS-NIB).**

PRU-1: U_x chooses user unique identity ID_x, password PW'_x and a long-term random secret $x \epsilon Z_p^*$ to calculate the masked password $RPW'_x = h(PW'_x \| x)$. U_x then sends ID_x, RPW'_x to the *TA* through a secure channel.

PRU-2: After receiving the registration information, the *TA* computes the pseudo identity $RD_x = h(ID_x \| d_{TA})$, generates temporary identity $TID_x = E_{d_y(RD_x || r_0)}$ (r_0 being a random number generated by *TA*) and a secret key $d_x = h(ID_x || d_{TA})$ for U_x. The *TA* computes temporal credential of U_x as $TC_x = h(ID_x \| RPW'_x \| d_x \| d_{TA} \| RTS_x)$, $\alpha'_x = h(RPW'_x \| RD_x) \oplus d_x$ and its public key as $Q_x = d_x \cdot P$. The *TA* then sends RD_x, TID_x, RD_{TA}, TC_x, α'_x, Q_x, $h(\cdot)$, $E_p(a, b)$, P to D_x of U_x through a secure channel.

Note that Q_x is published publicly to other network entities.

PRU-3: After receiving the information from *TA*, U_x furnishes biometric data BO_x to the biometric sensor

of his/her mobile device D_x to compute $(\alpha'_x, \tau_x) = Gen(BO_x)$, where α'_x and τ_x are the biometric secret key of l bits and public reproduction parameter, respectively and "$Gen(\cdot)/Rep(\cdot)$ are the fuzzy extractor probabilistic generation and deterministic reproduction functions, respectively [41]". Furthermore, U_x computes $d_x = h(RPW'_x \| RD_x) \oplus \alpha'_{U_x}$, $TC_x = h(TC_x \| x \| \alpha'_x)$, $x^* = x \oplus h(ID_x \| PW'_x \alpha'_x)$, $RD^*_x = RD_x \oplus h(PW'_x \| \alpha'_x)$, $TID^*_x = TID_x \oplus h(ID_x \| PW'_x)$, $RD^*_{TA} = RD_{TA} \oplus h(ID_x \| RPW'_x \| \alpha'_x)$, $TC^*_x = TC_x \oplus h(ID_x \| RPW'_x \| \alpha'_x$, $d^*_x = d_x \oplus h(ID_x \| \alpha'_x)$ and $LV = h(ID_x \| RPW'_x \| TC_x \| d_x \| \alpha'_x)$. Finally, RID^*_x, TID^*_x, RD^*_{TA}, TC^*_x, d^*_x,Q_x, τ_x, LVx^*, $h(\cdot)$, $Gen(\cdot)$, $Rep(\cdot)$, t, $E_p(a, b)$, P are stored in the memory of D_x. Note that α'_x, x, ID_x, RPW'_x, RD_x, TID_x, RD_{TA}, TC_x, TC_x and d_x are deleted from the memory of D_x to protect against stolen verifier, privileged insider attack, unauthorised session key computation, illegal user's password guessing and user impersonation attacks.

PRU-4: The TA sends the credentials RD_x, TID_x to CS_y in a secure way through a pre-shared symmetric secret key K_y, TA. The TA also erases RD_x, TID_x, RD_y, RD_z, d_x, d_y, d_z, TC_x, TC_z, α'_x, RPW'_x from its memory to protect against stolen verifier, privileged insider attack, unauthorized session key computation, illegal user's password guessing and user impersonation attacks.

B. USER LOGIN PHASE

To access the services of the NIB, a legitimate user U_x first needs to login into the system. For such propose, the following steps are required

PLU-1: U_x furnishes his/her identity ID_x and password PW'_x, and also imprints biometrics BO'_x at the sensor of his/her mobile device D_x to calculate biometric secret key $\alpha'_x = Rep(BO'_x, \tau'_x)$ provided that the "Hamming distance between the real biometrics BO_x provided during the user registration phase and current BO'_x is less than or equal to a pre-defined error tolerance threshold, say t".

PLU-2: U_x then computes $\alpha'_x = Rep(BO'_x, \tau'_x)$, $x = x^* \oplus h(ID_x \| PW'_x \| \alpha'_x)$, $RPW'_x = h(PW'_x \| x)$, $RD'_x = RD_x \oplus h(PW'_x \| \alpha'_x)$, $TID'_x = TID_x \oplus h(ID_x \| PW'_x)$, $RD'_{TA} = RD_{TA} \oplus h(ID_x \| RPW'_x \| \alpha'_x)$, $TC'_x = TC *_x \oplus h(ID_x \| RPW'_x \| \alpha'_x)$, $d_x = d *_x \oplus h(ID_x \| \alpha'_x)$ and checks the condition $LV' \stackrel{?}{=} h(ID_x) \| RPW'_x \| TC'_x \| d_x \| \alpha'_x)$. If it holds, U_x is a genuine user; otherwise, the login phase is halted immediately.

PLU-3: D_x generates a current timestamp T_1 and a random secret $r_x \epsilon Z^*_p$ to calculate $M_1 = h(r_x \| T_1) \oplus h(RD_{TA} \| RD_x \| d_x \cdot Q_y \| T_1)$, $MM_1 = h(h(r_x \| T_1) \| TC_x \| T_1 \| RD_x \| RD_{TA}) \oplus h(h(r_x \| T_1) \| RD_{TA} \| T_1)$, $M_x = h(RD_x) \| RD_{TA})$, $M_2 = M_x \cdot P$, $M_3 = M_x + h(r_x \| T_1) \cdot d_x$. U_x then picks an accessed smart device SD_z with its pseudo identity RD_z and sends the login message $M_{sg1} = \{TID_x, RD_z, M_1, MM_1, M_2, M_3, T_1\}$ to CS_y via open channel.

C. USER AUTHENTICATION AND KEY AGREEMENT PHASE

This phase is required for mutual authentication among a registered user U_x, a content server CS_y and an accessed smart industrial device SD_z. After the successful completion of the following steps, both U_x and SD_z establish a session key for their secure communication via CS_y.

PKM-1: After receiving M_{sg1} from U_x, CS_y first verifies the timeliness of T_1 through the condition, $|T_1 - T^*_1| \leq \Delta T$, where the "maximum transmission delay" is represented by ΔT and T^*_1 is reception time of the message M_{sg1}. If it matches, CS_y extracts $(RD_x || r_0) = D_{d_y}(TID_x)$. CS_y further calculates $h(r_x \| T_1) = M_1 \oplus h(RD_{TA} \| RD_x \| d_y \cdot Q_x \| T_1)$, $M_x = h(RD_x \| RD_{TA})$ and checks if $M_3 \cdot P = M_2 + h(r_x \| T_1) \cdot Q_x$. If CS_y finds this condition true, U_x is authenticated by CS_y.

PKM-2: CS_y generates a current timestamp T_2 and a random secret $r_y \epsilon Z^*_p$ to compute $M_4 = h(r_y \| T_2 \| RD_y) \oplus h(RD_z \| d_y \cdot Q_z \| T_2)$, $MM_2 = MM_1 \oplus h(h(r_x \| T_1) \| RD_{TA} \| T_1) \oplus h(h(r_y \| T_2 \| RD_y) \| T_2 \| RD_z)$, $M_y = h(RD_z \| T_2)$, $M_5 = M_y \cdot P$ and the ElGamal type signature $M_6 = M_y + h(r_y \| T_2 \| RD_y) \cdot d_y$. CS_y then sends the message $M_{sg2} = \{RD_z, M_4, MM_2, M_5, M_6, T_1, T_2\}$ to SD_z via open channel.

PKM-3: After receiving M_{sg2} from CS_y, SD_z first verifies the timeliness of T_2 by checking $|T_2 - T^*_2| \leq \Delta T$ where T^*_2 is reception time of the message M_{sg2}. If it is valid, SD_z computes $h(r_y \| T_2 \| RD_y) = M_4 \oplus h(RD_z \| d_z \cdot Q_y \| T_2)$, $h(h(r_x \| T_1) \| TC_x \| T_1 \| RD_x \| RD_{TA}) = MM_2 \oplus h(h(r_x \| T_1) \| RD_{TA} \| T_1) \oplus h(h(r_x \| T_1) \| RD_{TA} \| T_1) \oplus h(h(r_y \| T_2 \| RD_y) \| T_2 \| RD_z)$, $M_y = h(RD_z \| T_2)$ and checks $M_6 \cdot P \stackrel{?}{=} M_5 + h(r_y \| T_2 \| RD_y) \cdot Q_y$. If SD_z finds this condition true, CS_y is authenticated by SD_z, and SD_z sets $X_s = h(h(r_x \| T_1) \| TC_x \| T_1 \| RD_x \| RD_{TA})$.

PKM-4: SD_z generates a current timestamp T_3 and a random secret $r_z \epsilon Z^*_p$ to calculate $M_7 = h(r_z \| T_3) \oplus h(T_1 \| T_3 \| d_z \cdot Q_x)$, $M_w = h(RD_z \| TC_z) \oplus h(h(r_z \| T_3) \| T_1)$, $M_z = h(h(RD_z \| TC_z) \| T_1 \| T_3)$, $M_8 = M_z \cdot P$, session key $SK_{z,x} = h(X_s \| h(r_z \| T_3) \| T_1 \| T_2 \| T_3 \| M_z)$, and generates the ElGamal type signature $M_9 = M_z + h(SK_{z,x} \| T_1 \| T_3) \cdot d_z$. Now, SD_z computes $M_S = h(ID_y || h(r_y \| T_2 \| RD_y || T_3)$ and then sends the message $M_S = h(ID_y || h(r_y \| T_2 \| RD_y || T_3)$ to U_x through the open channel.

PKM-5: After receiving M_{sg3} from SD_z, CS_y first verifies the timeliness of T_3 by checking $|T_3 - T^*_3| \leq \Delta T$ where T^*_3 is reception time of the message M_{sg3}. If it is valid, CS_y further checks $M_S \stackrel{?}{=} h(ID_y || h(r_y \| T_2 \| RD_y || T_3)$ and on verification it computes new pseduo and temporary identity $TID^{new}_x = E_{d_y}(RD_x || r_y)$ for U_x and then generates current T_4 to compute $M_T = TID^{new}_x \oplus h(h(r_x \| T_1) \| RD_{TA} \| T_4)$,

$M_C = h(TID_x^{new}||T_4||TID_x)$ and sends $M_{sg4} = \{M_{sg3}, M_T, M_C, T_3, T_4\}$ to U_x.

PKM-6: After receiving M_{sg4} from CS_y and after successful verification of the timeliness of T_4, U_x computes $h(r_z\|T_3) = M_7 \oplus h(T_1\|T_3\|Q_z \cdot d_x)$, $h(RD_z\|TC_z) = M_w \oplus h(h(r_z\|T_3)\|T_1)$, $M_z = h(h(RD_z\|TC_z)\|T_1\|T_3)$, and session key $SK_{x,z} = h(h(h(r_x\|T_1)\|TC_x\|T_1\|RD_x\|RD_{TA})\|h(r_z\|T_3)\|T_1\|T_2\|T_3\|M_z)$, and checks $M_9 \cdot P \stackrel{?}{=} M_8 + h(SK_{x,z}\|M_T\|T_1\|T_3) \cdot Q_z$. If this condition holds true, SD_z is genuine; otherwise, U_x immediately aborts the process. U_x also computes $TID_x^{new} = M_T \oplus h(h(r_x\|T_1)\|RD_{TA}\|T_4)$ and checks $M_C \stackrel{?}{=} h(TID_x^{new}||T_4||TID_x)$ In addition and if the above condition is true U_x replaces TID_x with TID_x^{new} in it's memory database which will be used in the upcoming sessions.

VII. PERFORMANCE ANALYSIS

This section evaluates the performance of the proposed scheme in terms of computation cost, and communication cost of the proposed scheme with the existing schemes. The details are given in the following subsections.

A. COMPUTATIONAL COST ANALYSIS

The subsection presents a high-level overview of the comparative computing cost study of our method and similar schemes such as [13], [37], [42], [43], [44]. We set up a real-time environment in which we run an experiment using the MIRACL Library on a smartphone, the iPhone Xs Max, which has 8 GB of RAM and a Dual Core + 1.6 GHz Quad-Core Processor. The underlying IOS operating system version is version 15.1. In other words, the iPhone Xs Max is used and represents a user/mobile device in this experiment. The Dell Ultrabook 8757P, with an Intel Core i5-6300C processor and 8 GB of RAM, was used as a content server, with the Windows 10 Pro operating system running on top of the machine. In a similar way, we utilized a Raspberry Pi 3 B+ with a Cortex-A53 (ARMv8) 64-bit SoC running at 1.4 GHz and 1 GB of LPDDR2 SDRAM RAM to simulate a smart device. Table 2 contains the simulation results for each device; also, following the analogy of [45], we consider $T_f \approx T_e$, where T_f is the running time of executing a fuzzy extractor and T_e is the time used to compute the results. According to the experimental results, the proposed scheme may complete the authenticated process in about 59.00 milliseconds at a cost of 40 $T_h + 16T_e + 3\ T_a + 3\ T_r$. In comparison to the schemes such as Wazid *et al.* [13], Hussain *et al.* [42], Jia *et al.* [43], Chang *et al.* [37], and Challa *et al.* [44], complete the authentication processes in about 60.428, 32.929, 58.561, 14.339, and 12.574 milliseconds, respectively. According to the computational cost, the Challa *et al.* performs the best; however, the proposed scheme is significantly more secure than the rest of the schemes.The comparison is each of the entity is given in the Table 3.

TABLE 2. Experimental results.

↓Operation/ Device→	Mobile	Server	Drone
T_b: Bi-linear Pairing	17.36	4.038	12.52
T_e: Point Multiplication	5.116	0.926	4.107
T_a: Point Addition	0.013	0.006	0.018
T_h: One way Hash	0.009	0.004	0.006
T_r: Random Number Generation	2.011	0.118	1.185
T_{se}: Symmetric Key Operations	0.017	0.08	0.013

B. COMMUNICATION COST

In this section, the communication cost of the proposed scheme is calculated and compared with the existing schemes. Table 4 displays a size of different metric entities used in the proposed scheme. For the sake of comparison and simplicity, the size of user identities is taken to be 64 bits long, the timestamp is 32 bits, the hash function is 160 bits, the random number is 64 bits, encryption (AES) is 128 bits, and the size of ECC operations are fixed at 320 bits in order to maintain a comparable security level with 1024 bits RSA. Table 5 displays a detailed comparison among the suggested schemes presented in [13], [37], [42], [43], [44] with regard to the bits transferred. The cost of communication of the proposed scheme is 3072 bits, which is equal to Wazid's *et al.* scheme. The total communication cost of Jia *et al.* is 3520 bits, which is slightly higher than the proposed scheme. On the other hand, the total communication costs of Challa *et al.*, Hussain *et al.*, and Chang *et al.*, are 1536 bits, 2080 bits, and 2144 bits, respectively; which are less than the proposed scheme. However, the proposed scheme provides better security than all the above mentioned schemes.

VIII. THE SECURITY ANALYSIS

To describe the security of the proposed scheme, we have scrutinized the scheme through formal and informal security analysis in the following subsections:

A. AUTHENTICATION PROOF BASED ON THE Burrows–ABADI–NEEDHAM LOGIC (BAN LOGIC)

The security of the proposed scheme is formally analyzed in the standard model using the widely accepted Burrows–Abadi– Needham logic [46].

1) POSTULATES FOR BAN LOGIC

Some of the logical postulates of BAN logic and the meaning related to the postulates are given below in Table 6:

2) SECURITY GOAL ESTABLISHMENT

Established security goals and logical notations of the BAN logic are given below in Table 7.

G_1: $U_x| \equiv SD| \equiv Ux \stackrel{SK_{x,y}}{\longleftrightarrow} SD$

3) PROPOSED SCHEMES IDEALIZED FORM

M1: $SD \rightarrow U_x$: $(h(r_z||T_3) \oplus h(T_1||T_2||T_3||d_z||Q_x))$, $h(RD_z||TC_z) \oplus h(h(r_z||T_3)||T_1)$, $Mz.P$, $Mz + h$

TABLE 3. Computational costs.

Reference	Mobile User	Content Server	Smart Device	RT(ms)
Wazid *et* al. [13]	$19T_h + 6T_e + T_a + T_r$	$11T_h + 6T_e + T_a + T_r$	$12T_h + 5T_e + T_a + T_r$	60.425
Hussain *et* al. [42]	$8T_h + 2T_e + 2T_r$	$7T_h + T_e$	$6T_h + 4T_e + T_r$	32.929
Jia. *et* al. [43]	$5T_h + 2T_e + T_r + T_b$	$9T_h + 3T_e + T_r + T_b$	$4T_h + 2T_e + T_r + T_b$	58.561
Chang *et* al. [37]	$6T_h + 2T_e + T_r$	$6T_h + 2T_e + T_r$	$8T_h$	14.339
Challa *et* al. [44]	$11T_h + T_e + T_r$	$5T_h$	$6T_h + T_e + T_r$	12.574
Proposed	$19T_h + 6T_e + T_a + T_r$	$9T_h + 5T_e + T_a + 2T_{sc} + T_r$	$12T_h + 5T_e + T_a + T_r$	59.651

TABLE 4. Communication cost values.

Attribute	Cost Value
Identity	64 bits
Timestamp	32 btis
Hash Function (SHA-1)	160 btis
Random Number	64 btis
Encryption (AES)	128 btis
Elliptic Curve (ECC)	320 btis

TABLE 5. Communication cost analysis.

Reference	User (U_x)	Content Server (CS_y)	Smart Device (SD_z)	Total Cost
Proposed	800 bits	928 + 352 bits	992 bits	3072 bits
Wazid *et* al. [13]	1056 bits	1088 bits	928 bits	3072 bits
Hussain *et* al. [42]	896 bits	672 bits	512 bits	2080 bits
Jia. *et* al. [43]	672 bits	1344 + 832 bits	672 bits	3520 bits
Chang *et* al. [37]	672 bits	608 + 352 bits	512 bits	2144 bits
Challa *et* al. [44]	672 bits	352 bits	512 bits	1536 bits

$(SKz, x||T_1||T_3).dz$, $h(ID_y||h(r_y||T_z||RDy||T_3),T_3)$, $TID_x^{new} \oplus h(h(r_x, T_1)||RD_{TA}||T_4)$, $h(TID_x^{new}||T_4||TID_x)$, $(T_3, t4)$

4) ASSUMPTIONS

$A1 : U_x| \equiv \text{`}\#(r_x, T1)$
$A2 : U_x| \equiv SD| \equiv SD \sim X$
$A3 : U_x| \equiv SD \Rightarrow (SD \overset{SK_{Ix}}{\longleftrightarrow} SD)$
$A4 : SD| \equiv CS \Rightarrow CS| \sim X$
$A5 : CS| \equiv (r_y, T_4, T_2)$
$A6 : SD| \equiv \#(r_z, T_3)$
$A7 : U_x| \equiv (U_x \overset{RD_x}{\longleftrightarrow} CS)$
$A8 : SD| \equiv (CS \overset{RD_z}{\longleftrightarrow} SD)$
$A9 : SD| \equiv (CS \overset{dz}{\longleftrightarrow} SD)$
$A10 : U_x| \equiv (U_x \overset{RD_{TA}}{\longleftrightarrow} CS)$
$A11 : U_x| \equiv (U_x \overset{TID_x}{\longleftrightarrow} CS)$
$A12 : U_x| \equiv (U_x \overset{TID_x}{\longleftrightarrow} SD)$
$A13 : U_x| \equiv CS| \Rightarrow CS| \sim X$
$A14 : SD| \equiv (SD \overset{RD_{TA}}{\longleftrightarrow} M_z)$

Step-1 According to Message 1:

- $P1 : U_x \lhd \langle U_x \overset{Q_x}{\longleftrightarrow} SD,\ T_1,\ T_3,\ d_z\rangle_{\langle rz\rangle}, \langle U_x \overset{RD_z}{\longleftrightarrow} SD, TC_z, T_1, T_3\rangle_{\langle rz\rangle}, \langle M_z.P\rangle, \langle M_z, T_1, T_3\rangle_{\langle U_x \overset{SK_{zx}}{\longleftrightarrow} SD,\ d_z\rangle}$, $\langle ID_y,\ U_x \overset{RD_y}{\longleftrightarrow} SD,\ T_2,\ T_3\rangle_{\langle ry\rangle}$, $\langle T_3\rangle$, $\langle U_x \overset{RD_x}{\longleftrightarrow} CS,\ TID_x,\ T_1,\ T_4\rangle\ U_x \overset{r_x}{\longleftrightarrow} SD$, $\langle U_x \overset{TID_x}{\longleftrightarrow} CS,\ T_3,\ T_4\rangle_{\langle TID_x^{new}\rangle}$

Step-2 Based on P1, Assumptions 1,2,3 and message meaning rule we get:

- $P2 : U_x \lhd \langle T_1,\ T_2,\ d_z\rangle_{\langle rz\rangle}, \langle T_1,\ T_3,\ TC_z\rangle_{\langle rz\rangle}, \langle Mz.P\rangle, \langle M_z, T_2, T_3\rangle_{\langle dz\rangle}, \langle ID_y, T_1,\ T_3\rangle_{\langle ry\rangle}, \langle T_3\rangle, \langle T_1, T_4\rangle_{\langle TID_x^{new}\rangle}$

Step-3 According to the P2 and message belief rule, nonce verification and freshness rule we get:

- $P3 : U_x| \equiv CS| \equiv \langle dz\rangle_{\langle rz\rangle}, \langle TC_z\rangle_{\langle rz\rangle}, \langle Mz.P\rangle, \langle Mz\rangle_{\langle dz\rangle}, \langle ID_y\rangle_{\langle ry\rangle}$

Step-4 based on S3, Assumptions A2 and A13 and jurisdiction rule we get:

- $P4 : U_x| \equiv \langle dz\rangle_{\langle rz\rangle}, \langle TCz\rangle_{\langle rz\rangle}, \langle Mz.P\rangle, \langle Mz\rangle_{\langle dz\rangle}, \langle ID_y\rangle_{\langle ry\rangle}$

Step-5 Based on P4 and P3 and assumptions A2, A13, A14 and belief rule we get:

- $P5 : U_x| \equiv SD| \equiv Ux \overset{SK_{x,y}}{\longleftrightarrow} SD$ **Goal1**

TABLE 6. Postulates for BAN logic.

$\frac{A\|\equiv A \overset{K}{\longleftrightarrow} Y, A \lhd <B>_K}{A\|\equiv Y\|\sim K}$	Message-meaning rule
$\frac{A\|\equiv \#B, A\|\equiv Y\|\sim B}{A\|\equiv Y\|\sim K}$	Nonce-verification rule
$\frac{A\|\equiv B, A\|\equiv C}{A\|\equiv (B,C)}$	Belief Rule
$\frac{A\|\equiv \#B, A\|\equiv C}{A\|\equiv \#(B,C)}$	Fresh conjuncatenation rule
$\frac{A\|\equiv Y \Rightarrow B, A\|\equiv Y\|\sim B}{A\|\equiv B}$	Jurisdiction rule

TABLE 7. BAN logic notations.

$A\| \equiv B$	A believes a statement B
$A \overset{K}{\longleftrightarrow} Y$	Share a key K between A and Y
$\#B$	B is fresh
$A \lhd B$	A sees B
$A\| \sim B$	A said B
$(B, C)_K$	B, C is hashed by key K
$\{B\}_K$	B is hashed with key K
$< B >_K$	B is encrypted with key K

IX. CONCLUSION

In this article, we analyzed a recent authentication scheme by the Wazid *et al.* and found some incorrectness.

An authentication scheme is proposed in Wazid *et al*. for the NIB-enabled 6G networking systems. However, the scheme has missed an essential step of encryption at the content server. Therefore, the scheme is impractical and can not complete the authentication process. In response, the article proposed a modified version of the scheme in order to provide a better authentication mechanism. The article provides a detailed comparison of the proposed scheme with existing schemes in terms of computational cost and communication costs. The security analysis is also provided in this scheme. The proposed scheme will be implemented in the IoT-based networking system in the future.

REFERENCES

[1] M. Pozza, A. Rao, H. Flinck, and S. Tarkoma, "Network-in-a-box: A survey about on-demand flexible networks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2407–2428, Feb. 2018.

[2] H. Yi, "A secure blockchain system for Internet of Vehicles based on 6G-enabled network in box," *Comput. Commun.*, vol. 186, pp. 45–50, Mar. 2022.

[3] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May/Jun. 2020.

[4] (Apr. 2020). 3G4G. *Beginners: Network in a Box (NIB)*. [Online]. Available: https://www.slideshare.net/3G4GLtd/

[5] (Apr. 2020). A. Networks. *System Architecture Evolution (SAE) and the Evolved Packet Core (EPC)*. [Online]. Available: https://www.artizanetworks.com/resources/tutorials/sae_tec.html

[6] P. P. Ray, N. Kumar, and M. Guizani, "A vision on 6G-enabled NIB: Requirements, technologies, deployments, and prospects," *IEEE Wireless Commun.*, vol. 28, no. 4, pp. 120–127, Aug. 2021.

[7] J.-S. Huang and Y.-N. Lien, "Challenges of emergency communication network for disaster response," in *Proc. IEEE Int. Conf. Commun. Syst. (ICCS)*, Nov. 2012, pp. 528–532.

[8] Z. Shao, Y. Liu, Y. Wu, and L. Shen, "A rapid and reliable disaster emergency mobile communication system via aerial ad hoc BS networks," in *Proc. 7th Int. Conf. Wireless Commun., Netw. Mobile Comput.*, Sep. 2011, pp. 1–4.

[9] (Sep. 2021). T. Networks. *Network in a Box Rapidly Deployable Communications*. [Online]. Available: https://www.tecore.com/network-in-a-box-products/

[10] M. K. Mahmood and F. M. Al-Naima, "Developing a multi-layer strategy for securing control systems of oil refineries," *Wireless Sensor Netw.*, vol. 2, no. 7, p. 520, 2010.

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

[12] S. A. Chaudhry, A. Irshad, M. A. Khan, S. A. Khan, S. Nosheen, A. A. AlZubi, and Y. B. Zikria, "A lightweight authentication scheme for 6G-IoT enabled maritime transport system," *IEEE Trans. Intell. Transp. Syst.*, early access, Dec. 22, 2021, doi: 10.1109/TITS.2021.3134643.

[13] M. Wazid, A. K. Das, N. Kumar, and M. Alazab, "Designing authenticated key management scheme in 6G-enabled network in a box deployed for industrial applications," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 7174–7184, Oct. 2021.

[14] D. M. Nessett, "A critique of the burrows, Abadi and Needham logic," *ACM SIGOPS Operating Syst. Rev.*, vol. 24, no. 2, pp. 35–38, Apr. 1990.

[15] H. Wu, L. Wang, and G. Xue, "Privacy-aware task allocation and data aggregation in fog-assisted spatial crowdsourcing," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 1, pp. 589–602, Jan. 2020.

[16] K. Zhao, S. Tang, B. Zhao, and Y. Wu, "Dynamic and privacy-preserving reputation management for blockchain-based mobile crowdsensing," *IEEE Access*, vol. 7, pp. 74694–74710, 2019.

[17] C. Miao, L. Su, W. Jiang, Y. Li, and M. Tian, "A lightweight privacy-preserving truth discovery framework for mobile crowd sensing systems," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, May 2017, pp. 1–9.

[18] Y. Zheng, H. Duan, and C. Wang, "Learning the truth privately and confidently: Encrypted confidence-aware truth discovery in mobile crowdsensing," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 10, pp. 2475–2489, Oct. 2018.

[19] X. Guo, H. Lin, Z. Li, and M. Peng, "Deep-reinforcement-learning-based QoS-aware secure routing for SDN-IoT," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6242–6251, Jul. 2020.

[20] F. Qiu, F. Wu, and G. Chen, "Privacy and quality preserving multimedia data aggregation for participatory sensing systems," *IEEE Trans. Mobile Comput.*, vol. 14, no. 6, pp. 1287–1300, Jun. 2014.

[21] A. Liu, W. Wang, S. Shang, Q. Li, and X. Zhang, "Efficient task assignment in spatial crowdsourcing with worker and task privacy protection," *GeoInformatica*, vol. 22, no. 2, pp. 335–362, 2018.

[22] Z. Zhang, S. He, J. Chen, and J. Zhang, "REAP: An efficient incentive mechanism for reconciling aggregation accuracy and individual privacy in crowdsensing," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 12, pp. 2995–3007, Dec. 2018.

[23] D. Yuan, Q. Li, G. Li, Q. Wang, and K. Ren, "PriRadar: A privacy-preserving framework for spatial crowdsourcing," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 299–314, 2020.

[24] Z. Ma, T. Zhang, X. Liu, X. Li, and K. Ren, "Real-time privacy-preserving data release over vehicle trajectory," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 8091–8102, Aug. 2019.

[25] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," *J. Manuf. Syst.*, vol. 47, pp. 93–106, Apr. 2018.

[26] J. Zhang, Z. Wang, D. Wang, X. Zhang, B. B. Gupta, X. Liu, and J. Ma, "A secure decentralized spatial crowdsourcing scheme for 6G-enabled network in box," *IEEE Trans. Ind. Informat.*, vol. 18, no. 9, pp. 6160–6170, Sep. 2021.

[27] V. Ramaswamy and J. T. Correia, "Enhancing service availability of LTE-in-a-box systems using 3GPP-compliant strategies," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Los Angeles, CA, USA Oct. 2018, pp. 512–517.

[28] A. S. Thyagaturu, Y. Dashti, and M. Reisslein, "SDN-based smart gateways (Sm-GWs) for multi-operator small cell network management," *IEEE Trans. Netw. Service Manage.*, vol. 13, no. 4, pp. 740–753, Dec. 2016.

[29] H. Viswanathan and P. E. Mogensen, "Communications in the 6G era," *IEEE Access*, vol. 8, pp. 57063–57074, 2020.

[30] P. Yang, Y. Xiao, M. Xiao, and S. Li, "6G Wireless communications: Vision and potential techniques," *IEEE Netw.*, vol. 33, no. 4, pp. 70–75, Jul./Aug. 2019.

[31] K. Samdanis and T. Taleb, "The road beyond 5G: A vision and insight of the key technologies," *IEEE Netw.*, vol. 34, no. 2, pp. 135–141, Mar./Apr. 2020.

[32] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[33] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. 19th Annu. Int. Cryptol. Conf. (CRYPTO)*, Santa Barbara, CA, USA, vol. 1666, 1999, pp. 388–397.

[34] S. A. Chaudhry, J. Nebhan, K. Yahya, and F. Al-Turjman, "A privacy enhanced authentication scheme for securing smart grid infrastructure," *IEEE Trans. Ind. Informat.*, vol. 18, no. 7, pp. 5000–5006, Jul. 2021.

[35] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Proc. Int. Conf. Theory Appl. Cryptograph Techn. Adv. Cryptol. (EUROCRYPT)*, Innsbruck, Austria, 2001, pp. 453–474.

[36] T. Maitra, M. S. Obaidat, R. Amin, S. H. Islam, S. A. Chaudhry, and D. Giri, "A robust ElGamal-based password-authentication protocol using smart card for client-server communication," *Int. J. Commun. Syst.*, vol. 30, no. 11, p. e3242, Jul. 2017.

[37] 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.

[38] Z. Ali, S. A. Chaudhry, K. Mahmood, S. Garg, Z. Lv, and Y. B. Zikria, "A clogging resistant secure authentication scheme for fog computing services," *Comput. Netw.*, vol. 185, Feb. 2021, Art. no. 107731.

[39] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2691, Aug. 2015.

[40] S. A. Chaudhry, A. Irshad, J. Nebhen, A. K. Bashir, N. Moustafa, Y. D. Al-Otaibi, and Y. B. Zikria, "An anonymous device to device access control based on secure certificate for internet of medical things systems," *Sustain. Cities Soc.*, vol. 75, Dec. 2021, Art. no. 103322.
[41] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: A brief survey of results from 2004 to 2006," in *Security With Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*. Springer-Verlag, 2017, pp. 79–99. [Online]. Available: https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.207.3446
[42] S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan, and N. Kumar, "Amassing the security: An ECC-based authentication scheme for Internet of Drones," *IEEE Syst. J.*, vol. 15, no. 3, pp. 4431–4438, Sep. 2021.
[43] X. Jia, D. He, N. Kumar, and K.-K. R. Choo, "Authenticated key agreement scheme for fog-driven IoT healthcare system," *Wireless Netw.*, vol. 25, pp. 4737–4750, May 2019.
[44] S. Challa, A. K. Das, P. Gope, A. V. Vasilakos, N. Kumar, and F. Wu, "Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems," *Future Gener. Comput. Syst.*, vol. 108, pp. 1267–1286, Nov. 2020.
[45] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in Internet of Drones deployment," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3572–3584, Apr. 2019.
[46] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proc. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 426, no. 1871, pp. 233–271, 1989.

IJAZ DARMAN received the B.Sc. degree in computer system engineering from the University of Engineering and Technology (UET) Peshawar, Peshawar, Pakistan, in 2018. He is currently pursuing the Master of Science degree in electrical and electronics engineering with Istanbul Gelisim University (IGU), Istanbul, Turkey. His research interests include 5G and 6G wireless communication systems, security especially authentication, authorization, accounting (AAA) management, and the Internet of Things (IoT).

MUSARIA KARIM MAHMOOD received the B.Sc. degree in electronics engineering from ENSIETA, France, and the M.S. and Ph.D. degrees in communication and electronics engineering from Al-Nahrian University. From 2003 to 2021, he was a Lecturer with the Department of Electrical Engineering, Tikrit University, Iraq, an Assistant Professor with the Department of Electrical and Electronic Engineering, Philadelphia University, Jordan, a Visiting Professor with the Department of Electrical and Electronic Engineering, Atilim University, Turkey, and an Assistant Professor with the Department of Electrical and Electronic Engineering, IGU, Turkey. He is currently working as an Assistant Professor with the Department of Energy Systems Engineering, Ankara Yildirim Beyazit University, Turkey. His research interests include network reliability, data security, and WSN.

SHEHZAD ASHRAF CHAUDHRY received the master's and Ph.D. degrees (Hons.). He is currently an Associate Professor in cybersecurity engineering with the Department of Computer Science and Information Technology, College of Engineering, Abu Dhabi University, Abu Dhabi, United Arab Emirates, and the Department of Computer Engineering, Faculty of Engineering and Architecture, Nisantasi University, Istanbul, Turkey. Before this, he served at Istanbul Gelisim University, Turkey, University of Sialkot, Pakistan, and International Islamic University, Islamabad, Pakistan. He has also supervised more than 40 graduate students in their research. Working in the field of information and communication security, he has published extensively in prestigious venues, such as *IEEE Communications Standards Magazine*, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS, IEEE TRANSACTIONS ON RELIABILITY, *ACM Transactions on Internet Technology*, *Sustainable Cities and Society* (Elsevier), *FGCS*, *IJEPES*, *Computer Networks*, and *Digital Communications and Networks*. He occasionally writes on issues of higher education in Pakistan. Over 150 publications and with an H-index of 37, I-10 index of 76, and accumulate impact factor of more than 340, he has published more than 115 SCI/E indexed manuscripts and has been cited more than 3800 times. His current research interests include lightweight cryptography, elliptic/hyper elliptic curve cryptography, multimedia security, e-payment systems, MANETs, SIP authentication, smart grid security, IP multimedia subsystems, and next generation networks. He was awarded a Gold Medal for achieving maximum distinction of 4/4 CGPA in his mater's degree. In 2018, considering his research, Pakistan Council for Science and Technology granted him the Prestigious Research Productivity Award, while affirming him among Top Productive Computer Scientist in Pakistan. For the consecutive two years, he is being listed among Top 2% Computer Scientists across the world in Stanford University's report.

SAJJAD AHMAD KHAN received the Ph.D. degree in computer engineering from Kocaeli University, Turkey, in 2020. He is currently associated as a Postdoctoral Researcher with the Department of Computer Engineering, Hoseo University, South Korea. Before this, he worked as an Associate Researcher at Istanbul Technical University (ITU), Turkey, for two years. In 2017, he visited Adam Mickiewicz University, Poznan, Poland, in order to conduct research. He has also published over 20 research papers. Besides, he is also an active reviewer for many international conferences and journals. His research interests include 5G and beyond wireless communication and mobile networks, such as named data network (NDN) over VANETs, mobility and handover management, cooperative communication, radio resource management, authentication, authorization, and accounting (AAA) management, the Internet of Things (IoT), and machine learning.

HUHNKUK LIM (Member, IEEE) received the Ph.D. degree in computer engineering from the Gwangju Institute of Science and Technology (GIST), South Korea, in 2006. He was worked as a Principal Researcher with the Korea Institute of Science and Technology Information (KISTI), from 2006 to 2019. He was a Research Associate with the Department of Computer Science, California Institute of Technology (Caltech), Pasadena, CA, USA, from 2013 to 2014. Since March 2020, he has been an Associate Professor with the Department of Computer Engineering, Hoseo University. He has published more than 70 refereed papers in the areas of the IoT, information centric networking (ICN), cloud/edge computing, and user-driven network/computing resource control in archival journals and conference proceedings. His current research interests include the IoT, edge computing, AI, and named data networking (NDN) for connected vehicles. He is currently serving as an Associate Editor for *KSII Transactions on Internet and Information Systems* (SCI Indexed), *The Journal of Korean Institute of Communications and Information Sciences*, and the *Journal of Internet Computing and Services*.