Designing Authenticated Key Management Scheme in 6G-Enabled Network in a Box Deployed for Industrial Applications

by

Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, Mamoun Alazab

in

IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS 1

Report No: IIIT/TR/2020/-1

Centre for Security, Theory and Algorithms
International Institute of Information Technology
Hyderabad - 500 032, INDIA
June 2020

Designing Authenticated Key Management Scheme in 6G-Enabled Network in a Box Deployed for Industrial Applications

Mohammad Wazid, *Senior Member, IEEE*, Ashok Kumar Das, *Senior Member, IEEE*, Neeraj Kumar, *Senior Member, IEEE*, and Mamoun Alazab, *Senior Member, IEEE*

***Abstract*—6G-enabled network in a box (NIB) is a multigenerational, rapidly deployable hardware, and software technology for the communication. 6G-enabled NIB provides high level of flexibility which makes it capable to provide connectivity services for different types of applications as it is effective for the communications of after disaster scenario, battlefields scenario, and industrial scenario. In 6G-enabled NIB deployed industrial applications, various passive and active attacks are possible because the involved entities communicate over insecure channel. In this article, a new remote user authentication and key management scheme is proposed for securing 6G-enabled NIB deployed for industrial applications, which we call in short as UAKMS-NIB. The security analysis shows the resilience of UAKMS-NIB against various types of possible attacks. The practical demonstration of UAKMS-NIB is also provided to measure its impact on the network performance parameters. Finally, a comparative analysis with other closely related existing schemes shows that UAKMS-NIB performs better than the existing schemes.**

***Index Terms*—Authentication, automated validation of Internet security protocols and applications (AVISPA), key management, multiprecision integer and rational arithmetic cryptographic library (MIRACL), network in a box (NIB), NS2 simulation, security.**

Manuscript received May 29, 2020; revised July 13, 2020; accepted August 25, 2020. This work was supported in part by the Ripple Centre of Excellence Scheme, CoE in Blockchain under Sanction IIIT/R&D Office/Internal Projects/001/2019, IIIT Hyderabad, India, and in part by the Mathematical Research Impact Centric Support (MATRICS) project funded by the Science and Engineering Research Board (SERB), India under Reference MTR/2019/000699. Paper no. TII-20-2664. *(Corresponding authors: Ashok Kumar Das; Neeraj Kumar.)*

Mohammad Wazid is with the Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun 248002, India (e-mail: wazidkec2005@gmail.com).

Ashok Kumar Das is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India (e-mail: iitkgp.akdas@gmail.com).

Neeraj Kumar is with the Department of Computer Science and Engineering, Thapar University, Patiala 147004, India (e-mail: neeraj.kumar@thapar.edu).

Mamoun Alazab is with the College of Engineering, IT and Environment, Charles Darwin University, Casuarina, NT 0810, Australia (e-mail: alazab.m@ieee.org).

Color versions of one or more of the figures in this article are available online at https://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2020.3020303

I. Introduction

NETWORK in a box (NIB) or network in a bag is considered as a multigenerational 2G, 3G, 4G, 5G, and 6G all-in-one, rapidly deployable hardware and software solution for the network communication. The idea of NIB revolves around incorporating all types of software and hardware modules which are essential by a mobile network in a single bag contains a handful of physical devices [1]. The 6G-enabled NIB provides high level of flexibility which makes it in providing connectivity services for various applications (for example, "after disaster scenario," "battlefields scenario," and "industrial scenario"). It is worth noticing that the emergency and tactical networks are designed to be flexible as well as adaptable due to the reason that deployment of these networks is not known properly. These kinds of networks fall under the "mobile ad hoc networks (MANETs)." Moreover, NIB is portable in nature. So, it can be applicable for disasters management, such as earthquakes and tsunamis.

Recently, the standards for emergency and tactical networks have been developed which can support solutions with less number of physical devices along with the main goal in increasing the viability. Many networks providers have also followed such an idea to launch these networks, which can be deployed using very few physical devices or even a single one. Hence, NIB makes an alternative network communication technology in order to satisfy the next-generation mobile networks requirements (i.e., battlefield communication, communication network for industrial use). In general, the 6G-enabled NIB can be "configured to work either completely alone or together with other legacy network components or with other NIBs." It also provides operational availability for all wireless networks in a small, compact and portable form for commercial, industrial, private, government, and military uses [2]–[6].

The 6G-enabled NIB deployed for industrial applications consists of various components, such as "evolved packet core (EPC)," "tower along with antenna," "user with mobile device," "Internet Protocol (IP) multimedia subsystem (IMS)," "content server," "smart industrial devices," and "trusted authority." All these components facilitate the communication of a user with the other users or to access important services, such as access of webs, multimedia services or data of smart industrial devices

[1]–[3]. The smart industrial devices are deployed for monitoring and controlling of industrial equipments. The 6G wireless communication technology facilitates communication among these components and devices.

A. Motivation

Though 6G-enabled NIB provides many advantages over other wireless communication technologies, network security issues exist with the upcoming 6G-enabled wireless networks (i.e., NIB). It happens because security measurements are not fully adopted in the new wireless communication networks, such as 6G. There is a newly discovered potential for man-in-the-middle attack in "terahertz-based 6G networks," which is observed through multiple research studies [7]. Therefore, it is very important to highlight "6G-enabled NIB deployed for industrial applications" may have various security and privacy issues as it may be vulnerable to different types of attacks [7]. In 6G-enabled NIB deployed for industrial applications, various attacks, such as replay, man-in-the-middle, impersonation, sensitive information leakage, illegal session key computation, privileged insider, and smart industrial device stolen attack may be possible [7]. Therefore, we need to deploy security mechanisms in a "6G-enabled NIB deployed for industrial applications." Furthermore, a registered user needs to authenticate with the concerned smart industrial devices to access the real-time data. There are several critical applications of NIB, such as disasters management (earthquakes and tsunami), where a user needs to access the real-time data directly from the smart devices deployed in the network. To mitigate these issues, authentication and key establishment between a legitimate user and an accessed smart industrial device should be executed through the important intermediate node, called the content server. We, therefore, aim to design a novel robust "user authentication and key agreement scheme" for mutual authentication and key establishment among the user and smart industrial devices via the content server.

B. Research Contributions

The main contributions are manifold.

1) A new remote user authentication scheme is proposed for secure communication happens in 6G-enabled NIB deployed for industrial applications, called UAKMS-NIB. Using the UAKMS-NIB, a genuine user can authenticate a smart industrial device, and then can access its real-time data using the establish session key.
2) The provided security analysis including the formal security verification using the widely-accepted "automated validation of Internet security protocols and applications (AVISPA)" [8] proves the resilience of UAKMS-NIB against various types of possible attacks that are needed in 6G-enabled NIB environment.
3) The practical demonstration of UAKMS-NIB using widely used NS2 simulation is then provided to measure its impact on various network performance parameters.
4) The testbed experiments on various cryptographic primitives using the broadly accepted "Multiprecision Integer and Rational Arithmetic Cryptographic Library (MIRACL)" [9] under both server and Raspberry PI 3 settings have been performed.
5) Finally, a detailed comparative study among UAKMS-NIB and other existing competing user authentication schemes shows the performance of UAKMS-NIB is better than other existing competing schemes.

C. Paper Outline

The rest of this article is organized as follows. Section II provides a brief survey on related existing schemes. Section III explains the network and threat models used in UAKMS-NIB. Section IV explains the phases associated with the proposed scheme (UAKMS-NIB). Section V provides the security analysis of the proposed UAKMS-NIB. In addition, Section VI gives the formal security verification using the widely accepted AVISPA tool [8]. Section VII provides the practical demonstration of UAKMS-NIB using NS2 simulation study. Section VIII provides the experimental results using MIRACL [9]. Next, Section IX gives a detailed comparative study of UAKMS-NIB with other existing competing schemes. Finally, Section X concludes this article.

II. Literature Review

Pozza *et al.* [1] presented some use cases around which the concept of NIB was conceived. The common features of NIB implementations were discussed along with different proposals. Some of the possible future research directions were also highlighted.

Ramaswamy and Correia [10] provided different methods to enhance resilience of 'long-term evolution (LTE)" networks deployed for military and public safety missions. Their methods can be enabled through 3GPP LTE specifications and also could be implemented as software enhancement for available systems. Thyagaturu *et al.* [11] presented a management technique which allowed multiple operators (for example, multiple servicing/packet gateways (S/P-GWs)) to flexibly interoperate via multiple smart gateways (Sm-GWs) in multitude of small cells. The software-defined networking (SDN) coordinated the adaptive allocation of uplink transmission bit rates to SDN-based Sm-GWs which in turn allocated the uplink transmission bit rates to evolved NodeBs on the basis of requirements.

Viswanathan and Mogensen [12] discussed the main technological transformations which defined the 6G. Some of them include "cognitive spectrum sharing techniques new spectrum bands," "integration of localization and sensing capabilities" into the definition of system, "achievement of extreme performance requirements on latency and reliability," new network architecture paradigms which included "subnetworks" and "RAN-core convergence" and new schemes for security and privacy requirements.

Yang *et al.* [13] highlighted some potential needs and presented an overview of the latest research on promising methods evolving to 6G, which had achieved the considerable attention. Moreover, the key technical challenges along with potential solutions associated with 6G were discussed. Samdanis and

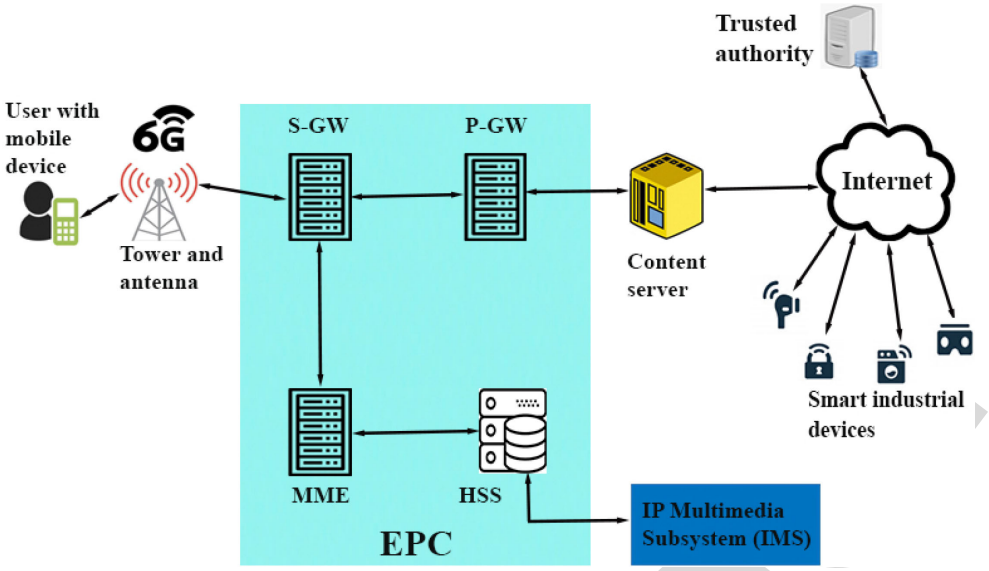

Fig. 1. 6G-enabled NIB deployed for industrial applications.

Taleb [14] provided the overview of key technologies which constituted the pillars for the evolution of wireless communication beyond 5G by considering "microservice oriented core network," "native IP based user plane," "network analytics," and "support for low latency-high reliability." The open challenges related to technical and business needs were also discussed by elaborating "footprint of softwarization," "security and trust," and "distributed architectures and services" in the direction of implementations of 6G.

III. System Models

The following two models are used to explain and analyze the UAKMS-NIB.

A. Network Model

The network model of "6G-enabled network in a box (NIB) deployed for industrial applications" is provided Fig. 1. It depicts the connection and flow of communication among different types of entities of NIB. EPC unit is used for providing converged voice and data on communication network such as 3G and 4G. EPC contains important components, such as packet data network gateway (P-GW), serving gateway (S-GW), mobility management entity (MME), and home subscriber server (HSS). P-GW is the connecting node between a user's mobile device and external networks. It is an entry point of data traffic for user's mobile device. To access multiple P-GWs, the user's mobile device can be connected to several P-GWs at the same time. Moreover, S-GW does task of routing and forwarding of user data packets. It is also responsible for inter-eNB handovers and provides mobility between LTE and other types of networks (for example, in between 2G/3G and P-GW). eNB is a base station which controls the mobiles in one or more cells. The base station which communicates with a user's mobile device is known as its serving eNB. MME is an important controller node in NIB, which is responsible for different types of tasks such as "idle mode user's mobile device tracking," "paging procedure (i.e., retransmissions)," "bearer activation and deactivation process," "S-GW selection for a user's mobile device at the initial attach," "intrahandover with core network," and "user's mobile device authentication with HSS. Apart from that MME handles the ciphering/integrity protection for nonaccess stratum signaling and the security key management. HSS is also an important component of NIB. It is a master user database which is stored in one single node (i.e., device). It allows the communications service providers to manage the users in real-time and in a cost effective way. The database of HSS stores information about the subscribers (i.e., users) to help in the authorization, details of devices as well as the user's location and the related service information. HSS also connects the user's request with the IMS. IMS is an essential component of an integrated network of telecommunications carriers to facilitate the use of IP for different types of packet transmission in wired or wireless communication for example, telephony, fax, e-mail, Internet access, web services, voice over IP, etc. There is also an important node, called as content server, which connects the users with the smart industrial devices.

Smart industrial devices are installed in this network for monitoring and controlling of industrial equipments. Each smart industrial device has an objective according to which it acts. Sometimes users of the industrial plant are interested in accessing the real-time data of smart industrial devices. For that purpose, user and smart industrial device have to perform the steps of authentication and key establishment mechanism so that they can exchange their information in a secure way.

B. Threat Model

The well-known "Dolev-Yao threat model (also known as the DY model)" [15] is followed in the design of UAKMS-NIB.

TABLE I
NOTATIONS UTILIZED IN UAKMS-NIB

Symbol	Significance
$\mathcal{A}$	An adversary
U_i, MD_{U_i}	i^{th} user and his/her mobile device, respectively
ID_{U_i}, RID_{U_i},	U_i's identity and pseudo identity, respectively
PW_{U_i}, BIO_{U_i}	U_i's password and biometric, respectively
TA, ID_{TA}	Trusted authority and its identity, respectively
RID_{TA}	TA's pseudo identity
CS_j, ID_{CS_j}	j^{th} content server and its identity, respectively
RID_{CS_j}	Pseudo identity of CS_j
SD_k, ID_{SD_k}	j^{th} smart industrial device & its identity, respectively
RID_{SD_k}	Pseudo identity of SD_k
d_{U_i}, d_{CS_j}	160-bit secret keys of U_i and CS_j, respectively
d_{SD_k}, d_{TA}	Secret keys of SD_k and TA, respectively
x	1024-bit long-term random secret of U_i
r_{U_i}, r_{CS_j},	160-bit random secrets of U_i and CS_j, respectively
r_{SD_k}	160-bit random secret of SD_k
T_x	Various current timestamps
ΔT	Maximum transmission delay
$Gen(\cdot)$	Generation process in fuzzy extractor
$Rep(\cdot)$	Reproduction process in fuzzy extractor
σ_{U_i}	Biometric secret key of U_i for BIO_i
τ_{U_i}	Public reproduction parameter of U_i for BIO_i
t	Error tolerance threshold required by fuzzy extractor
$h(\cdot)$	Collision-resistant cryptographic one-way hash function
SK_{U_i,SD_k}	Session key between U_i and SD_k
$\|\|$, $\oplus$	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

Thus, the communicating entities (parties) communicate among each other via a open channel. The end-point entities (i.e., users and smart industrial devices) are not in general trustworthy. However, the trusted authority (TA) of "6G-enabled NIB deployed for industrial applications" is considered as the fully trusted node. Since the TA performs the registration of network entities (users, content server, and smart industrial devices), it should not be compromised in any case; otherwise, the security of the entire network will be compromised. Apart from that, the content server can be considered as the semitrusted entity. Moreover, it is assumed that memory unit of the mobile device (MD) of the user is not equipped with tamper-resistant functioning. $\mathcal{A}$ can steal the mobile device of a user, and extracts all the stored sensitive information from the memory of MD by the power analysis attacks [16].

The current *de facto* standard model in the designing of key-exchange schemes, called as the "CK-adversary model" [17], is also considered in UAKMS-NIB. Under such a model, $\mathcal{A}$ can tamper messages such as in the DY model, and in addition to that he/she can compromise the session keys, private keys and other session states through the session hijacking attacks.

IV. PROPOSED SCHEME

The detailed description of various phases associated with the proposed UAKMS-NIB is provided in this section. The details of notations used in design of UAKMS-NIB are also provided in Table I.

A. Registration Phase

In this phase, a fully trusted authority (TA) selects a "non-singular elliptic curve $E_p(a,b)$ of the form: "$y^2 = x^3 + ax + b \pmod p$ over a Galois (finite) field $GF(p)$, where p is a large prime" so 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." In addition, the TA picks a "collision-resistant one-way cryptographic hash function $h(\cdot)$."

1) Smart Industrial Device Registration: The registration process of deployed smart industrial devices is performed by the TA through the following steps.

RSD1: The TA picks a unique identity ID_{SD_k} and a random secret key $d_{SD_k} \in Z_p^*$ for smart device SD_k, and also generates its own random secret key $d_{TA} \in Z_p^*$. For SD_k, the TA computes the pseudo identity of SD_k as $RID_{SD_k} = h(ID_{SD_k}||d_{TA})$, the public key of d_{SD_k} as $Q_{SD_k} = d_{SD_k} \cdot P$ and the temporal credential as $TC_{SD_k} = h(d_{SD_k} \, ||ID_{SD_k} \, ||RTS_{SD_k}||d_{TA})$, where RTS_{SD_k} is the registration timestamp of SD_k.

RSD2: The credentials $\{RID_{SD_k}, TC_{SD_k}, Q_{SD_k}, d_{SD_k}, h(\cdot), E_p(a,b), P\}$ are then stored in the memory of SD_k prior to deployment of each SD_k. Note that Q_{SD_k} is published publicly to other network entities, and the TA also sends RID_{SD_k} to CS_j in a secure way (encrypted using a symmetric secret key, say $K_{CS_j,TA}$ preshared among TA and CS_j).

2) Content Server Registration: In this phase, the registration of a content server CS_j is performed by the trusted authority TA through following steps.

RCS1: The TA chooses a unique identity ID_{CS_j} and a random secret key d_{CS_j} for CS_j to compute the pseudo identity of CS_j as $RID_{CS_j} = h(ID_{CS_j} \, ||d_{TA})$, public key $Q_{CS_j} = d_{CS_j} \cdot P$ and its own pseudorandom identity $RID_{TA} = h(ID_{TA} \, ||d_{TA})$.

RCS2: The credentials $\{RID_{CS_j}, RID_{U_i}, TID_{U_i}, RID_{TA}, RID_{SD_k}, Q_{CS_j}, d_{CS_j}, h(\cdot), E_p(a,b), P\}$ are then stored in CS_j's secure/tamper-resistant database by the TA. Note that RID_{U_i} and TID_{U_i} related to a registered user U_i are generated in Section IV-A3 during the user registration phase. In addition, Q_{CS_j} is published publicly to other network entities.

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

RU1: U_i chooses his/her unique identity ID_{U_i}, password PW_{U_i} and a long-term random secret $x \in Z_p^*$ to calculate the masked password $RPW_{U_i} = h(PW_{U_i} \, ||x)$. U_i then sends $\{ID_{U_i}, RPW_{U_i}\}$ to the TA through a secure channel.

RU2: After receiving the registration information, the TA computes the pseudoidentity $RID_{U_i} = h(ID_{U_i}||d_{TA})$, generates temporary identity TID_{U_i} and a random secret key $d_{U_i} \in Z_p^*$ for U_i. The TA computes temporal credential of U_i as $TC_{U_i} = h(ID_{U_i} \, ||RPW_{U_i}|| \, d_{U_i} \, ||d_{TA}|| \, RTS_{U_i})$, $\alpha_{U_i} = h(RPW_{U_i} \, ||RID_{U_i}) \oplus d_{U_i}$ and its public key as $Q_{U_i} = d_{U_i} \cdot P$. The TA then sends $\{RID_{U_i}, TID_{U_i}, RID_{TA}, TC_{U_i}, \alpha_{U_i}, Q_{U_i}, h(\cdot), E_p(a,b), P\}$ to MD_{U_i} of U_i through a secure channel. Note that Q_{U_i} is published publicly to other network entities.

RU3: After receiving the information from TA, U_i furnishes biometric data BIO_{U_i} to the biometric sensor of his/her mobile device MD_{U_i} to compute $(\sigma_{U_i}, \tau_{U_i}) = Gen(BIO_{U_i})$, where σ_{U_i} and τ_{U_i} 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 [18]." Furthermore, U_i computes $d_{U_i} = h(RPW_{U_i} \, ||RID_{U_i})$

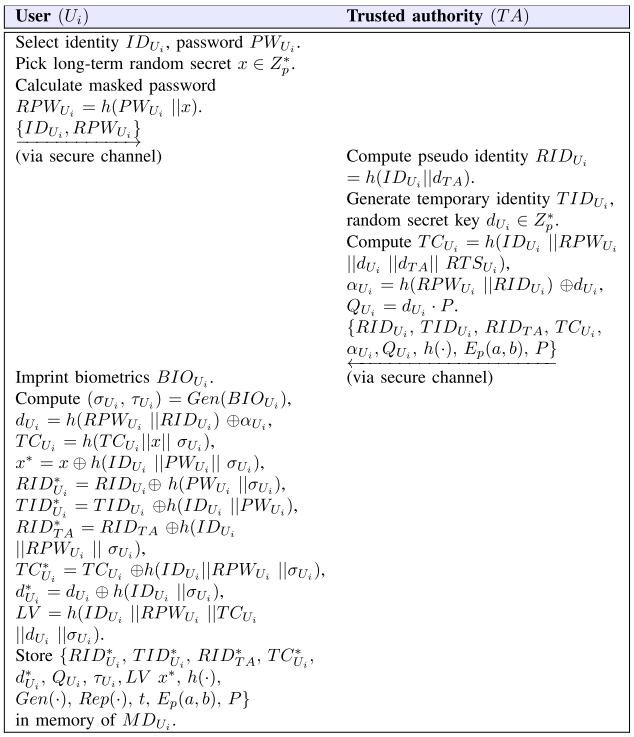

Fig. 2. User registration phase of the proposed UAKMS-NIB.

$\oplus\alpha_{U_i}, TC_{U_i} = h(TC_{U_i}||x|| \sigma_{U_i}), x^* = x \oplus h(ID_{U_i} ||PW_{U_i}||$ $\sigma_{U_i}), RID^*_{U_i} = RID_{U_i} \oplus h(PW_{U_i} ||\sigma_{U_i}), TID^*_{U_i} = TID_{U_i}$ $\oplus h(ID_{U_i} ||PW_{U_i}), RID^*_{TA} = RID_{TA} \oplus h(ID_{U_i} ||RPW_{U_i} ||$ $\sigma_{U_i}), TC^*_{U_i} = TC_{U_i} \oplus h(ID_{U_i}||RPW_{U_i} ||\sigma_{U_i}), d^*_{U_i} = d_{U_i} \oplus$ $h(ID_{U_i} ||\sigma_{U_i})$, and $LV = h(ID_{U_i} ||RPW_{U_i} ||TC_{U_i} ||d_{U_i}$ $||\sigma_{U_i})$. Finally, $\{RID^*_{U_i}, TID^*_{U_i}, RID^*_{TA}, TC^*_{U_i}, d^*_{U_i}, Q_{U_i},$ $\tau_{U_i}, LV\ x^*, h(\cdot), Gen(\cdot), Rep(\cdot), t, E_p(a,b), P\}$ are stored in the memory of MD_{U_i}. Note that α_{U_i}, x, ID_{U_i}, RPW_{U_i}, RID_{U_i}, TID_{U_i}, RID_{TA}, TC_{U_i}, TC_{U_i}, and d_{U_i} are deleted from the memory of MD_{U_i} to protect against stolen verifier, privileged insider attack, unauthorised session key computation, illegal user's password guessing and user impersonation attacks.

RU4: The TA sends the credentials $\{RID_{U_i}, TID_{U_i}\}$ to CS_j in a secure way through a preshared symmetric secret key $K_{CS_j,TA}$. The TA also erases $\{RID_{U_i}, TID_{U_i}, RID_{CS_j}$, RID_{SD_k}, d_{U_i}, d_{CS_j}, d_{SD_k}, TC_{U_i}, TC_{SD_k}, α_{U_i}, $RPW_{U_i}\}$ from its memory to protect against stolen verifier, privileged insider attack, unauthorised session key computation, illegal user's password guessing, and user impersonation attacks.

The user registration phase is summarized in Fig. 2.

B. User Login Phase

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

LGU1: U_i furnishes his/her identity ID_{U_i} and password PW'_{U_i}, and also imprints biometrics BIO'_{U_i} at the sensor of his/her mobile device MD_{U_i} to calculate biometric secret key $\sigma_{U_i} = Rep(BIO'_{U_i}, \tau_{U_i})$ provided that the "Hamming distance between the real biometrics BIO_i provided during the user registration phase and current BIO'_{U_i} is less than or equal to a predefined error tolerance threshold, say t".

LGU2: U_i then computes $x = x^* \oplus h(ID_{U_i} ||PW'_{U_i}||$ $\sigma_{U_i}), RPW'_{U_i} = h(PW'_{U_i} ||x), RID'_{U_i} = RID^*_{U_i} \oplus h(PW'_{U_i}$ $||\sigma_{U_i}), TID'_{U_i} = TID^*_{U_i} \oplus h(ID_{U_i} ||PW'_{U_i}), RID'_{TA}$ $= RID^*_{TA} \oplus h(ID_{U_i} ||RPW'_{U_i} || \sigma_{U_i}), TC'_{U_i} = TC^*_{U_i}$ $\oplus h(ID_{U_i}||RPW'_{U_i} ||\sigma_{U_i}), d_{U_i} = d^*_{U_i} \oplus h(ID_{U_i} ||\sigma_{U_i})$, and $LV' = h(ID_{U_i} ||RPW'_{U_i} ||TC'_{U_i} ||d_{U_i} ||\sigma_{U_i})$, and checks the condition $LV' = LV$. If it holds, U_i is a genuine user; otherwise, the login phase is halted immediately.

LGU3: MD_{U_i} generates a current timestamp T_1 and a random secret $r_{U_i} \in Z_p^*$ to calculate $M_1 = h(r_{U_i} ||T_1) \oplus h(RID_{TA}$ $||RID_{U_i} ||d_{U_i} \cdot Q_{CS_j} ||T_1), MM_1 = h(h(r_{U_i} ||T_1) ||TC_{U_i}||$ $T_1|| RID_{U_i} ||RID_{TA}) \oplus h(h(r_{U_i} ||T_1)|| RID_{TA} ||T_1), M_{U_i}$ $= h(RID_{U_i} ||RID_{TA}), M_2 = M_{U_i} \cdot P$ and the ElGamal type signature $M_3 = M_{U_i} + h(r_{U_i} ||T_1).d_{U_i} \pmod p$. MD_{U_i} then picks an accessed smart device SD_k with its pseudoidentity RID_{SD_k} and sends the login message $Msg_1 = \{TID_{U_i}$, $RID_{SD_k}, M_1, MM_1, M_2, M_3, T_1\}$ to CS_j via open channel.

C. User Authentication and Key Agreement Phase

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

AKM1: After receiving Msg_1 from U_i, CS_j 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 Msg_1. If it matches, CS_j searches for the same TID_{U_i} in its database and fetches corresponding RID_{U_i} from its database. CS_j further calculates $h(r_{U_i} ||T_1) = M_1 \oplus h(RID_{TA} ||RID_{U_i} ||d_{CS_j} \cdot Q_{U_i}$ $||T_1), M_{U_i} = h(RID_{U_i} ||RID_{TA})$ and checks if $M_3 \cdot P = M_2$ $+ h(r_{U_i} ||T_1) \cdot Q_{U_i}$. If CS_j finds this condition true, U_i is authenticated by CS_j.

AKM2: CS_j generates a current timestamp T_2 and a random secret $r_{CS_j} \in Z_p^*$ to compute $M_4 = h(r_{CS_j} ||T_2 ||RID_{CS_j}) \oplus$ $h(RID_{SD_k} ||d_{CS_j} \cdot Q_{SD_k} ||T_2), MM_2 = MM_1 \oplus h(h(r_{U_i}$ $||T_1)|| RID_{TA} ||T_1) \oplus h(h(r_{CS_j} ||T_2 ||RID_{CS_j})|| T_2||$ $RID_{SD_k}), M_{CS_j} = h(RID_{SD_k} ||T_2), M_5 = M_{CS_j} \cdot P$ and the ElGamal type signature $M_6 = M_{CS_j} + h(r_{CS_j} ||T_2||$ $RID_{CS_j}) \cdot d_{CS_j} \pmod p$. CS_j further generates a new random temporary identity $TID^{\text{new}}_{U_i}$ for U_i and computes M_T $= TID^{\text{new}}_{U_i} \oplus h(h(r_{U_i}||T_1)||RID_{TA}||T_2)$. CS_j then sends the message $Msg_2 = \{RID_{SD_k}, M_4, MM_2, M_5, M_6, M_T, T_1, T_2\}$ to SD_k via open channel.

AKM3: After receiving Msg_2 from CS_j, SD_k 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 Msg_2. If it is valid, SD_k computes $h(r_{CS_j} ||T_2 ||RID_{CS_j}) = M_4 \oplus h(RID_{SD_k} ||d_{SD_k} \cdot$ $Q_{CS_j} ||T_2), h(h(r_{U_i} ||T_1) ||TC_{U_i}|| T_1|| RID_{U_i} ||RID_{TA})$ $= MM_2 \oplus h(h(r_{U_i} ||T_1)|| RID_{TA} ||T_1) \oplus h(h(r_{U_i} ||T_1)||$ $RID_{TA} ||T_1) \oplus h(h(r_{CS_j} ||T_2 ||RID_{CS_j})|| T_2|| RID_{SD_k})$, $M_{CS_j} = h(RID_{SD_k} ||T_2), M_6 \cdot P = M_{CS_j} \cdot P + (h(r_{CS_j}$ $||T_2|| RID_{CS_j}).d_{CS_j}) \cdot P = M_5 + h(r_{CS_j} ||T_2|| RID_{CS_j}) \cdot$

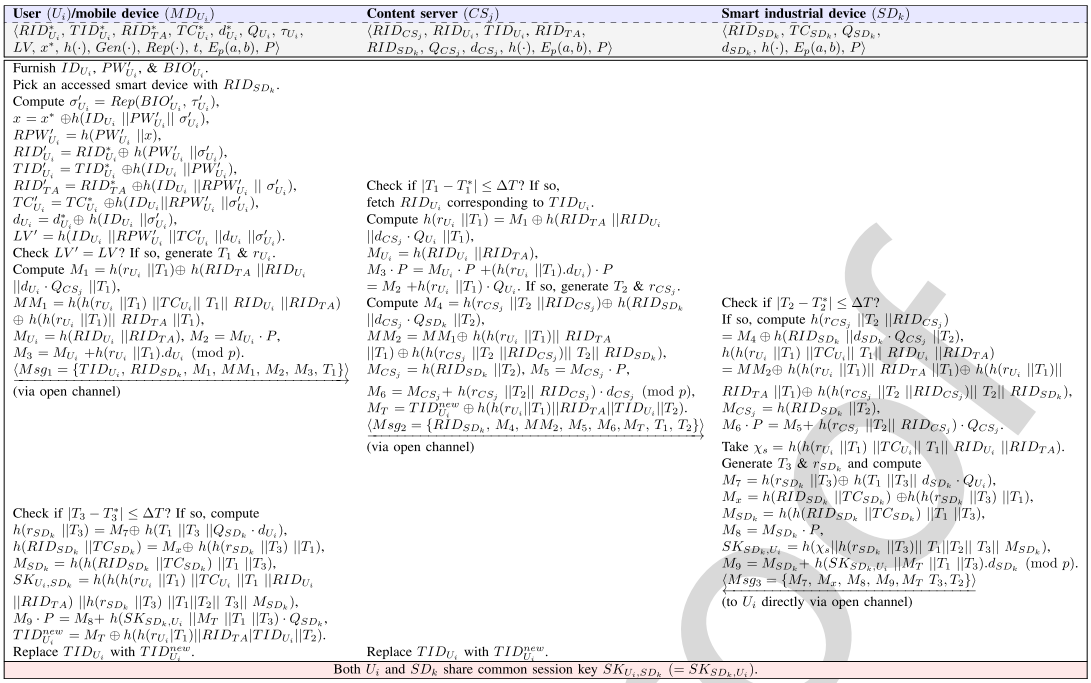

Fig. 3. Login and authentication, and key agreement phases.

Q_{CS_j}. If SD_k finds this condition true, CS_j is authenticated by SD_k, and SD_k sets $\chi_s = h(h(r_{U_i} ||T_1) ||TC_{U_i}|| T_1|| RID_{U_i} ||RID_{TA})$.

AKM4: SD_k generates a current timestamp T_3 and a random secret $r_{SD_k} \in Z_p^*$ to calculate $M_7 = h(r_{SD_k} ||T_3) \oplus h(T_1 ||T_3|| d_{SD_k} \cdot Q_{U_i})$, $M_x = h(RID_{SD_k} ||TC_{SD_k}) \oplus h(h(r_{SD_k} ||T_3) ||T_1)$, $M_{SD_k} = h(h(RID_{SD_k} ||TC_{SD_k}) ||T_1 ||T_3)$ and $M_8 = M_{SD_k} \cdot P$, session key $SK_{SD_k,U_i} = h(\chi_s||h(r_{SD_k} ||T_3)|| T_1||T_2|| T_3|| M_{SD_k})$, and generates the ElGamal type signature $M_9 = M_{SD_k} + h(SK_{SD_k,U_i} ||M_T ||T_1 ||T_3).d_{SD_k} \pmod p$. SD_k then sends the message $Msg_3 = \{M_7, M_x, M_8, M_9, M_T\ T_3, T_2\}$ to U_i through the open channel.

AKM5: After receiving Msg_3 from SD_k, after successful verification of the timeliness of T_3, U_i computes $h(r_{SD_k} ||T_3) = M_7 \oplus h(T_1 ||T_3 ||Q_{SD_k} \cdot d_{U_i})$, $h(RID_{SD_k} ||TC_{SD_k}) = M_x \oplus h(h(r_{SD_k} ||T_3) ||T_1)$, $M_{SD_k} = h(h(RID_{SD_k} ||TC_{SD_k}) ||T_1 ||T_3)$ and session key $SK_{U_i,SD_k} = h(h(h(r_{U_i} ||T_1) ||TC_{U_i} ||T_1 ||RID_{U_i} ||RID_{TA}) ||h(r_{SD_k} ||T_3) ||T_1||T_2|| T_3|| M_{SD_k})$, $M_9 \cdot P = M_8 + h(SK_{U_i,SD_k} ||M_T ||T_1 ||T_3) \cdot Q_{SD_k}$. If this condition holds true, SD_k is genuine; otherwise, U_i immediately aborts the process. U_i also computes $TID^{\text{new}}_{U_i} = M_T \oplus h(h(r_{U_i}||T_1)||RID_{TA}||T_2)$. In addition, MD_{U_i} of U_i and CS_j replace TID_{U_i} with $TID^{\text{new}}_{U_i}$ in their memory and database which will be used in the upcoming sessions.

Overall, the "login and authentication, and key establishment phases" is also provided in Fig. 3.

D. User Password and Biometric Update Phase

In this phase, a legitimate user can update his/her password and biometric information at any time without involving TA. The following steps need to be executed.

PBU1: U_i furnishes his/her identity ID_{U_i} and his/her old password $PW^o_{U_i}$, and old biometrics information $BIO^o_{U_i}$ at the sensor of the MD_{U_i}. After that MD_i applies the steps LGU1 and LGU2 to check if the user U_i is a genuine user to proceed for the password and biometric update process; otherwise, the process is halted immediately.

PBU2: U_i chooses his/her new password $PW^n_{U_i}$ and also provide new biometric data $BIO^n_{U_i}$ to the biometric sensor of his/her mobile device MD_{U_i} to compute $(\sigma^n_{U_i}, \tau^n_{U_i}) = Gen(BIO^n_{U_i})$, where $\sigma^n_{U_i}$ and $\tau^n_{U_i}$ are the biometric secret key of l bits and public reproduction parameter, respectively. U_i also computes $RPW^n_{U_i} = h(PW^n_{U_i} ||x)$, $x^n = x \oplus h(ID_{U_i} ||PW^n_{U_i}|| \sigma^n_{U_i})$, $RID^n_{U_i} = RID_{U_i} \oplus h(PW^n_{U_i} ||\sigma^n_{U_i})$, $TID^n_{U_i} = TID_{U_i} \oplus h(ID_{U_i} ||PW^n_{U_i})$, $RID^n_{TA} = RID_{TA} \oplus h(ID_{U_i} ||RPW^n_{U_i} || \sigma^n_{U_i})$, $TC^n_{U_i} = TC_{U_i} \oplus h(ID_{U_i}||RPW^n_{U_i} ||\sigma^n_{U_i})$, $d^n_{U_i} = d_{U_i} \oplus h(ID_{U_i} ||\sigma^n_{U_i})$ and $LV^n = h(ID_{U_i} ||RPW^n_{U_i} ||TC_{U_i} ||d_{U_i} ||\sigma^n_{U_i})$. The values of $RID^*_{U_i}$, $TID^*_{U_i}$, RID^*_{TA}, $TC^*_{U_i}$, $d^*_{U_i}$, τ_{U_i}, LV and x^* will be replaced by $RID^n_{U_i}$, $TID^n_{U_i}$, RID^n_{TA}, $TC^n_{U_i}$, $d^n_{U_i}$, $\tau^n_{U_i}$, LV^n and x^n.

PBU3: Finally, $\{RID^n_{U_i}, TID^n_{U_i}, RID^n_{TA}, TC^n_{U_i}, d^n_{U_i}, Q_{U_i}, \tau^n_{U_i}, LV^n, x^n, h(\cdot), Gen(\cdot), Rep(\cdot), t, E_p(a,b), P\}$ are stored in the memory of MD_{U_i}. Note that $x, ID_{U_i}, RPW_{U_i}, RID_{U_i}, TID_{U_i}, RID_{TA}, TC_{U_i}$ and d_{U_i} are deleted from the memory of MD_{U_i} to protect against stolen verifier, privileged insider attack, unauthorised session key computation, illegal user's password guessing and user impersonation attacks.

The user password and biometric update phase is also summarized in Fig. 4.

E. Dynamic Smart Industrial Device Addition Phase

Suppose a smart industrial device is lost/stolen or failed due to some reasons (e.g., battery power exhaustion). In that case, we

User (U_i)	**User mobile device** MD_{U_i}
Input identity ID_{U_i}, old password $PW^o_{U_i}$. Imprint old biometrics $BIO^o_{U_i}$.	Verify $PW^o_{U_i}$ and $BIO^o_{U_i}$ using the steps LGU1 and LGU2. If both are valid, the user U_i is genuine. Ask U_i for new password/biometrics.
Input new password $PW^n_{U_i}$. Imprint new biometrics $BIO^n_{U_i}$.	Compute $(\sigma^n_{U_i}, \tau^n_{U_i}) = Gen(BIO^n_{U_i})$, $RPW^n_{U_i} = h(PW^n_{U_i} \|\|x)$, $x^n = x \oplus h(ID_{U_i} \|\|PW^n_{U_i}\|\| \sigma^n_{U_i})$, $RID^n_{U_i} = RID_{U_i} \oplus h(PW^n_{U_i} \|\|\sigma^n_{U_i})$, $TID^n_{U_i} = TID_{U_i} \oplus h(ID_{U_i} \|\|PW^n_{U_i})$, $RID^n_{TA} = RID_{TA} \oplus h(ID_{U_i}$ $\|\|RPW^n_{U_i} \|\| \sigma^n_{U_i})$, $TC^n_{U_i} = TC_{U_i} \oplus h(ID_{U_i}\|\|RPW^n_{U_i} \|\|\sigma^n_{U_i})$, $d^n_{U_i} = d_{U_i} \oplus h(ID_{U_i} \|\|\sigma^n_{U_i})$, $LV^n = h(ID_{U_i} \|\|RPW^n_{U_i} \|\|TC_{U_i}$ $\|\|d_{U_i} \|\|\sigma^n_{U_i})$. Replace $RID^*_{U_i}$, $TID^*_{U_i}$, RID^*_{TA}, $TC^*_{U_i}$, $d^*_{U_i}$, τ_{U_i}, LV and x^* by $RID^n_{U_i}$, $TID^n_{U_i}$, RID^n_{TA}, $TC^n_{U_i}$, $d^n_{U_i}$, $\tau^n_{U_i}$, LV^n and x^n, respectively, in MD_{U_i}.

Fig. 4. User password/biometric update phase of UAKMS-NIB.

need to deploy new smart industrial devices SD^{new}_k after initial deployment. This process is executed with the help of TA using the following steps.

DSD1: The TA chooses a unique identity $ID^{\text{new}}_{SD_k}$ and a random secret $d^{\text{new}}_{SD_k} \in Z^*_p$ for smart device SD^{new}_k. The TA uses its own random secret key d_{TA} to compute the pseudoidentity of SD^{new}_k as $RID^{\text{new}}_{SD_k} = h(ID^{\text{new}}_{SD_k} \|\|d_{TA})$, public key $Q^{\text{new}}_{SD_k} = d^{\text{new}}_{SD_k} \cdot P$ and temporal credential as $TC^{\text{new}}_{SD_k} = h(d^{\text{new}}_{SD_k} \|\|ID^{\text{new}}_{SD_k} \|\|RTS^{\text{new}}_{SD_k} \|\|d_{TA})$, where $RTS^{\text{new}}_{SD_k}$ is the registration timestamp of SD^{new}_k.

DSD2: The credentials $\{RID^{\text{new}}_{SD_k}, TC^{\text{new}}_{SD_k}, Q^{\text{new}}_{SD_k}, d^{\text{new}}_{SD_k}, h(\cdot), E_p(a,b), P\}$ are then loaded in the memory of SD^{new}_k prior to deployment. $Q^{\text{new}}_{SD_k}$ is published publicly to other network entities, and the TA also sends $RID^{\text{new}}_{SD_k}$ to CS_j securely for further processing.

V. Security Analysis

In this section, we show that UAKMS-NIB can resist the following potential attacks that are crucial for 6G-enabled NIB deployed for industrial applications.

1) Replay Attack: In UAKMS-NIB, the exchanged messages Msg_1, Msg_2, Msg_3, and Msg_4 use the freshly generated timestamps T_1, T_2, and T_3. When an entity receives a message, it verifies the condition: $|T_x - T^*_x| \leq \Delta T$, $x = 1, 2, 3$ on the timeliness check. If this condition holds, the replay attack is detected by the receiving end.

2) Man-in-the-Middle Attack: Suppose an adversary $\mathcal{A}$ tries to update the messages exchanged among the communicating parties. For instance, $Msg_1 = \{TID_{U_i}, RID_{SD_k}, M_1, MM_1, M_2, M_3, T_1\}$ between U_i and CS_j. To modify Msg_1, $\mathcal{A}$ has to generate current timestamp T^a_1 and random secret $r^a_{U_i} \in Z^*_p$ to compute $M^a_1 = h(r^a_{U_i} \|\|T^a_1) \oplus h(RID_{TA} \|\|RID_{U_i} \|\|d_{U_i} \cdot Q_{CS_j} \|\|T^a_1)$, $MM^a_1 = h(h(r^a_{U_i} \|\|T^a_1) \|\|TC_{U_i}\|\| T^a_1\|\| RID_{U_i} \|\|RID_{TA}) \oplus h(h(r^a_{U_i} \|\|T^a_1)\|\| RID_{TA} \|\|T^a_1)$, $M^a_{U_i} = h(RID_{U_i} \|\|RID_{TA})$, $M^a_2 = M_{U_i} \cdot P$, and $M^a_3 = M^a_{U_i} + h(r^a_{U_i} \|\|T^a_1).d_{U_i} \pmod p$. However, $\mathcal{A}$ can not succeed in completing Msg_1 as he/she does not have the knowledge of secret values $(TC_{U_i}, TC_{U_i}, RID_{U_i}, RID_{TA}, RPW_{U_i}, x, d_{TA}, d_{U_i})$. Moreover, computing secret (private) keys from the public keys is also "computationally infeasible due to the ECDLP." Similar situation will arise for other messages Msg_2 and Msg_3. Hence, man-in-the-middle attack is resisted in UAKMS-NIB.

3) Impersonation Attacks: Suppose an adversary $\mathcal{A}$ tries to create a valid login message on behalf of a registered user U_i. To create a genuine login message Msg_1, $\mathcal{A}$ has to generate current timestamp T^a_1 and random secret $r^a_{U_i}$ on behalf of U_i. However, $\mathcal{A}$ will stuck in computing $M^a_1 = h(r^a_{U_i} \|\|T^a_1) \oplus h(RID_{TA} \|\|RID_{U_i} \|\|d_{U_i} \cdot Q_{CS_j} \|\|T^a_1)$, $MM^a_1 = h(h(r^a_{U_i} \|\|T^a_1) \|\|TC_{U_i}\|\| T^a_1\|\| RID_{U_i} \|\|RID_{TA}) \oplus h(h(r^a_{U_i} \|\|T^a_1)\|\| RID_{TA} \|\|T^a_1)$, $M^a_{U_i} = h(RID_{U_i} \|\|RID_{TA})$, $M^a_2 = M_{U_i} \cdot P$, and $M^a_3 = M^a_{U_i} + h(r^a_{U_i} \|\|T^a_1).d_{U_i} \pmod p$, because the essential secrets are not available. Therefore, $\mathcal{A}$ is not able to create the original login request message Msg_1 on behalf of U_i. Thus, $\mathcal{A}$ can not have ability to impersonate a genuine user. In the similar way, UAKMS-NIB also protects against content server and smart industrial device impersonation attacks.

4) Privileged-Insider and Stolen User Mobile Device Attacks: A privileged insider user of the TA, being an internal attacker, say $\mathcal{A}$, may know the registration information of a registered user U_i. However, $\mathcal{A}$ is not able to compute the session key $SK_{U_i,SD_k} = h(h(h(r_{U_i} \|\|T_1) \|\|TC_{U_i} \|\|T_1 \|\|RID_{U_i} \|\|RID_{TA}) \|\|h(r_{SD_k} \|\|T_3) \|\|T_1\|\|T_2\|\| T_3\|\| M_{SD_k})$, where $TC_{U_i} = h(TC_{U_i}\|\|x\|\| \sigma_{U_i})$ as he/she does not have any information about user's secret number x, password PW_{U_i} and secret biometric key σ_{U_i} even if he/she has the lost/stolen user's mobile device MD_{U_i}. This is because we have not stored any secret values directly in the memory of MD_{U_i}. In the similar way, $\mathcal{A}$ does not have the ability to compute/derive the password/biometric key of the user U_i through offline guessing attacks.

5) Ephemeral Secret Leakage (ESL) Attack: In UAKMS-NIB, the session key computed by a smart industrial device (SD_k) shared with the user U_i is $SK_{SD_k,U_i} = h(\chi_s\|h(r_{SD_k} \|\|T_3)\|\| T_1\|\|T_2\|\| T_3\|\| M_{SD_k})$, where $M_{SD_k} = h(h(RID_{SD_k} \|\|TC_{SD_k}) \|\|T_1 \|\|T_3)$. Similarly, the same session key computed by U_i shared with SD_k is $SK_{U_i,SD_k} = h(h(h(r_{U_i} \|\|T_1) \|\|TC_{U_i} \|\|T_1 \|\|RID_{U_i} \|\|RID_{TA}) \|\|h(r_{SD_k} \|\|T_3) \|\|T_1\|\|T_2\|\| T_3\|\| M_{SD_k})$ $(= SK_{SD_k,U_i})$. It is worth noticing that the session key SK_{SD_k,U_i} $(=SK_{SD_k,U_i})$ is based on both the short term (i.e, random secrets) and long term secrets (i.e., various identities and secret keys). In the following, we consider the following cases.

1) Case 1: If only the short term secrets (r_{U_i}, r_{SD_k}) are compromised through the session hijacking attacks, the session key SK_{SD_k,U_i} $(=SK_{SD_k,U_i})$ can not be compromised by an adversary $\mathcal{A}$ without having the long term secrets $(TC_{SD_k}, RID_{U_i}$, and $RID_{TA})$.
2) Case 2: If the long term secrets $(TC_{SD_k}, RID_{U_i}$ and $RID_{TA})$ are only compromised by the adversary $\mathcal{A}$, the session key SK_{SD_k,U_i} $(=SK_{SD_k,U_i})$ can not also be compromised without having the short term secrets (r_{U_i}, r_{SD_k}).

Thus, the session key SK_{SD_k,U_i} $(=SK_{SD_k,U_i})$ is only compromised when both the short term secrets and long term secrets

are compromised by the adversary $\mathcal{A}$. Therefore, in UAKMS-NIB $\mathcal{A}$ does not have ability to compute the session key on the behalf of the genuine network entities (U_i and SD_k). In addition, $\mathcal{A}$ can neither perform this attack through the user's stolen mobile device attack nor through the eavesdropped messages. Hence, UAKMS-NIB provides session key security. In other words, we can say that UAKMS-NIB is secured against "ESL attack under the considered CK-adversary model" as described in our threat model (see Section III-B).

6) Anonymity and Untraceability: Let an adversary $\mathcal{A}$ capture the messages Msg_1, Msg_2, and Msg_3 during the "login and authentication & key establishment phases" among U_i, CS_j, and SD_k. These messages are calculated using different "random nonces" and "current timestamps" that help to obtain dynamic and unique messages in different sessions. Moreover, we have not exchanged any user identity information in the "plaintext forms." Other exchanged messages are also created in the similar way. This method assisted us to attain both "user and content server anonymity and untraceability" properties in UAKMS-NIB.

7) Smart Industrial Device Physical Capture Attack: A smart device SD_k stores the credentials $\{RID_{SD_k}, TC_{SD_k}, Q_{SD_k}, d_{SD_k}, h(\cdot), E_p(a,b), P\}$ which are required for "authentication and key establishment" process with a user U_i. Suppose SD_k is physically captured by $\mathcal{A}$ and the stored information are extracted from SD_k's memory using the power analysis attacks [16]. Since RID_{SD_k}, TC_{SD_k}, Q_{SD_k}, and d_{SD_k} are different for all deployed smart devices, the revealing of these sensitive information does not affect the security among noncompromised smart devices and the user U_i. Therefore, UAKMS-NIB protects against "smart industrial device physical capture attack." In other words, UAKMS-NIB is "unconditionally secure against device physical capture attack."

VI. Formal Security Verification Using AVISPA: Simulation Study

This section provides the formal security verification of our proposed scheme (UAKMS-NIB) using one of the most used formal security software verification tools, known as "AVISPA" [8]. The main purpose of doing the formal security verification using AVISPA tool is to assure the safety of the proposed UAKMS-NIB against "replay" as well as "man-in-the-middle" attacks.

AVISPA has the following four back-ends: 1) "on-the-fly model-checker (OFMC);" 2) 'constraint logic based attack searcher (CL-AtSe);" 3) "SAT-based model-checker;" 4) "tree automata based on automatic approximations for the analysis of security protocols." To implement the proposed UAKMS-NIB, it needs to be written in the "high-level protocol specification language (HLPSL)." With the help of the HLPSL2IF translator, HLPSL code with extension (.hlpsl) is converted into the "Intermediate Format (IF)." The generated IF is then fed into one of the four available back-ends as input, and the "Output Format (OF)" is produced, which tells whether the tested scheme is "safe, unsafe, or inconclusive." In addition, the OF has a DETAILS section which provides an explanation supporting

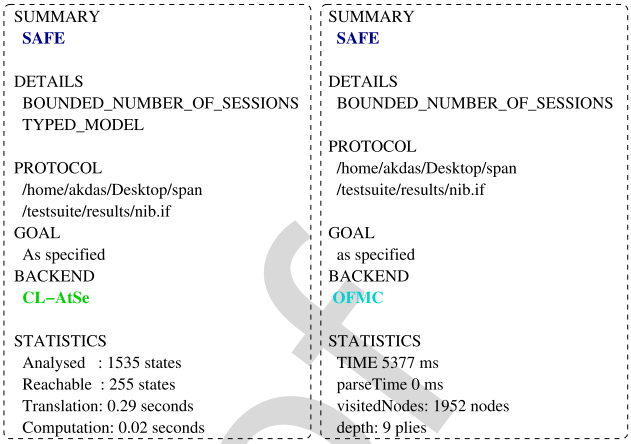

Fig. 5. Simulation results of UAKMS-NIB under CL-AtSe and OFMC backends.

the result displayed in the "SUMMARY" section, so as to why the protocol is safe or unsafe. The detailed description about AVISPA tool and HLPSL implementation are available in [8].

It is worth noticing that HLPSL is a role-oriented language. The HLPSL implementation of UAKMS-NIB involves four basic roles for the TA, a user (U_i), a content server (CS_j) and a smart industrial device (SD_k), and two mandatory roles of *session* and, *goal and environment*. The registration phase described in Section IV-A is implemented, which is performed through the secure channel. In addition, we have also done the HLPSL implementation of the user login phase described in Section IV-B and user authentication and key agreement phase explained in Section IV-C.

AVISPA implements the "DY threat model" [15]. Thus, an intruder (defined in HLPSL by i) cannot only intercept the messages but can also modify, delete or insert false messages during communication. The "Security Protocol ANimator for AVISPA (SPAN)" tool [19] is a broadly accepted tool which is used to perform formal security verification simulation. The simulation results of the proposed UAKMS-NIB illustrated in Fig. 5 clearly indicate that UAKMS-NIB is secured against replay and man-in-the-middle-attacks.

VII. Practical Perspective: NS2 Simulation

This section provides a simulation study of UAKMS-NIB using the "widely accepted network simulator, NS2 2.35" on "Ubuntu 18.04 LTS" platform. The purpose is to measure the impact of UAKMS-NIB on the important "network performance parameters, such as end-to-end delay (in seconds) and network throughput (in bps)".

Various simulation parameters used in the practical study are provided Table II. We have taken total 1800 s (30 min) as the simulation time. Both types of users (static and mobile) are considered in the simulation who move with different speeds ranging from 2 to 15 meters per second (mps). The remaining parameters are considered with standard values as used in NS2. We take 3, 5, and 8 users in "scenario-1," "scenario-2," and "scenario-3," respectively, and a single content server is

TABLE II
DIFFERENT PARAMETERS USED IN SIMULATION

Parameter	Value
Platform	Ubuntu 18.04 LTS
Considered scenarios	1, 2 and 3
Number of users (U_i)	3, 5, 8 for scenarios 1, 2, 3
Number of content servers (CS_j)	1 for all scenarios
Number of smart devices (SD_k)	50 for all scenarios
Mobility of users	2, 10, 15 mps, respectively
Simulation time	1800 seconds

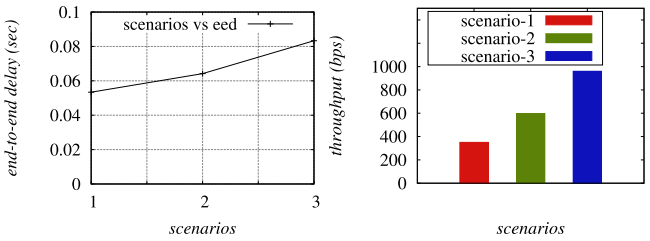

Fig. 6. Impact on (a) end-to-end delay and (b) throughput.

considered along with 50 smart industrial devices SD_k in all scenarios. The communication range of SD_k is taken as 50 m. The hash output (in case of use of "SHA-1 hash algorithm") and an "identity" are considered as 160 b and 160 b, conjointly. Three exchanged messages Msg_1 from U_i to CS_j, Msg_2 from CS_j to SD_k, and Msg_3 from SD_k to U_i need 1152 , 1184 , and 1024 b, conjointly.

A. Discussion on Results

The following outcomes are obtained during the simulation.

1) End-to-End Delay: The end-to-end delay (EED) is measured as the "average time taken by the messages to reach the destination node from a source node," which is defined as $\sum_{i=1}^{n_{pt}}(T_{R_i} - T_{S_i})/n_{pt}$, where "$T_{R_i}$ and T_{S_i} are the receiving and sending time of a packet i," conjointly, and n_{pt} denotes the "total number of packets." From Fig. 6, it is observed that the EED values for the scenarios 1, 2, and 3 are 0.05340, 0.06420, and 0.08333 s, conjointly. It is important to notice that the EED values increase as the number of users increases due to the reason that more users induce more exchanged messages which then increases congestion in the network.

2) Throughput: The network throughput is the "measurement of the number of bits transmitted per unit of time" that can be estimated as "$\frac{N_\rho \times |pt|}{T_\delta}$, where T_δ is the total time (in seconds), $|pt|$ is a packet size, and N_ρ is the total number of received packets." The throughput (in bps) of UAKMS-NIB in different considered scenarios presented in Fig. 6 shows that the throughput are 349.90, 596.11, and 959.82 bps for scenarios 1, 2, and 3, conjointly. The values of throughput also increase in case of "increment in the users," because in those cases "the number of messages exchanged also gets increased."

VIII. EXPERIMENTAL RESULTS USING MIRACL

In this section, we provide the experimental results for computational time needed for various cryptographic primitives using the widely used "MIRACL" [9]. MIRACL is a "C/C++ based programming software library that has been already recognized by the cryptographers as the gold standard open source SDK for elliptic curve cryptography (ECC)."

TABLE III
EXECUTION TIME FOR A SERVER OF CRYPTOGRAPHIC PRIMITIVES USING MIRACL

Primitive	Max. time (ms)	Min. time (ms)	Average time (ms)
T_h	0.149	0.024	0.055
T_{ecm}	2.998	0.284	0.674
T_{eca}	0.002	0.001	0.002
T_{se}	0.003	0.001	0.001
T_{sd}	0.002	0.001	0.001

TABLE IV
EXECUTION TIME UNDER RASPBERRY PI 3 SETTING FOR CRYPTOGRAPHIC PRIMITIVES USING MIRACL

Primitive	Max. time (ms)	Min. time (ms)	Average time (ms)
T_h	0.643	0.274	0.309
T_{ecm}	4.532	2.206	2.288
T_{eca}	0.021	0.015	0.016
T_{se}	0.038	0.017	0.018
T_{sd}	0.054	0.009	0.014

The symbols T_{ecm}, T_{eca}, T_{se}/T_{sd}, and T_h are used to represent the computational time needed to execute "elliptic curve point (scalar) multiplication," "elliptic curve point addition," "symmetric key [Advanced Encryption Standard (AES-128)] encryption/decryption," and "one-way hash function," respectively. The elliptic curve point addition and multiplication are performed on a nonsingular elliptic curve of the form: "$y^2 = x^3 + ax + b \pmod p$" such that $4a^3 + 27b^2 \neq 0 \pmod p$.

In the following, we consider the following two types of scenarios for MIRACL.

1) Scenario 1: The first scenario involves the platform for MIRACL using the setup: "Ubuntu 18.04.4 LTS, with memory: 7.7 GiB, processor: Intel Core i7-8565U CPU @ 1.80GHz × 8, OS type: 64-b and disk: 966.1 GB." The experiments for each cryptographic primitive are executed for 100 runs. From these runs, we have computed the maximum, minimum and average run-time in milliseconds for each cryptographic primitive. The experimental results are shown in Table III.
2) Scenario 2: The second scenario involves the testbed platform which is considered for MIRACL under the setting: "Model: Raspberry PI 3 B+ Rev 1.3, with CPU: 64-b, Processor: 1.4 GHz Quad-core, 4 cores, Memory (RAM): 1GB, and OS: Ubuntu 20.04 LTS, 64-bit.". The experiments are executed for each cryptographic primitive for 100 runs. From these runs, we have also calculated the maximum, minimum and average run-time in milliseconds for each cryptographic primitive. The experimental results are then tabulated in Table IV.

IX. COMPARATIVE ANALYSIS

This section provides a comparative analysis of UAKMS-NIB with other existing ECC-based user authentication schemes designed by Chang and Le [20], and Sadhukhan *et al.* [21].

For communication costs comparison, an identity (temporary/pseudo), a random secret (nonce), a current timestamp, an

TABLE V
COMMUNICATION COST COMPARISON

Scheme/ Cost (in bits)	User	Server	Smart device	Total cost (in bits)
Chang and Le [20]	672	512	1216	2400
Sadhukhan *et al.* [21]	704	1344	2204	4252
UAKMS-NIB	1152	1184	1024	3360

TABLE VI
COMPUTATION COSTS COMPARISON

Scheme/Cost	User	Server	Smart device
Chang and Le [20]	$2T_{ecm} + 7T_h$ ≈ 6.739 ms	$9T_h$ ≈ 0.495 ms	$2T_{ecm} + 5T_h$ ≈ 6.121 ms
Sadhukhan *et al.* [21]	$2T_h + 2T_{se}/T_{sd}$ $+T_{ecm}$ ≈ 2.938 ms	$T_h + 2T_{se}/T_{sd}$ $+T_{ecm}$ ≈ 0.786 ms	$2T_h + 4T_{se}/T_{sd}$ ≈ 0.682 ms
UAKMS-NIB	$T_{fe} + 19T_h +$ $T_{eca} + 4T_{ecm}$ ≈ 17.327 ms	$T_h + 5T_{ecm}$ $+T_{eca}$ ≈ 3.427 ms	$12T_h + 4T_{ecm}$ $+T_{eca}$ ≈ 12.876 ms

TABLE VII
SECURITY AND FUNCTIONALITY FEATURES COMPARISON

Feature	Chang and Le [20]	Sadhukhan *et al.* [21]	UAKMS-NIB
SF_1	✓	×	✓
SF_2	✓	×	✓
SF_3	×	✓	✓
SF_4	✓	×	✓
SF_5	✓	✓	✓
SF_6	✓	✓	✓
SF_7	✓	✓	✓
SF_8	✓	×	✓
SF_9	✓	✓	✓
SF_{10}	×	×	✓
SF_{11}	✓	✓	✓
SF_{12}	N/A	×	✓
SF_{13}	×	×	✓
SF_{14}	×	×	✓
SF_{15}	×	×	✓

SF_1 : "user anonymity;" SF_2 : "user untraceability;" SF_3 : "offline guessing attacks;" SF_4 : "fast wrong input detection;" SF_5 : "mutual authentication and session key agreement;" SF_6 : "impersonation attacks;" SF_7 : "privileged-insider attack;" SF_8 : "replay attack;" SF_9 : "man-in-the-middle attack;" SF_{10} : "stolen smart card/mobile device attack;" SF_{10} : "ESL attack under CK-adversary model;" SF_{11} : "smart device physical capture attack;" SF_{12} : "Denial-of-service (DoS) attack under biometric verification;" SF_{13} : "offline smart device registration phase;" SF_{14} : "freely and locally password/biometric changing facility;" SF_{15} : "dynamic smart device addition;" ✓: "a scheme is secure or supports a functionality feature;" × "a scheme is insecure or does not support a feature;" N/A: "not applicable."

"elliptic curve point," and a "hash output (digest) using SHA-1 hash algorithm" are taken as 160, 160, 32, 320, and 160 b, respectively. It is assumed that the security level of an 1024-b "RSA public key cryptosystem" is same as that for an 160-b "ECC public key cryptosystem." Under these assumptions, the communications costs for a user, a server and an IoT smart device along with total cost among UAKMS-NIB and other schemes are listed in Table V. It is seen that UAKMS-NIB requires less cost as compared to the scheme of Sadhukhan *et al.* [21]. Although the cost of UAKMS-NIB is little bit high as compared to Chang and Le's ECC-based scheme [20], UAKMS-NIB is superior while the "security and functionality features" are compared to the scheme [20] in Table VII. However, for a smart device communication cost point of view, UAKMS-NIB requires less communication cost as compared to other schemes.

For computation costs comparison, T_{ecm}, T_{eca}, T_h, T_{se}/T_{sd}, and T_{fe} are the symbols to denote the time required for an "ECC point multiplication," an "ECC point addition," a "hash operation," a "symmetric encryption/decryption," and a "fuzzy extractor operation (Gen/Rep)." We neglect the bitwise XOR operation as it is negligible as compared to other operations. We consider the experiments on the cryptographic primitives using the widely-accepted MIRACL [9] as demonstrated in Section VIII. We use the average computational time for various cryptographic primitives listed in Table III for a server as it is computationally resource-rich than that for a user's mobile device or a smart device, whereas the average computational time for various cryptographic primitives listed in Table IV are used for the user's mobile device or the smart device. Thus, under a server setting, we have $T_{ecm} \approx 0.674$ ms, $T_{eca} \approx 0.002$ ms, $T_h \approx 0.055$ ms, $T_{fe} \approx T_{ecm}$ [22], which is 0.674 ms, $T_{se} \approx 0.001$ ms, and $T_{sd} \approx 0.001$ ms. On the other side, under user's mobile device or smart device using Raspberry PI 3 setting, we have $T_{ecm} \approx 2.288$ ms, $T_{eca} \approx 0.016$ ms, $T_h \approx 0.309$ ms, $T_{fe} \approx T_{ecm} \approx 2.288$ ms, $T_{se} \approx 0.018$ ms, and $T_{sd} \approx 0.014$ ms. The comparative study on computational costs among the considered schemes in Table VI shows that UAKMS-NIB requires little bit high cost as compared to other schemes. However, it is justified by considering the offered "security and functionality features" by the proposed UAKMS-NIB as compared with those for other schemes [20], [21].

Finally, in Table VII, possible essential "security and functionality features (SF_1–SF_{15})" are compared among UAKMS-NIB and other competing schemes. It is observed that UAKMS-NIB is superior in terms of the features (SF_1–SF_{15}) as compared to other schemes.

X. CONCLUSION

In this article, we attempted to solve an important security service by means of designing a new authentication protocol in "6G-enabled NIB deployed industrial applications." The proposed UAKMS-NIB allowed a legal registered user to access the service (real time data) from a smart device with the help of content server provided a successful mutual authentication between the user and smart device occurs. The robustness of the proposed UAKMS-NIB had been shown through the security analysis. NS2-based simulation study had been conducted to show the impact of UAKMS-NIB for various network performance parameters. Finally, a detailed comparative study revealed that the superiority of UAKMS-NIB in terms of "security and functionality requirements," "communication," and "computational" overheads. Therefore, we concluded that UAKMS-NIB was practical for 6G-enabled NIB deployed industrial applications.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable feedback on the article, which helped to improve its quality and presentation.

REFERENCES

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

[2] 3G4G, *Beginners: Network in a Box (NIB)*. Accessed: Apr. 2020. [Online]. Available: https://www.slideshare.net/3G4GLtd/beginners-network-in-a-box-nib

[3] Artiza Networks, *System Architecture Evolution (SAE) and the Evolved Packet Core (EPC)*. Accessed: April 2020. [Online]. Available: https://www.artizanetworks.com/resources/tutorials/sae_tec.html

[4] Tecore Networks, *Network in A Box Rapidly Deployable Communications*. Accessed: April 2020. [Online]. Available: https://www.tecore.com/network-in-a-box-products/

[5] J. Huang and Y. Lien, "Challenges of emergency communication network for disaster response," in *Proc. IEEE Int. Conf. Commun. Syst.*, Singapore, 2012, pp. 528–532.

[6] 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.*, Wuhan, China, 2011, pp. 1–4.

[7] Communications Today, *5G And 6G Wireless Technologies Have Security Issues*. Accessed: April 2020. [Online]. Available: https://www.communicationstoday.co.in/5g-and-6g-wireless-technologies-have-security-issues/

[8] "Automated Validation of Internet Security Protocols and Applications," (2019). Accessed: March 2020. [Online]. Available: http://www.avispa-project.org/

[9] *MIRACL Cryptographic SDK: Multiprecision Integer and Rational Arithmetic Cryptographic Library.* (2020). Accessed: June 2020. [Online]. Available: https://github.com/miracl/MIRACL

[10] 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.*, 2018, pp. 512–517.

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

[12] H. Viswanathan and P. E. Mogensen, "Communications in the 6G Era," *IEEE Access*, vol. 8, pp. 57 063–57 074, 2020.

[13] 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.

[14] 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.

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

[16] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Proc. 19th Annu. Int. Cryptology Conf., LNCS*, Santa Barbara, CA, USA, 1999, vol. 1666, pp. 388–397.

[17] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *International Conference on the Theory and Applications of Cryptographic Techniques– Advances in Cryptology (EUROCRYPT 2001)*. Innsbruck, Austria: Springer, 2001, pp. 453–474.

[18] 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*. New York, NY, USA: Springer-Verlag, 2017, pp. 79–99.

[19] *SPAN, the Security Protocol ANimator for AVISPA*, (2019). Accessed: Mar. 2020. [Online]. Available: http://www.avispa-project.org/

[20] 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.

[21] D. Sadhukhan, S. Ray, G. P. Biswas, M. K. Khan, and M. Dasgupta, "A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography," *J. Supercomput.*, 2020. [Online]. Available: https://doi.org/10.1007/s11227-020-03318-7

[22] 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 Secur.*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.

Mohammad Wazid (Senior Member, IEEE) received the M.Tech. degree in computer network engineering from Graphic Era University, Dehradun, India, and the Ph.D. degree in computer science and engineering from the International Institute of Information Technology, Hyderabad, India.

He is currently working as an Associate Professor with the Department of Computer Science and Engineering, Graphic Era University. He is the Head of the cybersecurity and IoT research group, Graphic Era University. He has authored or coauthored more than 70 papers in international journals and conferences in the areas of his research interests. His current research interests include security, remote user authentication, the Internet of Things (IoT), and cloud computing.

Ashok Kumar Das (Senior Member, IEEE) received the M.Sc. degree in mathematics, the M.Tech. degree in computer science and data processing, and the Ph.D. degree in computer science and engineering, from IIT Kharagpur, India.

He is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, IIIT, Hyderabad, India. He has authored over 235 papers in international journals and conferences in the areas of his research interests, including over 200 reputed journal papers. His current research interests include cryptography and network security including.

Dr. Das was the recipient of the Institute Silver Medal from IIT Kharagpur. He is on the editorial board of IEEE Systems Journal, *KSII Transactions on Internet and Information Systems*, *International Journal of Internet Technology and Secured Transactions (Inderscience)*, and *IET Communications*.

Neeraj Kumar (Senior Member, IEEE) received the Ph.D. degree in CSE from Shri Mata Vaishno Devi University, Katra, India.

He was a Postdoctoral Research Fellow with Coventry University, Coventry, U.K. He is working as an Associate Professor with the Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology (Deemed to be University), Patiala, India. He has published more than 450 technical research papers in leading journals and conferences from IEEE, Elsevier, Springer, John Wiley, etc.

Dr. Kumar is on the editorial board of *ACM Computing Survey*, IEEE Transactions on Sustainable Computing, *IEEE Network Magazine*, *IEEE Communication Magazine*, *Journal of Networks and Computer Applications* (Elsevier), and *Computer Communications* (Elsevier).

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

He is currently an Associate Professor with the College of Engineering, IT and Environment, Charles Darwin University, Casuarina NT, Australia. He is also a Cyber Security Researcher and a Practitioner with industry and academic experience. His research interests include multidisciplinary that focuses on cyber security and digital forensics of computer systems with a focus on cybercrime detection and prevention, including cyber terrorism and cyber warfare.