Designing Secure User Authentication Protocol for Big Data Collection in IoT-Based Intelligent Transportation System

Jangirala Srinivas, *Member, IEEE*, Ashok Kumar Das, *Senior Member, IEEE*, Mohammad Wazid, *Senior Member, IEEE*, and Athanasios V. Vasilakos, *Senior Member, IEEE*

***Abstract*—Secure access of the real-time data from the Internet-of-Things (IoT) smart devices (e.g., vehicles) by a legitimate external party (user) is an important security service for big data collection in the IoT-based intelligent transportation system (ITS). To deal with this important issue, we design a new three-factor user authentication scheme, called UAP-BCIoT, which relies on elliptic-curve cryptography (ECC). The mutual authentication between the user and an IoT device happens via the semitrusted cloud-gateway (CG) node in UAP-BCIoT. UAP-BCIoT supports several functionality features needed for IoT-based ITS environment including IoT smart device credential validation and big data analytics. A detailed security analysis is conducted based on the defined threat model to show that UAP-BCIoT is resilient against many known attacks. A thorough comparative study reveals that UAP-BCIoT supports better security, offers various functionality attributes, and also provides similar costs in communication as well computation as compared to other relevant schemes Finally, the practical demonstration of the proposed UAP-BCIoT is also provided to measure its impact on the network performance parameters.**

***Index Terms*—Automated validation of Internet security protocols and applications (AVISPA), formal security, Internet of Things (IoT)-based intelligent transportation system (ITS), key agreement, NS2 simulation study, secure big data collection, user authentication.**

I. Introduction

THE Internet of Things (IoT) brings a new era in computing which is formed using various networked objects, called smart devices. The smart devices are interconnected each other for gathering, processing, refining, and also exchanging important data over the public Internet. The devices can be assigned to IP addresses (IPv4 or IPv6) or even device identities. Due to the shortage of IPv4 addresses, IPv6 over low-power wireless personal-area networks (6LoWPAN) has drastically changed the IoT scenery by seeking to increase the use of IPv6 to smart as well as small-scaled objects [1]. These days, IoT is utilized in many environments and platforms. Along these lines, IoT has numerous potential applications, for example, smart homes, smart cities, smart traffic monitoring, smart health care, and intelligent transportation system (ITS). A cloud-based policy can be applied for storing the information collected by IoT devices (nodes) in a cloud-driven IoT-based big data deployment that can be further treated as a Big Data warehouse. Such a situation should be highly versatile and it ought to likewise give significant processing for the real-time events (for instance, surveillance & monitoring).

ITS is an emerging transportation structure that is incorporated an advanced information and communicate correspondences sort out for users, roads, and vehicles. ITS is the fused usage of pattern setting advancements using equipment, PCs, communications, and impelled sensors. These applications give voyagers huge information while improving the safety, security, and capability of the transportation system [2]. The data assembled by the nodes in the IoT-based ITS environment is of colossal volume. In any case, the imperatives of the relational database management system (RDBMS) [3] led to the inception of big data [4], [5].

The intelligent vehicle parking system [4] is one of the potential applications of ITS. The IoT sensing devices help in collecting different data with respect to the geographic area of the vehicles, accessibility of the parking area, earlier reservation details, parking position, insights about the vehicle and current traffic information, and so on. The generated data can be of colossal volume and huge. Thus, big data incorporates all the varieties of data, including structured data and unstructured data from e-mails, social media, text streams, and so on. This kind of data management requires companies to leverage both their structured and unstructured data. This necessitates for the big data that will play a major role in such situation as it incorporates the real-time application with the facility to render an intelligent system

Manuscript received September 29, 2020; revised November 21, 2020; accepted November 24, 2020. Date of publication November 26, 2020; date of current version April 23, 2021. This work was supported in part by the Mathematical Research Impact Centric Support Project Funded by the Science and Engineering Research Board, India, under Grant MTR/2019/000699, and in part by the Centre for Supply Chain and Logistics Management from O. P. Jindal Global University, India. *(Corresponding author: Ashok Kumar Das.)*

Jangirala Srinivas is with the Jindal Global Business School, O. P. Jindal Global University, Haryana 131001, India (e-mail: sjangirala@jgu.edu.in).

Ashok Kumar Das is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India (e-mail: iitkgp.akdas@gmail.com).

Mohammad Wazid is with the Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun 248 002, India (e-mail: wazidkec2005@gmail.com).

Athanasios V. Vasilakos is with the School of Electrical and Data Engineering, University of Technology Sydney, Ultimo NSW 2007, Australia, also with the Department of Computer Science and Technology, Fuzhou University, Fuzhou 350116, China, and also with the Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, 97187 Luleå, Sweden (e-mail: th.vasilakos@gmail.com).

Digital Object Identifier 10.1109/JIOT.2020.3040938

for transportation. Likewise, the intelligent vehicle parking system, there are several applications, such as smart traffic monitoring.

It is estimated that by 2020, there will be 250 million connected vehicles on the road, which represents 75% of the total vehicles [6]. In ITS, the connected cars exchange information of the sensors in the cars with other devices such as vehicle to vehicle (V2V). Meanwhile, the information is also exchanged between the connected cars from the roads and equipments in traffic facilities such as vehicle to roadside (V2R) and vehicle to infrastructure (V2I). Modern cars are equipped with numerous electronic control units, such as onboard diagnostic (OBD), in-vehicle infotainment (IVI), and telematics control unit (TCU). They communicate with each other over the vehicle Internet. Furthermore, thanks to the important elements, such as IVI, TCU, and OBD, drivers in the vehicles are seamlessly connected to the Internet [2], [5].

The advance methods, such as *sensing equipments* are installed onboard, where a control area network (CAN) gateway can extract the sensing information from the on-board sensors (e.g., direction, temperature, velocity, and airbag status), parking assistance radars, and rear and front cameras. Furthermore, a different set of characteristics is utilized in *communication equipment* to extract communication range, transmission power, bit rates and frequency bands. Basically, the communication is considered as two types based on their ranges: 1) short-range *ad hoc* communication and 2) long-range communication. The former communication is considered primarily to V2V and on the other side, the later communication is infrastructure-based primarily for V2I purposes only. However, for vehicle-to-cloud communication (V2C), the Internet connection is required. Similarly, an external user can access the real-time data of an installed IoT device in a vehicle through the Internet. The transportation system is based on four fundamental principles: 1) safety; 2) responsiveness; 3) integration; and 4) sustainability. This helps in achieving the main objectives of ITS, such as mobility, accessibility, safety, environmental sustainability, and economic development [4].

A. Motivation

There are serious issues on the safety protection at all critical end-point devices, and once broken to the hackers, vehicles may face hazards of malfunctions. There should be a secure communication design to restrict the hackers in creating hazards of malfunctions. Malicious parties can easily attack the vulnerable systems of the vehicles which may lead to loss or leakage of sensitive data. Hackers can also grasp the vehicle owner's private information for extortion or maliciously manipulate the vehicles functionality. In the era of IoT-based smart vehicles, the future of associated cybersecurity mechanisms rely on the secure communication design to ensure the security of the data transmission. In IoT-based smart vehicles, the accessibility of the real-time data has become extremely important as the users wish to access the desired IoT devices directly. In such sort of real-time information accessing, the legitimate external users can be permitted to get the information from the IoT devices. In addition, a legitimate user may also demand for big data query processing and big data analytics over the information stored in the cloud servers to make sense of hidden patterns of certain marvels (i.e., prediction of fire in an ITS environment). This demands for designing a secure authentication scheme for IoT-based ITS environment that will enable an enlisted legitimate user to get to the real-time data from an assigned IoT device directly in a secure way.

B. Research Contributions

The main contributions are highlighted as follows.

1) A new ECC-based three-factor user authentication scheme, called UAP-BCIoT, has been designed for big data collection in the IoT-based ITS environment. UAP-BCIoT achieves the mutual authentication among a user and an IoT device via the semitrusted cloud-gateway (CG). Furthermore, UAP-BCIoT supports various functionality attributes, such as supporting password/biometric update phase, dynamic IoT device addition phase, user mobile device revocation phase if the mobile device of an authorized registered user is stolen/lost. In addition, UAP-BCIoT also supports IoT node credential validation and big data analytics phases.
2) A detailed formal security analysis under the widely accepted real-or-random (ROR) model [7], informal (nonmathematical) security analysis and formal security verification based on simulation using the broadly applied automated validation of Internet security protocols and applications (AVISPA) tool [6] reveal that UAP-BCIoT can combat many known attacks that are relevant in an IoT-based ITS environment. The detailed comparative analysis reveals that UAP-BCIoT provides better tradeoff among security and functionality features, communication, as well computation costs with relevant existing schemes.
3) Finally, the practical demonstration of the proposed UAP-BCIoT is also provided to measure the impact on various network performance parameters.

C. Paper Outline

The outline of this article is as follows. While the related work is discussed in Section II, the network model and threat models of the proposed scheme (UAP-BCIoT) are provided in Section III. Different phases of UAP-BCIoT have been discussed in Section IV. A detailed formal as well as informal (nonmathematical) security analysis is presented in Section V. To further strengthen the security of UAP-BCIoT, the formal security verification using one of the widely accepted software verification tools, known as AVISPA has been carried out on UAP-BCIoT in Section VI. A comparative study on UAP-BCIoT and other relevant existing competing user authentication schemes is illustrated in Section VII. The practical demonstration of UAP-BCIoT using NS2 simulation study is also conducted in Section VIII. Finally, the concluding remarks are put in Section IX.

II. Related Work

In this section, we confine our discussion on related existing authentication schemes.

Das *et al.* [8] provided a taxonomy of various security protocols, such as "key management," "user and device authentication," "access control," "privacy preservation," and "identity management" protocols, which are needed for an IoT-based environment and emphasized that user authentication mechanism is one of the important security services in the IoT deployment. They presented several security requirements that are needed to design security protocols in the IoT deployment. They further highlighted several attacks associated with the IoT deployment, such as "replay," "man-in-the-middle," "stolen/lost smart card/mobile device," "privileged-insider," "impersonation," "password guessing," "password change," and "physical IoT smart devices capture" attacks. In addition, they also provided a threat model that can be considered for designing the security protocols in the IoT deployment. Wazid *et al.* [9] their review work also discussed about a scientific classification of different existing validation plans appropriate for a "cloud-driven IoT-based big data environment," which covers a near investigation of several user authentication schemes.

Turkanoviá *et al.* [10] suggested a "two-factor user authentication method" which is lightweight in computation and communication, and also applicable for the IoT environment. Unfortunately, their approach is vulnerable to various well-known attacks, including "privileged-insider," "off-line password guessing," "stolen smart card," and "user and smart device impersonation" attacks.

Porambage *et al.* [11] designed a mechanism for user authentication in the IoT deployment, which allows the end users to authenticate themselves to the IoT sensing nodes directly and access sensing information and services. Though this scheme is computationally efficient, it is vulnerable to several known attacks.

Porambage *et al.* [12] also proposed two schemes in IoT environment: 1) Scheme-1 is facilitated with the key derivation process to the legitimate users of the multicast group and 2) Scheme-2 deals with the shared secret key which is established among the entities in a multicast group.

Farash *et al.* [13] designed another lightweight two-factor user authentication mechanism for the IoT deployment. However, their mechanism is also vulnerable to several well-known attacks, such as "known session-specific temporary information," "offline password-guessing," "stolen/lost smart card," "new smart card issue," and "user-impersonation" attacks. In addition, their scheme also fails to preserve "user anonymity" goal.

Challa *et al.* [14] designed an "ECC-based user authentication technique" which is aimed for the future IoT applications, which depends on ECC-based digital signature. Though their scheme supports various functionality attributes, a noted observation is that their scheme requires high computation and communication costs for the involved entities in order to apply in the IoT environment.

Tai *et al.* [15] proposed a lightweight authentication scheme in the IoT deployment. Unfortunately, their mechanism is also found to have several vulnerabilities, such as "privileged-insider," "password guessing," "man-in-the-middle," and "replay" attacks. In addition, their scheme fails to achieve the "forward secrecy" property.

Wazid *et al.* [16] designed a "three-factor user authentication mechanism in the IoT deployment" using a legal registered user's smart card, password, and personal biometrics. Though their scheme has the ability to protect various well-known attacks, it does not support the revocability property where new credentials for the mobile device of a user are required in case the mobile device of that user is stolen/lost.

Li *et al.* [17] framed an industrial IoT environment using an ECC-based authentication mechanism. Furthermore, an important observation on their scheme is that it fails to ensure some of the functionality attributes (Section VII-A). In addition to this, due to the high-computation cost generated during the execution of the authentication mechanism, it is not suitable for the resource limited IoT sensing nodes.

Banerjee *et al.* [19] proposed a "three-factor user authentication mechanism" for generic IoT deployment. In their design, symmetric key encryption/decryption technique was used to establish the session key between a user and an IoT smart device. A "DeviceList" is used in their scheme, which needs to be updated each time when the login and authentication phase as well as password/biometric update phase are executed. However, their scheme does not provide the "big data analytics phase," and as a result, it may not be suitable for the big data collection and analysis in IoT-based ITS. In addition, no mechanism is provided to validate the credentials in IoT devices by the gateway nodes after the deployment of the IoT smart devices in the network.

Srinivas *et al.* [18] also designed a new authentication mechanism for a "wearable healthcare monitoring system" in which the Bigdata Registration Centre (BRC) is responsible for registering the Cloud of Things-centric (CoTC), users and wearable sensor devices. In their scheme, a session key is derived between a legal registered user and a wearable sensor device for the real-time sensor data access provided a mutual authentication is successful among them via the CoTC. Though the scheme in [18] provides several functionality features, its communication cost is more than that for our proposed scheme (UAP-BCIoT) in this article. Moreover, the scheme in [18] is a two-factor user authentication scheme where user password is used. On the other side, the proposed scheme (UAP-BCIoT) is a three-factor user authentication that applies user password and biometrics both, and it increases the security of user authentication locally by the user mobile device/smart card. It is also worth noticing that while the scheme in [18] is based on the computational integer factorization problem (IFP) in finding two large distinct prime factors p and q from a composite modulus $n = p \times q$, the proposed UAP-BCIoT relies on the computational elliptic-curve decisional Diffie–Hellman problem (ECDDHP). Therefore, to achieve the same level security, the proposed UAP-BCIoT works with smaller ECC-based key size as compared to larger RSA-based key size in the scheme [18]. In addition, the proposed UAP-BCIoT is based on the more recent Zipf's law [20] for the user-chosen passwords as compared to traditional uniform distributed dictionary for user-selected passwords.

TABLE I
SUMMARY OF CRYPTOGRAPHIC TECHNIQUES APPLIED AND LIMITATIONS OF PREVIOUS EXISTING USER AUTHENTICATION MECHANISMS

Scheme	Year	Cryptographic Techniques	Advantages	Drawbacks/Limitations
Turkanovic *et al.* [10]	2014	* Based on "two-factor (smart card and user password)" * Uses "one-way cryptographic hash function"	* Lightweight key agreement protocol * Fits in heterogeneous ad hoc wireless sensor networks, based on IoT	* Vulnerable to "privileged-insider, off-line password guessing, stolen mart card, user impersonation and smart device impersonation attacks" * No "formal security" analysis
Porambage *et al.* [11]	2014	* Based on "two-phase authentication" and " implicit certificate-based authentication" mechanism * Uses "ECC cryptographic technique"	* Applicable to wireless sensor networks (WSNs) in distributed IoT applications * It is lightweight and supports the heterogeneity of the entities	* Vulnerable to various attacks * Fails to preserve "user anonymity" * No "formal security" analysis
Porambage *et al.* [12]	2015	* Based on "group communications" * Applies "ECC digital signature"	* Supports broadcasting and multicasting * Applicable for "multicast communication in WSNs deployed for IoT applications"	* Vulnerable to various attacks * Fails to preserve "user anonymity" * No "formal security" analysis
Farash *et al.* [13]	2016	* Based on "two-factor (smart card and user password)" Uses "one-way cryptographic hash function"	* Lightweight key agreement protocol * Fits in heterogeneous ad hoc wireless sensor networks, based on IoT	* Vulnerable to "known session-specific temporary information, off-line password-guessing, stolen/lost smart card, new smart card issue, and user-impersonation attacks" * Fails to preserve "user anonymity" * Gateway node secret key is not protected * No "formal security" analysis
Challa *et al.* [14]	2017	* Based on "three-factor (smart card, user password & biometrics)" * Uses ECC with signature & "one-way cryptographic hash function"	* Applicable for IoT applications	* Though secure against various attacks, no "formal security" analysis * Needs more computation cost as compared to proposed UAP-BCIoT
Tai *et al.* [15]	2017	* Based on "two-factor (smart card & user password)" Uses "one-way cryptographic hash function"	* Applicable for IoT-enabled heterogeneous ad hoc wireless sensor networks	* Vulnerable to various known attacks. * No "formal security" analysis.
Wazid *et al.* [16]	2018	* Based on "three-factor (smart card, user password & biometrics)" Uses "one-way cryptographic hash function" * Based on "fuzzy extractor for biometric verification"	* Fits for generic IoT networking environment	* Fails to preserve "revocability" * No "formal security" analysis.
Li *et al.* [17]	2018	* Based on "three-factor (user mobile device, user password and personal biometrics" * Applies "ECC cryptographic technique" * Uses "fuzzy extractor for biometric verification"	* Applicable in industrial IoT environment	Does not support "revocability, and password/biometric update" Vulnerable to "known session key attack"
Srinivas *et al.* [18]	2018	* Based on "two-factor (smart card and user password) * Based on Chinese Remainder Theorem (CRT)-based public key concept * Uses "one-way hash function"	* Applicable for "wearable healthcare monitoring system"	* Works on larger key size as compared to the ECC-based key size used in UAP-BCIoT * Needs more communication cost as compared to UAP-BCIoT
Banerjee *et al.* [19]	2019	* Based on "three-factor (smart card, user password & personal biometrics) * Uses "symmetric key encryption/decryption" technique * Applies "fuzzy extractor for biometric verification"	* Applicable for general IoT deployment	* Big Data analytics phase is not supported. Thus, it may not be suitable for the Big Data collection and analysis in IoT-based intelligent transportation system * The "DeviceList" needs to be updated each time when the login and authentication phase,and password/biometric update phase are executed * Does not support device credentials update phase
Proposed (UAP-BCIoT)	2020	* Based on "three-factor (mobile device, user password & personal biometrics) * Uses "ECC cryptographic technique" * Applies "fuzzy extractor for biometric verification"	* Fits for "IoT-based intelligent transportation system" * Supports "revocability", "user anonymity", "untraceability" * Protects against various attacks including "known session key attack" * Provides "Big Data analytics" phase for secure storage and analysis of the Big Data * Supports "IoT device credential validation phase" to verify and detect the malicious behavior of the IoT nodes	* The security of the proposed UAP-BCIoT can be further improved by the deployment of blockchain based mechanism * Requires refinement for communication and computation overheads

Finally, a summary of various cryptographic techniques applied and limitations/drawbacks, as well as advantages of previously proposed user authentication protocols related to the IoT deployment is provided in Table I.

III. SYSTEM MODELS

In the designing of the proposed UAP-BCIoT, we use the following network and threat models.

A. Network Model

A network model for an IoT-based ITS [4] is provided in Fig. 1. The architecture consists of different types of entities, such as smart vehicles, roadside units (RSUs) (infrastructure), vehicle charging units, BRC, CG nodes (CG), and different types of users. The smart vehicles are installed with IoT devices [IoT nodes (IN)], which monitor various types of factors inside and outside of the vehicles. In this network model, there are different types of communications:

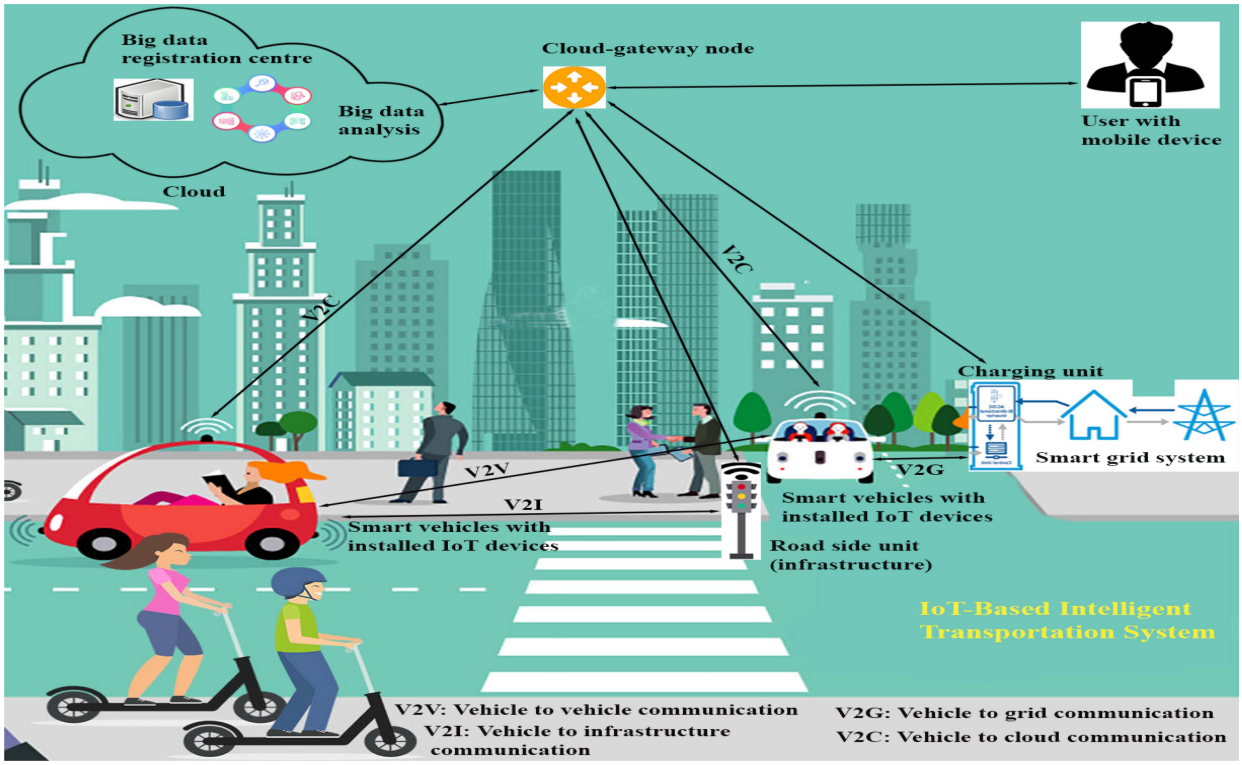


Fig. 1. Network model for the IoT-based intelligent transport system [4].

1) vehicle-to-vehicle communication (V2V); 2) vehicle-to-infrastructure communication (V2I); 3) vehicle-to-grid communication (V2G); and 4) vehicle-to-cloud communication (V2C). The authorized users can access the data of IoT nodes directly installed in smart vehicles through the CG node. The data of ITS is stored over the cloud to perform bigdata analysis, which is further helpful to draw useful conclusion from that. For example, prediction of road accident in a specific region on the basis of collected and analyzed data. The ITS structure is required to work with ultrahigh recurrent that will help in achieving the staggering division and recognize the information for around 4–6 m. In this model, an external party (user) (e.g., a traffic inspector) likes to retrieve real-time information from a smart vehicle (installed with IoT nodes) in a particular region. The user can have the list of the accessed registered vehicles in that particular region. To deal with this scenario, a user authentication mechanism is extremely required between the external party (user) and IoT nodes installed in the smart vehicles via the CG node, which serve as the gateway node. The secret credentials are loaded in the memory of IoT nodes that are installed in the smart vehicles through the trusted BRC. Also, each user has to register at the CG for retrieving real-time information from a particular IoT node in the IoT-based ITS environment. After the successful mutual authentication between a user and an IoT node through the CG, both entities generate and establish a session key for their secure communication in future. It is worth noticing that the proposed scheme (UAP-BCIoT) is also effective for V2V communication. For the secure V2V communication, the proposed authentication model can also be utilized. For that purpose, the registration of each vehicle will be done by the trusted authority (i.e., BRC) of the network. After the successful registration of each vehicle, the registration information of the vehicle can be stored in the on board memory unit of each vehicle. The preloaded information helps each vehicle to communicate with other vehicle in a secure way through the establishment of a computed session key.

B. Threat Model

The well-known "Dolev–Yao threat model (DY model)" [21] has been applied in the proposed UAP-BCIoT scheme. In the DY model, the participating entities communicate among each other via insecure channel, where the "end-point participants (e.g., vehicles and RSUs)" are not trusted. During the communication, an attacker $\mathcal{A}$ would then have the option to spy, alter, or delete the interchanged messages as they communicate over insecure channel. The trusted BRC is considered as a full-trusted entity, whereas the CG nodes are semitrusted. Moreover, since the IoT nodes cannot be monitored 24×7, some IoT nodes can be physically seized and it opens an opportunity to $\mathcal{A}$ to obtain the credentials stored in those seized IoT nodes using the "power analysis attacks" [22]. The CK-adversary model [23] is presently a *de facto* standard model under which $\mathcal{A}$ can convey information as in the DY model, and in addition, he/she can also compromise the secret credentials, such as "session keys, private keys and session state." Several attacks associated with the IoT-based ITS deployment need to be inspected while developing a user authentication protocol, such as "replay," "man-in-the-middle," "stolen/lost mobile device," "privileged-insider," "impersonation," ephemeral

TABLE II
NOTATIONS AND THEIR IMPORTANCE

Symbol	Significance
BRC, MK_{BRC}	Trusted Bigdata Registration Center and its master key
CG_k, ID_{CG_k}	k^{th} semi-trusted Cloud-Gateway and its identity
X_{CG_k}	Secret key of CG_k
IN_j, ID_{IN_j}	j^{th} IoT node (smart device) and its identity
U_i, MD_i	i^{th} user and his/her mobile device
PW_i, BIO_i	Password & biometrics of U_i, respectively
$E_p(a,b)$	A non-singular elliptic curve: $y^2 = x^3 + ax + b \pmod p$, $a, b \in Z_p = \{0, 1, 2, \ldots, p-1\}$, $4a^3 + 27b^2 \neq 0 \pmod p$
P	A base point in $E_p(a,b)$
$P + Q$	An elliptic curve point addition; $P, Q \in E_p(a,b)$
$k \cdot P$	An elliptic curve point multiplication; $k \in Z_p^*, P \in E_p(a,b)$
(g_{pri}, G_{pub})	Private-public key pair of CG_k, where $G_{pub} = g_{pri} \cdot P$
n_s	Number of IoT nodes deployed initially
$h(\cdot)$	A "cryptographic (collision resistant) one-way hash function"
SK_{ij}	A session key between two entities U_i and IN_j
x, y	Random numbers generated by U_i and IN_j, respectively
TS_1, TS_2, TS_3	Current timestamps used
ΔT	Maximum transmission delay
$Ex_i \stackrel{?}{=} Ex_j$	Verify whether expression Ex_i matches with expression Ex_j
$\|\|$, $\oplus$	Concatenation & bitwise XOR operations, respectively
$Gen(\cdot)$, $Rep(\cdot)$	Fuzzy extractor generation and reproduction functions
et	Fuzzy extractor error tolerance threshold value
$\mathcal{A}$	A passive/active adversary

secret leakage (ESL) (Section V-B7) and "physical IoT nodes capture" attacks. The detailed description of these attacks can be found in [8]. Apart from these attacks, mutual authentication, anonymity, and untraceability properties need to be preserved in the IoT-based ITS deployment.

IV. PROPOSED SCHEME

Different phases associated to our proposed user authentication protocol for big data collection in IoT-based ITS (UAP-BCIoT) are discussed in this section. We apply the notations listed in Table. II for analyzing and discussing the proposed UAP-BCIoT. To accommodate the replay attack protection, we utilize the current system timestamp validation of the communicated messages. This is a typical assumption applied in several authentication mechanisms across various networking environments [16], [18], [24]–[28].

UAP-BCIoT has seven phases, which are briefly discussed before their detailed description in the subsequent sections as follows.

1) In the *system initialization phase*, the BRC is the authorized entity in the network for picking up various system parameters for each deployed IoT node, and also the authorized CG selects other system parameters including its own private and public keys.
2) In the *IoT device enrollment phase*, the BRC preloads the essential credentials in each IoT node's memory before they are placed in the IoT-based ITS environment.
3) In the *user registration phase*, a legal user U_i first sends the registration request secretly to the trusted CG (CG_k). After receiving the request, CG_k issues registration reply to U_i and the credentials are finally stored in U_i's mobile device.
4) During the *login and authentication phase*, for accessing the services from a desired intelligent IoT device (IN_j) in real-time, a registered legal user U_i with his/her mobile device MD_i needs to login into the system and then to establish the session key with IN_j through the help of CG_k for secure communications among U_i and IN_j. In addition, this phase also allows to establish a session key between CG_k and IN_j at the same time in order to execute the *IoT device credential validation phase* discussed below.
5) During the *password and/or biometric update phase*, UAP-BCIoT permits an authorized registered user U_i to update his/her password/biometric using the credentials stored in the mobile device MD_i without further help of the CG_k, and this phase is executed completely locally.
6) The *dynamic IoT device addition phase* allows deployment of a new IoT device node in the existing network by preloading the necessary credentials in its memory.
7) The *user mobile device revocation phase* permits a scenario where the mobile device of an authorized registered user may be stolen/lost, and in that case, the new credentials for the mobile device are obtained.
8) The *big data analytics phase* permits the secure storage and analysis of the big data generated by the smart devices of the IoT-based ITS environment. This phase is very useful to draw some useful conclusion from the stored, processed and analyzed data. For example, it may be used to predict the chances of a road accident in a particular region, roadside condition, weather condition, etc.
9) The *IoT device credential validation phase* is particularly needed when the CG (CG_k) periodically checks the credentials stored in an IoT node IN_j are valid after its deployment in the network. For this purpose, the established session key between CG_k and IN_j is utilized for secure execution of this phase. In addition, this phase also allows if the IoT nodes are working as per the expectations of the CG_k to detect the malicious behavior of the IoT nodes.

A. System Initialization Phase

This phase incorporates the following steps.

S1: The BRC first picks a long-term secret key X_{CG_k} for the CG_k. It then picks a unique identity ID_{IN_j} for each deployed IoT node IN_j ($j = 1, 2, \ldots, n_s$), where n_s is the number of IoT nodes installed initially in the IoT-based ITS environment. Next, the BRC computes the secret key $SK_{CG-BRC} = h(X_{CG_k} \| MK_{BRC})$, where X_{CG_k} is the secret key of the CG_k and MK_{BRC} is a unique master key of the BRC.

S2: The BRC selects a cryptographic collision-resistant one-way hash function $h : \{0,1\}^* \rightarrow \{0,1\}^l$, where the bit length of hash output (message digest) is denoted by l. $h(\cdot)$ can be taken as SHA-1 (Secure Hash Standard) and for better security, SHA-256 can be also applied [29]. Moreover, the BRC selects a distinct identity ID_{CG_k} for each CG_k.

S3: CG selects a base point P with the order n over a non-singular elliptic curve $E_p(a,b)$, where n is large for sufficient security consideration (for example, n should be chosen at least 160-b number). The CG_k then derives its private/public key pair (g_{pri}, G_{pub}), where $G_{pub} = g_{pri} \cdot P$.

S4: Finally, the information (P, (g_{pri}, G_{pub}), $h(\cdot)$, $\{ID_{IN_j} | 1 \leq j \leq n_s\}$, X_{CG_k}, SK_{CG-BRC}) are stored in CG_k's storage database.

B. IoT Device Enrollment Phase

This phase is completed by the BRC in an offline manner. For each IoT node IN_j, the BRC calculates the secret credential $IC_{j1} = h(SK_{\text{CG-BRC}} \| \text{ID}_{\text{IN}_j})$. The BRC stores the information $(\text{ID}_{\text{IN}_j}, IC_{j1})$ into IN_j's memory before its deployment in the IoT-based ITS environment.

C. User Registration Phase

In this phase, a mobile user/traffic inspector U_i first registers to the CG (CG_k) in order to issue the credentials to be used in the mobile device MD_i through a secure channel. It is worth noting that in UAP-BCIoT we have applied the widely accepted fuzzy extractor for biometric verification purpose [30]. The fuzzy extractor compromises the following two procedures.

1) *Gen:* It is a probabilistic function that takes personal biometrics BIO_i of the user U_i (e.g., fingerprint) as input and a pair (σ_i, τ_i) is produced as output, where σ_i and τ_i signify the secret biometric key and public reproduction parameter, respectively, that is, $\text{Gen}(BIO_i) = (\sigma_i, \tau_i)$.
2) *Rep:* It is a deterministic function that takes a noisy biometric BIO'_i and public reproduction parameter τ_i as input and constructs the original biometric secret key σ_i as output, that is, $\text{Rep}(BIO'_i, \tau_i) = \tau_i$ with the criteria that the Hamming distance between BIO'_i and BIO_i is less than a predefined error tolerance threshold *et*.

U_i undergoes the procedure to receive the credentials from CD_k using the following steps.

R1: U_i is free to pick his/her identity ID_i and password PW_i. U_i then imprints his/her biometrics BIO_i at the mobile device MD_i and generates a random number b_i. U_i calculates $\text{Gen}(BIO_i) = (\sigma_i, \tau_i)$, $MID_i = h(\text{ID}_i \| b_i)$ and $MPW_i = h(PW_i \| \sigma_i)$, and submits the registration request $\langle MID_i, MPW_i \rangle$ secretly to the registered CD_k.

R2: Upon reception of the request, the CG_k calculates $G_1 = (g_{\text{pri}}.h(MID_i)) \cdot P$, $G_2 = G_1 \oplus h(MPW_i \| MID_i)$ and $G_3 = G_1 \oplus h(X_{\text{CG}_k})$. The CG_k then issues the secret credentials to U_i secretly as a registration reply message having the information $\{G_1, G_2, G_3, h(\cdot), P\}$.

R3: After receiving SC_i, U_i computes $L_i = b_i \oplus h(\text{ID}_i \| \sigma_i \| PW_i)$, $G_2^* = G_2 \oplus h(b_i \| \sigma_i \| PW_i) = G_1 \oplus h(MPW_i \| MID_i) \oplus h(b_i \| \sigma_i \| PW_i)$, $G_3^* = G_3 \oplus h(\sigma_i \| b_i \| PW_i) = G_1 \oplus h(X_{\text{CG}_k}) \oplus h(\sigma_i \| b_i \| PW_i)$, and $G_4 = h(G_1 \| PW_i \| b_i \| \sigma_i)$.

Finally, U_i stores $\{L_i, G_2^*, G_3^*, \text{Gen}(\cdot), \text{Rep}(\cdot), \tau_i\}$ into MD_i to complete the registration process. Hence, the U_i's MD_i finally contains $\{L_i, G_2^*, G_3^*, G_4, h(\cdot), \text{Gen}(\cdot), \text{Rep}(\cdot), \tau_i, P\}$. In addition, U_i deletes G_1, G_2 and G_3.

Note that for doing the bitwise XOR of an elliptic-curve point $Q = (Q_x, Q_y)$ with hash value $h(s)$ of an input string s, we will perform it as $Q \oplus h(s) = (Q_x \oplus h(s), Q_y \oplus h(s))$ where the x and y co-ordinates of Q are Q_x and Q_y, respectively. The above phase is outlined in Fig. 2.

User U_i	Cloud-Gateway (CG_k)
Choose ID_i, PW_i.	
Imprint biometric BIO_i.	
Generate random number b_i.	
Compute $Gen(BIO_i) = (\sigma_i, \tau_i)$,	
$MID_i = h(ID_i \| b_i)$,	Compute
$MPW_i = h(PW_i \| \sigma_i)$.	$G_1 = (g_{pri}.h(MID_i)) \cdot P$,
$\xrightarrow[Secure \quad channel]{\{MID_i, MPW_i\}}$	$G_2 = G_1 \oplus h(MPW_i \| MID_i)$,
	$G_3 = G_1 \oplus h(X_{CG_k})$.
	$\xleftarrow[Secure \quad channel]{\{G_1, G_2, G_3, h(\cdot), P\}}$
Compute $L_i = b_i \oplus h(ID_i \| \sigma_i \| PW_i)$,	
$G_2^* = G_2 \oplus h(b_i \| \sigma_i \| PW_i)$,	
$G_3^* = G_3 \oplus h(\sigma_i \| b_i \| PW_i)$,	
$G_4 = h(G_1 \| PW_i \| b_i \| \sigma_i)$.	
Store L_i, G_2^*, G_3^*, G_4 into MD_i.	
Delete G_1, G_2 and G_3.	
$MD_i = \{L_i, G_2^*, G_3^*, G_4, h(\cdot),$	
$Gen(\cdot), Rep(\cdot), \tau_i, P, et\}$.	

Fig. 2. User registration phase.

D. Login and Authentication Phase

To access a desired intelligent IoT device, say IN_j in real-time, a registered legal user U_i with his/her mobile device MD_i can login into the system and establish the session key with IN_j through the CG (CG_k) as follows.

LA1: U_i inserts his/her "identity ID_i" and "password PW_i" into the interface of MD_i, and also imprints "biometrics BIO'_i at MD_i's sensor." MD_i then calculates $\sigma_i^* = \text{Rep}(BIO'_i, \tau_i)$ provided that the "Hamming distance between earlier registered BIO_i and current BIO'_i is less than *et*," $MPW_i^* = h(PW_i \| \sigma_i^*)$, $b_i^* = L_i \oplus h(\text{ID}_i \| \sigma_i^* \| PW_i)$, $MID_i^* = h(\text{ID}_i \| b_i^*)$, $G_1 = h(MID_i^*) \cdot G_{\text{pub}}$, $G_2 = G_2^* \oplus h(b_i^* \| \sigma_i^* \| PW_i)$ $(= G_1 \oplus h(MPW_i \| MID_i))$, $G_3 = G_3^* \oplus h(\sigma_i^* \| b_i^* \| PW_i)$ $(= G_1 \oplus h(X_{\text{CG}_k}))$, and $G_4^* = h(G_1 \| PW_i \| b_i^* \| \sigma_i^*)$.

LA2: MD_i verifies $G_4^* \stackrel{?}{=} G_4$. If it is successful, MD_i confirms that U_i's entered credentials $(\text{ID}_i, PW_i, BIO'_i)$ are valid, and U_i then picks an accessed IoT node IN_j's identity ID_{IN_j} from which he/she likes to access the services. U_i generates a "random number $x \in Z_p^*$" and the "current timestamp TS_1," to compute $M_x = x \cdot P$, $HID_i = MID_i^* \oplus h((G_1 \oplus G_3) || TS_1) = MID_i^* \oplus h(h(X_{\text{CG}_k}) || TS_1)$, $A_1 = x \cdot (G_{\text{pub}} + h(\text{ID}_{\text{IN}_j}) \cdot P)$, $A_2 = A_1 \oplus h(G_2 \| G_1 \| M_x \| TS_1)$, $A_3 = h((G_1 \oplus G_3) \| MID_i^* \| TS_1 \| A_2)$, and dynamic identity of IN_j as $DID_{\text{IN}_j} = \text{ID}_{\text{IN}_j} \oplus h(G_1 \| TS_1)$ with its stored parameters. MD_i sends the login request message to the CG_k as $\text{MSG}_1 = \{A_3, HID_i, G_2, DID_{\text{IN}_j}, M_x, TS_1\}$ over the public channel.

LA3: CG_k checks if $|TS'_1 - TS_1| < \Delta T$ after receiving the message MSG_1 at time TS'_1. If the verification is successful, CG_k computes $MID_i^* = HID_i \oplus h(h(X_{\text{CG}_k}) || TS_1)$, $G_1^* = (g_{\text{pri}}.h(MID_i^*)) \cdot P$, $\text{ID}_{\text{IN}_j} = DID_{\text{IN}_j} \oplus h(G_1^* \| TS_1)$, $A_1^* = (g_{\text{pri}} + h(\text{ID}_{\text{IN}_j})) \cdot M_x$, and $A_2 = A_1^* \oplus h(G_2 \| G_1^* \| M_x \| TS_1)$, and verifies $A_3 \stackrel{?}{=} h((HID_i \oplus MID_i^*) \| MID_i^* \| TS_1 \| A_2)$. If the verification is successful, CG_k confirms that the message received from U_i is legitimate. Then, CG_k generates current timestamp TS_2, calculates $GI_1 = h(h(SK_{\text{CG-BRC}} || \text{ID}_{\text{IN}_j}) || TS_2) \oplus MID_i^*$, the session key shared with IoT node IN_j as $SK_{kj} = h(TS_2 \| \text{ID}_{\text{CG}_k} \| MID_i^* \| h(SK_{\text{CG-BRC}} || \text{ID}_{\text{IN}_j}))$ and $GI_2 = h(\text{ID}_{\text{IN}_j} \| MID_i^* \| M_x \| SK_{kj} \| TS_2)$, and then transmits the message $\text{MSG}_2 = \{GI_1, GI_2, M_x, TS_2\}$ to IN_j over public channel. In addition, CG_k stores the session key SK_{kj} shared with IN_j in its secure database.

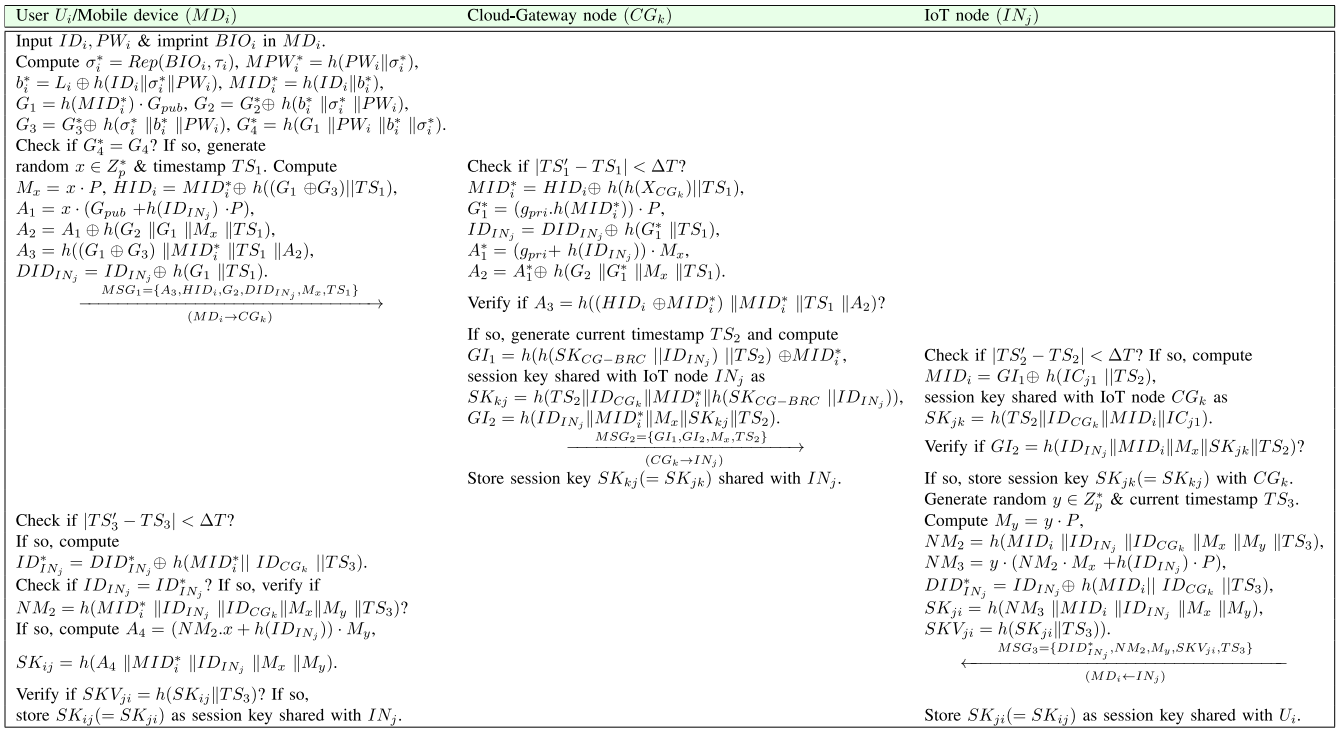


Fig. 3. Login and authentication phases.

LA4: The IoT node IN_j checks if $|TS_2' - TS_2| < \Delta T$ is met after receiving the message MSG_2 at time TS_2'. If the verification is successful, IN_j computes $MID_i = GI_1 \oplus h(IC_{j1} || TS_2)$ and the session key shared with IoT node CG_k as $SK_{jk} = h(TS_2 \| \text{ID}_{\text{CG}_k} \| MID_i \| IC_{j1})$, and verifies if $GI_2 = h(\text{ID}_{\text{IN}_j} \| MID_i \| M_x \| SK_{jk} \| TS_2)$. If it is legitimate, IN_j also stores the session key SK_{jk} $(= SK_{kj})$ shared with CG_k for its key revocation phase described in Section IV-I. Next, IN_j creates a random $y \in Z_p^*$ along with the current timestamp TS_3 and computes $M_y = y \cdot P$, $NM_2 = h(MID_i \| \text{ID}_{\text{IN}_j} \| \text{ID}_{\text{CG}_k} \| M_x \| M_y \| TS_3)$, $NM_3 = y \cdot (NM_2 \cdot M_x + h(\text{ID}_{\text{IN}_j}) \cdot P)$, its dynamic identity $DID_{\text{IN}_j}^* = \text{ID}_{\text{IN}_j} \oplus h(MID_i || \text{ID}_{\text{CG}_k} || TS_3)$, and finally the session key $SK_{ji} = h(NM_3 \| MID_i \| \text{ID}_{\text{IN}_j} \| M_x \| M_y)$ shared with U_i and its verifier $SKV_{ji} = h(SK_{ji} \| TS_3))$. IN_j transmits the message $\text{MSG}_3 = \{DID_{\text{IN}_j}^*, NM_2, M_y, SKV_{ji}, TS_3\}$ to the user U_i via open channel.

LA5: MD_i receives the message MSG_3 at time TS_3' and checks if $|TS_3' - TS_3| < \Delta T$. If the verification is successful, MD_i computes $\text{ID}_{\text{IN}_j}^* = DID_{\text{IN}_j}^* \oplus h(MID_i^* || \text{ID}_{\text{CG}_k} || TS_3)$, and then verifies if accessed IN_j's identity $\text{ID}_{\text{IN}_j} \stackrel{?}{=} \text{ID}_{\text{IN}_j}^*$. If it is satisfied, MD_i verifies $NM_2 \stackrel{?}{=} h(MID_i^* \| \text{ID}_{\text{IN}_j} \| \text{ID}_{\text{CG}_k} \| M_x \| M_y \| TS_3)$ to validate the received message MSG_3 from legitimate IN_j. If the verification is successful, MD_i validates the IoT node IN_j and its legitimacy. Furthermore, MD_i computes $A_4 = (NM_2.x + h(\text{ID}_{\text{IN}_j})) \cdot M_y$ and the session key $SK_{ij} = h(A_4 \| MID_i^* \| \text{ID}_{\text{IN}_j} \| M_x \| M_y)$ shared with IN_j, and checks if $SKV_{ji} \stackrel{?}{=} h(SK_{ij} \| TS3)$. If it is so, SK_{ij} is treated as authentic.

Finally, two session keys are successfully established: 1) a session key between U_i and IN_j as $SK_{ij} = h(A_4 \| MID_i^* \| \text{ID}_{\text{IN}_j} \| M_x \| M_y) = h(NM_3 \| MID_i \| \text{ID}_{\text{IN}_j} \| M_x \| M_y) = SK_{ji}$ and 2) another session key between CG_k and IN_j as $SK_{kj} = h(TS_2 \| \text{ID}_{\text{CG}_k} \| MID_i^* \| h(SK_{\text{CG-BRC}} \| \text{ID}_{\text{IN}_j})) = h(TS_2 \| \text{ID}_{\text{CG}_k} \| MID_i \| IC_{j1}) = SK_{jk}$. This phase is also briefly illustrated in Fig. 3.

Remark 1: Through the proposed scheme (UAP-BCIoT), a legitimate user can access the data of the IoT devices installed inside the vehicles via the cloud gateway node using the Internet. This mechanism is applicable in scenarios where a legitimate user needs to access the real-time data of the vehicles (i.e., roadside conditions and vehicle accident in some particular regions). In such a scenario, enormous amount of data is generated, which we need to store the data to the cloud servers, which also form the ITS data. It is treated as the big data in ITS. Some big data analytics techniques are then required to draw useful conclusion from this (i.e., chances of road accident in a particular region). The data of IoT nodes can be transmitted to cloud servers in a secure way through the cloud gateway node using the authentication and key agreement mechanism. The proposed authentication and key agreement scheme (UAP-BCIoT) is useful in such scenarios because the real-time accessed data from the IoT nodes in the vehicles can be later securely stored at the cloud too. In addition, authentication and key agreement among IoT nodes, cloud gateway node and cloud servers are also required to store the data securely at the cloud for the big data analytics. In this way, the proposed UAP-BCIoT helps in big data collection at the cloud securely.

E. Password/Biometric Update Phase

A valid registered user U_i will undergo the following procedure to update his/her password/biometric using the credentials stored in mobile device MD_i without the involvement of CG_k.

User (U_i)	Mobile device (MD_i)
Choose ID_i, PW_i and BIO_i'.	Compute $\sigma_i^* = Rep(BIO_i', \tau_i)$,
$\xrightarrow{\{ID_i, PW_i, BIO_i'\}}$	$MPW_i^* = h(PW_i \| \sigma_i^*)$,
	$b_i^* = L_i \oplus h(ID_i \| \sigma_i^* \| PW_i)$,
	$MID_i^* = h(ID_i \| b_i^*)$,
	$G_1 = h(MID_i^*) \cdot G_{pub}$,
	$G_2 = G_2^* \oplus h(b_i^* \| \sigma_i^* \| PW_i)$,
	$G_3 = G_3^* \oplus h(\sigma_i^* \| b_i^* \| PW_i)$,
	Verify $G_4^* \stackrel{?}{=} h(G_1 \| PW_i \| b_i^* \| \sigma_i^*)$.
Select new password PW_i^{new}.	If so, inform U_i to select
Imprint new biometrics BIO_i^{new}.	new password/biometric.
$\xrightarrow{\{PW_i^{new}, BIO_i^{new}\}}$	
	Compute
	$Gen(BIO_i new) = (\sigma_i^{new}, \tau_i^{new})$,
	$L_i^{new} = b_i^* \oplus h(ID_i \| \sigma_i^{new} \| PW_i^{new})$,
	$MPW_i^{new} = h(PW_i^{new} \| \sigma_i^{new})$,
	$G_2^{*new} = G_2 \oplus h(b_i^* \| \sigma_i^{new} \| PW_i^{new})$,
	$G_3^{*new} = G_3 \oplus h(\sigma_i^{new} \| b_i^* \| PW_i^{new})$,
Replace L_i, G_2^*, G_3^*, G_4, τ_i	$G_4 = h(G_1 \| PW_i^{new} \| b_i^* \| \sigma_i^{new})$,
with L_i^{new}, G_2^{*new}, G_3^{*new}, τ_i^{new}.	

Fig. 4. Summary of the password/biometric update phase.

Mobile device (MD_i)/User (U_i)	Cloud-Gateway node (CG_k)
Keep same identity ID_i.	
Imprint same biometrics BIO_i' at MD_i.	
Input new password PW_i'.	
Generate new random number b_i'.	
Calculate $Gen(BIO_i') = (\sigma_i', \tau_i')$,	
$MID_i' = h(ID_i \| b_i')$,	Compute
$MPW_i' = h(PW_i' \| \sigma_i')$.	$G_1 = (g_{pri}.h(MID_i')) \cdot P$,
$\xrightarrow[Secure\ \ channel]{\{MID_i', MPW_i'\}}$	$G_2' = G_1 \oplus h(MPW_i' \| MID_i')$,
	$G_3 = G_1 \oplus h(X_{CG_k})$.
	$\xleftarrow[Secure\ \ channel]{\{G_1, G_2', G_3, h(\cdot), P\}}$
Compute $L_i' = b_i' \oplus h(ID_i \| \sigma_i' \| PW_i')$,	
$G_2^* = G_2' \oplus h(b_i' \| \sigma_i' \| PW_i')$,	
$G_3^* = G_3 \oplus h(\sigma_i' \| b_i' \| PW_i')$,	
$G_4 = h(G_1 \| PW_i' \| b_i' \| \sigma_i')$.	
Store $\{L_i', G_2^*, G_3^*, G_4, Gen(\cdot),$	
$Rep(\cdot), \tau_i'\}$ in MD_i.	
Erase G_1, G_2' and G_3 from MD_i.	

Fig. 5. Summary of the user mobile device revocation phase.

P1: U_i inserts his/her identity ID_i and password PW_i into the interface of MD_i, and also imprints biometrics BIO_i' at MD_i's sensor. MD_i then computes $\sigma_i^* = \mathrm{Rep}(BIO_i', \tau_i)$ provided that the Hamming distance between earlier registered BIO_i and current BIO_i' is less than *et*, $MPW_i^* = h(PW_i \| \sigma_i^*)$, $b_i^* = L_i \oplus h(\mathrm{ID}_i \| \sigma_i^* \| PW_i)$, $MID_i^* = h(\mathrm{ID}_i \| b_i^*)$, $G_1 = h(MID_i^*) \cdot G_{\mathrm{pub}}$, $G_2 = G_2^* \oplus h(b_i^* \| \sigma_i^* \| PW_i)$, $G_3 = G_3^* \oplus h(\sigma_i^* \| b_i^* \| PW_i)$ and $G_4^* = h(G_1 \| PW_i \| b_i^* \| \sigma_i^*)$.

P2: MD_i verifies $G_4^* \stackrel{?}{=} G_4$. If it is successful, MD_i confirms that U_i's entered old credentials $(\mathrm{ID}_i, PW_i, BIO_i')$ are valid, and U_i is then informed to choose a new password PW_i^{new} as well as a new biometrics $\mathrm{BIO}_i^{\mathrm{new}}$, if needed. MD_i calculates $\mathrm{Gen}(BIO_i^{\mathrm{new}}) = (\sigma_i^{\mathrm{new}}, \tau_i^{\mathrm{new}})$, $L_i^{\mathrm{new}} = b_i^* \oplus h(\mathrm{ID}_i \| \sigma_i^{\mathrm{new}} \| PW_i^{\mathrm{new}})$, $MPW_i^{\mathrm{new}} = h(PW_i^{\mathrm{new}} \| \sigma_i^{\mathrm{new}})$, $G_2^{*\mathrm{new}} = G_2 \oplus h(b_i^* \| \sigma_i^{\mathrm{new}} \| PW_i^{\mathrm{new}})$, $G_3^{*\mathrm{new}} = G_3 \oplus h(\sigma_i^{\mathrm{new}} \| b_i^* \| PW_i^{\mathrm{new}})$, and $G_4 = h(G_1 \| PW_i^{\mathrm{new}} \| b_i^* \| \sigma_i^{\mathrm{new}})$.

P3: Finally, U_i stores L_i^{new}, $G_2^{*\mathrm{new}}$, $G_3^{*\mathrm{new}}$, $\mathrm{Gen}(\cdot)$, $\mathrm{Rep}(\cdot)$ and τ_i^{new} into MD_i to complete the update process. Hence, U_i's MD_i contains $\{L_i^{\mathrm{new}}, G_2^{*\mathrm{new}}, G_3^{*\mathrm{new}}, G_4^{\mathrm{new}}, h(\cdot), \mathrm{Gen}(\cdot), \mathrm{Rep}(\cdot), \tau_i^{\mathrm{new}}, P\}$. In addition, U_i deletes G_2^* and G_3^* from MD_i.

The password/biometric change phase is then briefly illustrated in Fig. 4.

F. Dynamic IoT Device Addition Phase

For deployment of a new IoT device node, say $\mathrm{IN}_j^{\mathrm{new}}$ in the existing network, the BRC requires to pick a unique identity $\mathrm{ID}_{\mathrm{IN}_j}^{\mathrm{new}}$. After that the BRC needs to calculate the secret credential $IC_{j1}^{\mathrm{new}} = h(SK_{\mathrm{CG-BRC}} \| \mathrm{ID}_{\mathrm{IN}_j}^{\mathrm{new}})$. The *BRC* also stores the information $(\mathrm{ID}_{\mathrm{IN}_j}^{\mathrm{new}}, IC_{j1}^{\mathrm{new}})$ into $\mathrm{IN}_j^{\mathrm{new}}$'s memory before its deployment in the IoT-based ITS environment.

G. User Mobile Device Revocation Phase

If the mobile device MD_i of an authorized registered user U_i is stolen/lost, the following steps need to be executed for obtaining new credentials for the mobile device MD_i^{new}.

RE1: U_i keeps the same identity ID_i, but chooses a new password PW_i'. U_i can then imprint his/her biometrics BIO_i' at the mobile device MD_i and generates a random number b_i'. U_i calculates $\mathrm{Gen}(BIO_i') = (\sigma_i', \tau_i')$, $MID_i' = h(\mathrm{ID}_i \| b_i')$ and $MPW_i' = h(PW_i' \| \sigma_i')$, and submits the registration request $\langle MID_i', MPW_i' \rangle$ secretly to the registered CD_k.

RE2: On receiving the request, the CG_k computes $G_1 = (g_{\mathrm{pri}}.h(MID_i')) \cdot P$, $G_2' = G_1 \oplus h(MPW_i' \| MID_i')$ and $G_3 = G_1 \oplus h(X_{\mathrm{CG}_k})$. The CG_k then issues the secret credentials to U_i secretly as a registration reply message having the information $\{G_1, G_2', G_3, h(\cdot), P\}$.

RE3: After receiving registration reply message, U_i computes $L_i' = b_i' \oplus h(\mathrm{ID}_i \| \sigma_i' \| PW_i')$, $G_2^* = G_2' \oplus h(b_i' \| \sigma_i' \| PW_i')$, $G_3^* = G_3 \oplus h(\sigma_i' \| b_i' \| PW_i')$, and $G_4 = h(G_1 \| PW_i' \| b_i' \| \sigma_i')$.

Finally, U_i stores $\{L_i', G_2^*, G_3^*, G_4, \mathrm{Gen}(\cdot), \mathrm{Rep}(\cdot), \tau_i'\}$ into MD_i to complete the revocation process. Hence, the U_i's MD_i contains $\{L_i', G_2^*, G_3^*, G_4, h(\cdot), \mathrm{Gen}(\cdot), \mathrm{Rep}(\cdot), \tau_i', et, P\}$. In addition, U_i deletes G_1, G_2', and G_3.

The above user mobile device revocation phase is also briefly illustrated in Fig. 5.

H. Big Data Analytics Phase

This phase permits a secure storage and analysis of the big data generated by the smart devices of the IoT-based ITS environment. This phase is apparently useful to draw some useful conclusion from the stored, processed and analyzed data. For example, it will give the predictions about the chances of a road accident in a particular region, vehicle condition, roadside condition, etc. The following procedure is used in this phase.

BDA1: The deployed IoT nodes (i.e., smart devices inside the vehicles) produce enormous amount of data which is very sensitive in nature, because there are vulnerabilities to various types of attacks as discussed earlier. The data should be stored, processed and analyzed in a secure way. Note that for the secure exchange of data between the cloud gateway server CG_k and an IoT node IN_j, we can utilize the steps of authentication and key establishment phase as discussed in Section IV-D. For secure communication between CG_k and IN_j, they established a session key SK_{kj} $(= SK_{jk})$.

BDA2: IN_j now encrypts its data, say $\mathrm{data}_{\mathrm{IN}_j}$ as $E_{SK_{jk}}(\mathrm{data}_{\mathrm{IN}_j})$ with the session key SK_{jk} and sends the encrypted data to CG_k. After receiving encrypted data, CG_k decrypts it using the established session key SK_{kj} to extract the original data $\mathrm{data}_{\mathrm{IN}_j}$.

BDA3: Likewise, CG_k receives the data from different IoT nodes IN_j, where $j = 1, 2 \cdots n_s$ and n_s is the number of IoT nodes in the ITS environment. Again, CG_k executes other steps of the big data analytics, such as data acquisition and filtering, data extraction, data aggregation and representation, data analysis, and data visualization, on the received data. The final outcome of this phase will come in the form of some useful conclusion, such as chances of road accident in a particular region [31]–[33].

Remark 2: ITS is an emerging transportation structure in which several users, roads, and vehicles are involved. ITS is the fused usage of pattern setting advancements using equipment, communication, and impelled sensors. These applications give voyagers huge information while improving the safety, security and capability of the transportation system. The data assembled by different devices and users in an IoT-based ITS environment is of colossal volume which leads to the inception of big data. Thus, we require some big data analytical methods to draw useful conclusions from the assembled data. However, for such kind of data collection, we require strong security protocols (i.e., user authentication). In the absence of these security protocols, an adversary $\mathcal{A}$ may interfere in the communication and can change the value of the exchanged data. In that situation, there will not be any use of big data collection and analysis, because it may produce wrong predictions and results. Thus, there is an essential requirement of the deployment of user authentication in an IoT-based ITS for the big data collection and analysis. As a result, we have presented a secure user authentication protocol for big data collection and analysis in the IoT-based ITS environment.

I. IoT Device Credential Validation Phase

Due to the possibility of the IoT node physical capture attack by an adversary or malicious behavior of an IoT node, it is apparent to verify periodically by the CG node (CG_k) if an IoT node IN_j is behaving properly or not in the network. This phase uses the already established session key SK_{jk} ($= SK_{kj}$) between IN_j and CG_k. The following are the steps required to complete this phase.

DCV1: CG_k first initiates the communication by generating a current timestamp TS_{rg} and a random secret $rv_{rg} \in Z_q^*$ and then calculating $A_{CG_k} = h(X_{CG_k} \| rv_{rg} \| TS_{rg})$ and $Re_1 = A_{CG_k} \oplus h(SK_{kj} \| h(SK_{CG-BRC} \| ID_{IN_j}) \| TS_{rg})$. Next, CG_k sends the device credential validation request message $\{Re_1, TS_{rg}\}$ to IN_j via the public channel.

DCV2: If the message $\{Re_1, TS_{rg}\}$ is received at time TS'_{rg}, IN_j verifies the timestamp TS_{rg} by the condition: $|TS_{rg} - TS'_{rg}| < \Delta T$. If it is valid, IN_j proceeds to calculate $B_{CG_k} = Re_1 \oplus h(SK_{jk} \| IC_{j1} \| TS_{rg})$ using its stored credential IC_{j1} and session key SK_{jk} shared with CG_k. After that, IN_j generates a current timestamp TS_{rj}, calculates $Re_2 = h(SK_{jk} \| B_{CG_k} \| TS_{rj})$ and sends the device credential validation response message $\{Re_2, TS_{rj}\}$ to CG_k via public channel.

DCV3: After receiving the message $\{Re_2, TS_{rj}\}$ at time TS'_{rj}, CG_k checks if $|TS_{rj} - TS'_{rj}| < \Delta T$. If the timestamp validation passes, CG_k then calculates $Re_2^* = h(SK_{kj} \| A_{CG_k} \| TS_{rj})$ and validates the condition: $Re_2^* = Re_2$. If it is valid, CG_k assures that IN_j is behaving properly in the deployment area and also its credentials are genuine.

V. Security Analysis

Wang *et al.* [34] analyzed numerous anonymous two-factor authentication protocols and then specified that under the widely accepted adversarial model, such as the DY model [21], certain goals are beyond fulfillment. They also specified that the widely accepted formal methods including the random oracle model-based proof cannot catch some structural faults. This implies that assuring the soundness of authentication protocols still stands to be an open matter. Such crucial observations force us to have all sorts of security analysis, such as the random oracle model-based formal security analysis (Section V-A), informal security analysis (Section V-B), and formal security verification (Section VI) in order to strengthen security of the proposed scheme.

To analyze the security of the proposed scheme (UAP-BCIoT), we define a one-way collision-resistant hash function and ECDDHP as follows.

Definition 1: A "one-way collision-resistant hash function," say $h : \{0,1\}^* \rightarrow \{0,1\}^{l_h}$ is a "deterministic algorithm that gives output as a binary string $h(s) \in \{0,1\}^{l_h}$ of fixed-length l_h bits as hash output (message digest) on an input with an arbitrary length binary string $s \in \{0,1\}^*$." The advantage in finding collision for an adversary $\mathcal{A}$ is then "$Adv_{\mathcal{A}}^{HASH}(t) = Pr[(s_1, s_2) \leftarrow_R \mathcal{A} : s_1 \neq s_2, h(s_1) = h(s_2)]$, where an event E's probability is denoted by $Pr[E]$ and $(s_1, s_2) \leftarrow_R \mathcal{A}$ indicates that the input pair (s_1, s_2) is randomly picked by $\mathcal{A}$." An (ψ, t)-adversary $\mathcal{A}$ attacking h's collision resistance implies that the runtime allowed for $\mathcal{A}$ is at most t and $Adv_{(A)}^{HASH}(t) \leq \psi$.

Definition 2: Let $X \in E_p(a, b)$ be a point on an elliptic curve $E_p(a, b)$. The ECDDHP states that given a quadruple $(X, k_1.X, k_2.X, k_3.X)$, decide if $k_3 = k_1 k_2$ or it is a uniform value, where $k_1, k_2, k_3 \in Z_p^* = \{1, 2, \ldots, p-1\}$.

In order to maintain the intractability of ECDDHP, p must be picked as at least 160-b prime number.

A. Formal Security Analysis Using ROR Model

The semantic security of the proposed UAP-BCIoT under the ROR model [7] is demonstrated in this section. Wang *et al.* [20] mentioned that Zipf's law significantly differs from the uniform distribution for user-selected passwords. In practical scenario, "the size of password dictionary is very much constrained in the sense that the space of the passwords may not be fully utilized by the users, and only a small portion of the permitted characters space is used" [20]. We apply Zipf's law in proving the semantic security of the proposed UAP-BCIoT in Theorem 1 in order to show the session key security part, because Zif's law is widely used in several recently proposed authentication schemes [19], [35]. Prior to proving Theorem 1, we discuss below the ROR model in short.

TABLE III
VARIOUS QUERIES AND THEIR SIGNIFICANCE

Query	Purpose
$Send(\pi^i, m)$	This query permits $\mathcal{A}$ to dispatch a message m to π^i, and accordingly, π^i also responses to the received message m
$Execute(\pi_{U_i}^{i_1}, \pi_{CG_k}^{i_2}, \pi_{IN_j}^{i_3})$	With the help from such a query, $\mathcal{A}$ can eavesdrop the messages exchanged among U_i, CG_k and IN_j
$CorruptMD(\pi_{U_i}^{i_1})$	Under this query, $\mathcal{A}$ can have a legal user U_i's password PW_i as well as biometric secret key σ_i from "U_i's lost or stolen mobile device, MD_i"
$Reveal(\pi^i)$	The current session key SK_{ij} among π^i and its associated partner is revealed to $\mathcal{A}$
$Test(\pi^i)$	This query permits $\mathcal{A}$ appeals π^i for SK_{ij} and π^i provides with a "probabilistic outcome of a flipped unbiased coin, say c"

The considered ROR model has the following components that are associated with various queries accessed by an adversary $\mathcal{A}$. The purpose of various queries are tabulated in Table III.

1) *Participants:* The involved participants associated with the proposed UAP-BCIoT are the users (U_i), the CG nodes (CG_k), and IoT nodes (IN_j). The instances i_1, i_2, and i_3 of U_i, CG_k, and IN_j are denoted by the notations $\pi_{U_i}^{i_1}$, $\pi_{CG_k}^{i_2}$, and $\pi_{IN_j}^{i_3}$, and these are also termed as oracles.
2) *Accepted State:* An instance π^i is said to be in "accepted state," when after receiving the last presumed protocol message it gets into an accept state. The "session identification *sid* of π^i for the running session" is constituted when all the transmitted and received messages by the π^i are organized in continuation.
3) *Partnering:* Two instances, π^{i_1} and π^{i_2}, will be partners to each other once the following conditions are fulfilled.
   a) π^{i_1} and π^{i_2} need to be in "accepted states."
   b) π^{i_1} and π^{i_2} need to have the same *sid* and also need to "mutually authenticate each other."
   c) π^{i_1} and π^{i_2} need to be "mutual partners of each other."
4) *Freshness:* The instance $\pi_{U_i}^{i_1}$ or $\pi_{IN_j}^{i_3}$ is called fresh if the created session key SK_{ij} between U_i and IN_j is not leaked to the $\mathcal{A}$ using the Reveal(π^i) query provided in Table III.

Theorem 1: If $\mathcal{A}$ is a polynomial time adversary running in time t against the proposed UAP-BCIoT under the ROR model that applies Zipf's law for the user-chosen passwords, l_b is the number of bits in the biometrics secret key σ_i, and $\text{Adv}_{\mathcal{A}}^{\text{UAP-BCIoT}}(t)$ is $\mathcal{A}$'s advantage in breaking the proposed UAP-BCIoT's semantic security in time t for deriving the session key SK_{ij} between a user U_i and an IoT node IN_j, and also the session key SK_{jk} between an IoT node IN_j and the CG node (CG_k), then $\text{Adv}_{\mathcal{A}}^{\text{UAP-BCIoT}}(t) \leq (q_h^2/|\text{Hash}|) + 2(\max\{C'.q_s^{s'}, (q_s/2^{l_b})\} + \text{Adv}_{\mathcal{A}}^{\text{ECDDHP}}(t))$, where q_h, q_s, and $|Hash|$ denote, respectively, the number of hash queries, *Send* queries and range space of $h(\cdot)$, and $\mathcal{A}$'s advantage in cracking the ECDDHP (see Definition 2) is $\text{Adv}_{\mathcal{A}}^{\text{ECDDHP}}(t)$, and Zipf's parameters are C' and s' [20].

Proof: We follow the proof of this theorem in a similar manner as in the previous authentication protocols [18], [26], [36]. The defined five games, say $\text{Game}_j^{\mathcal{A}}$, $j = 0, 1, 2, 3, 4$, are associated with the proof, which are played in the following way. We denote $\text{Succ}_{\text{Game}_j^{\mathcal{A}}}$ as an "event where $\mathcal{A}$ can guess the random bit c in the game $\text{Game}_j^{\mathcal{A}}$ correctly," and $\mathcal{A}$'s advantage in winning $\text{Game}_j^{\mathcal{A}}$ as $\text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_j^{\mathcal{A}}} = Pr[\text{Succ}_{\text{Game}_j^{\mathcal{A}}}]$, where Pr[$E$] indicates the "probability of an event E."

1) $\text{Game}_0^{\mathcal{A}}$*:* This game corresponds to the actual attack executed by $\mathcal{A}$ against our proposed UAP-BCIoT in the ROR model. Because "the bit c is picked up randomly before the beginning of the $\text{Game}_0^{\mathcal{A}}$," the semantic security of UAP-BCIoT gives the following:

$$\text{Adv}_{\mathcal{A}}^{\text{UAP-BCIoT}}(t) = \left| 2\text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_0^{\mathcal{A}}} - 1 \right|. \quad (1)$$

2) $\text{Game}_1^{\mathcal{A}}$*:* This game is implemented as "an eavesdropping attack in which $\mathcal{A}$ can eavesdrop all the messages $\text{MSG}_1 = \{A_3, HID_i, G_2, DID_{\text{IN}_j}, M_x, TS_1\}$, $\text{MSG}_2 = \{GI_1, GI_2, M_x, TS_2\}$, and $\text{MSG}_3 = \{DID_{\text{IN}_j}^*, NM_2, M_y, SKV_{ji}, TS_3\}$ exchanged between U_i, CG_k, and IN_j during the login and authentication phase by executing the *Execute* query tabulated in Table III. Once this game is over, $\mathcal{A}$ needs to execute the *Reveal* along with *Test* queries in order to ensure if the derived session key SK_{ij} is original or just a "random key." However, only by eavesdropping the messages MSG_j ($j = 1, 2, 3$) the adversary $\mathcal{A}$'s winning probability in $\text{Game}_1^{\mathcal{A}}$ is not at all elevated as the calculation of SK_{ij} needs both temporal and long-term secret information, such as x, y, MID_i, ID_{CG_k}, and ID_{IN_j}. This means that both the games $\text{Game}_0^{\mathcal{A}}$ and $\text{Game}_1^{\mathcal{A}}$ are "indistinguishable." Hence, we have

$$\text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_1^{\mathcal{A}}} = \text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_0^{\mathcal{A}}}. \quad (2)$$

3) $\text{Game}_2^{\mathcal{A}}$*:* This game corresponds to an active attack where $\mathcal{A}$ can execute several hash queries. Assume that $\mathcal{A}$ intercepts all the messages $\text{MSG}_1 = \{A_3, HID_i, G_2, DID_{\text{IN}_j}, M_x, TS_1\}$, $\text{MSG}_2 = \{GI_1, GI_2, M_x, TS_2\}$, and $\text{MSG}_3 = \{DID_{\text{IN}_j}^*, NM_2, M_y, SKV_{ji}, TS_3\}$ exchanged between U_i, CG_k, and IN_j. It is worth noticing that $M_x = x \cdot P$, $HID_i = MID_i^* \oplus h((G_1 \oplus G_3)||TS_1) = MID_i^* \oplus h(h(X_{\text{CG}_k})||TS_1)$, $A_1 = x \cdot (G_{\text{pub}} + h(\text{ID}_{\text{IN}_j}) \cdot P)$, $A_2 = A_1 \oplus h(G_2 \| G_1 \| M_x \| TS_1)$, and $A_3 = h((G_1 \oplus G_3) \| MID_i^* \| TS_1 \| A_2)$, the dynamic identity of IN_j is $DID_{\text{IN}_j} = \text{ID}_{\text{IN}_j} \oplus h(G_1 \| TS_1)$, $GI_1 = h(h(SK_{\text{CG-BRC}} || \text{ID}_{\text{IN}_j}) || TS_2) \oplus MID_i^*$, the session key shared between the IoT node IN_j and CG_k is $SK_{kj} = h(TS_2 \| \text{ID}_{\text{CG}_k} \| MID_i^* \| h(SK_{\text{CG-BRC}} \| \text{ID}_{\text{IN}_j})) = h(TS_2 \| \text{ID}_{\text{CG}_k} \| MID_i \| IC_{j1}) = SK_{jk}$ and $GI_2 = h(\text{ID}_{\text{IN}_j} \| MID_i^* \| M_x \| SK_{kj} \| TS_2)$, $M_y = y \cdot P$, $NM_2 = h(MID_i \| \text{ID}_{\text{IN}_j} \| \text{ID}_{\text{CG}_k} \| M_x \| M_y \| TS_3)$, $NM_3 = y \cdot (NM_2 \cdot M_x + h(\text{ID}_{\text{IN}_j}) \cdot P)$, and $DID_{\text{IN}_j}^* = \text{ID}_{\text{IN}_j} \oplus h(MID_i || \text{ID}_{\text{CG}_k} || TS_3)$, the session key is $SK_{ji} = h(NM_3 \| MID_i \| \text{ID}_{\text{IN}_j} \| M_x \| M_y)$ shared between U_i and IN_j, and its verifier is $SKV_{ji} = h(SK_{ji} \| TS_3)$. All the

secret credentials in various components involved in the messages (MSG_1, MSG_2, and MSG_3) are protected by a "one-way collision-resistant hash function $h(\cdot)$" (see Definition 1). The chosen random numbers, identities, current timestamps, and also secrets are applied in the construction of the messages MSG_1, MSG_2, and MSG_3. Therefore, there is no collision when $\mathcal{A}$ executes the hash query. Since both the games $\text{Game}_1^{\mathcal{A}}$ and $\text{Game}_2^{\mathcal{A}}$ are "indistinguishable" apart from the inclusion of the simulation of the hash query in $\text{Game}_2^{\mathcal{A}}$, the results from the "birthday paradox" lead to the following:

$$\left|\text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_1^{\mathcal{A}}} - \text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_2^{\mathcal{A}}}\right| \leq \frac{q_h^2}{2|\text{Hash}|}. \quad (3)$$

4) $\text{Game}_3^{\mathcal{A}}$*:* This game implements the simulation of the *CorruptMD* query. Thus, $\mathcal{A}$ can extract "all the information $\{L_i, G_2^*, G_3^*, G_4, h(\cdot), \text{Gen}(\cdot), \text{Rep}(\cdot), \tau_i, P\}$ stored in the mobile device MD_i of the user U_i." The guessing probability of the "biometric secret key σ_i of length l_b bits (respectively, BIO_i)" is roughly $(1/2^{l_b})$ [37]. In addition, assume that $\mathcal{A}$ will attempt to guess the "low-entropy passwords using Zipf's law on passwords" [20]. When only the "trawling guessing attacks" are considered, the advantage of $\mathcal{A}$ turns out to be over 0.5 if $q_s = 10^7$ or 10^8 [20]. Now, if the "targeted guessing attacks (in which $\mathcal{A}$ can use the target user's personal information)" are considered, $\mathcal{A}$'s advantage turns out to be over 0.5 if $q_s \leq 10^6$ [20]. Since only a limited number of wrong password entries are allowed in a system in practice, and the games $\text{Game}_2^{\mathcal{A}}$ and $\text{Game}_3^{\mathcal{A}}$ are "indistinguishable" in the absence of guessing attacks, the following result is obtained [19], [35]:

$$\left|\text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_2^{\mathcal{A}}} - \text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_3^{\mathcal{A}}}\right| \leq \max\left\{C'.q_s^{s'}, \frac{q_s}{2^{l_b}}\right\}. \quad (4)$$

Here, C' and s' denote Zipf's parameters [20].

5) $\text{Game}_4^{\mathcal{A}}$*:* In this final game, $\mathcal{A}$ by eavesdropping the messages MSG_1, MSG_2 and MSG_3 will try to compute the session key between a legal user U_i and an IoT node IN_j. The session key shared between the IoT node IN_j and CG_k is $SK_{kj} = h(TS_2 \| \text{ID}_{\text{CG}_k} \| MID_i^* \| h(SK_{\text{CG-BRC}} \| \text{ID}_{\text{IN}_j})) = h(TS_2 \| \text{ID}_{\text{CG}_k} \| MID_i \| IC_{j1}) = SK_{jk}$. The session key between U_i and IN_j is computed as $SK_{ij} = h(A_4 \| MID_i^* \| \text{ID}_{\text{IN}_j} \| M_x \| M_y) = h(NM_3 \| MID_i \| \text{ID}_{\text{IN}_j} \| M_x \| M_y) = SK_{ji}$. We have $NM_3 = y \cdot (NM_2 \cdot M_x + h(\text{ID}_{\text{IN}_j}) \cdot P) = ((xy) \cdot P).NM_2 + h(\text{ID}_{\text{IN}_j}) \cdot M_y$, and $A_4 = (NM_2.x + h(\text{ID}_{\text{IN}_j})) \cdot M_y = ((xy) \cdot P).NM_2 + h(\text{ID}_{\text{IN}_j}) \cdot M_y = NM_3$. Thus, if $\mathcal{A}$ is able to derive $(xy) \cdot P$ from the intercepted $M_x = x \cdot P$ and $M_y = y \cdot P$ in polynomial time t, the derivation of SK_{ij} becomes easy. Both the games $\text{Game}_3^{\mathcal{A}}$ and $\text{Game}_4^{\mathcal{A}}$ are also "indistinguishable" in the absence of solving ECDDHP (see Definition 2). As a result, the ECDDHP leads to the following result:

$$\left|\text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_3^{\mathcal{A}}} - \text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_4^{\mathcal{A}}}\right| \leq \text{Adv}_{\mathcal{A}}^{\text{ECDDHP}}(t). \quad (5)$$

Now, all the queries are executed by $\mathcal{A}$. Therefore, it is only pending to guess the bit c for "winning the game after querying the *Test* query." It then follows that:

$$\text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_4^{\mathcal{A}}} = \frac{1}{2}. \quad (6)$$

From (1), (2), and (6), we have

$$\begin{aligned}\frac{1}{2}\text{Adv}_{\mathcal{A}}^{\text{UAP-BCIoT}}(t) &= \left|\text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_0^{\mathcal{A}}} - \frac{1}{2}\right| \\ &= \left|\text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_0^{\mathcal{A}}} - \text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_4^{\mathcal{A}}}\right| \\ &= \left|\text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_1^{\mathcal{A}}} - \text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_4^{\mathcal{A}}}\right|. \end{aligned} \quad (7)$$

Applying the triangular inequality on (7), and from (3)–(5), we obtain the following result:

$$\begin{aligned}&\frac{1}{2}\text{Adv}_{\mathcal{A}}^{\text{UAP-BCIoT}}(t) \\ &\leq \left|\text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_1^{\mathcal{A}}} - \text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_2^{\mathcal{A}}}\right| \\ &\quad + \left|\text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_2^{\mathcal{A}}} - \text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_3^{\mathcal{A}}}\right| \\ &\quad + \left|\text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_3^{\mathcal{A}}} - \text{Adv}_{\text{UAP-BCIoT}}^{\text{Game}_4^{\mathcal{A}}}\right| \\ &\leq \frac{q_h^2}{2|Hash|} + \max\left\{C'.q_s^{s'}, \frac{q_s}{2^{l_b}}\right\} + \text{Adv}_{\mathcal{A}}^{\text{ECDDHP}}(t). \end{aligned} \quad (8)$$

Finally, by multiplying both sides of (8) by a factor of 2, we obtain the final result: $\text{Adv}_{\mathcal{A}}^{\text{UAP-BCIoT}}(t) \leq (q_h^2/|\text{Hash}|) + 2(\max\{C'.q_s^{s'}, (q_s/2^{l_b})\} + \text{Adv}_{\mathcal{A}}^{\text{ECDDHP}}(t))$. ■

B. Informal Security Analysis

This section discusses the security of the proposed UAP-BCIoT informally (nonmathematically).

1) Impersonation Attacks: We consider the following three cases.

1) *User Impersonation Attack:* Consider an active attacker $\mathcal{A}$ who tries to capture the transmitted messages MSG_i $(i = 1, 2, 3)$ between entities U_i and CG_k, between entities CG_k and IN_j and between entities U_i and IN_j. If $\mathcal{A}$ tries to impersonate U_i, $\mathcal{A}$ needs to produce the MSG_1 with valid credentials to the CG_k. But, due to the lack of knowledge of the CG_k's private key, ID_i, b_i, x, and G_1, it becomes a computationally expensive task for $\mathcal{A}$ to impersonate U_i in a polynomial time using the trapped messages. A similar logic also holds for impersonating CG_k and IN_j for generating valid messages MSG_2 and MSG_3, respectively, in polynomial time.
2) *CG Impersonation Attack:* Consider an active attacker $\mathcal{A}$ tries to capture the transmitted messages between CG_k and IN_j such as $MSG_2 = \{GI_1, GI_2, M_x, TS_2\}$ during the execution of the protocol. If $\mathcal{A}$ tries to impersonate

CG_k, $\mathcal{A}$ needs to produce MSG_2 with valid credentials to IN_j. But due to the lack of knowledge on the CG_k's private key, Master secret key, ID_i, SK_{CG-BRC}, and G_1, it is computationally expensive task for the attacker to impersonate CG_k in polynomial time from the trapped messages.

3) *IoT Node Impersonation Attack:* Consider an active attacker $\mathcal{A}$ tries to capture the transmitted messages between U_i and IN_j such as $MSG_3 = \{DID^*_{IN_j}, NM_2, M_y, TS_3\}$ during the execution of the protocol. If $\mathcal{A}$ tries to impersonate IN_j, $\mathcal{A}$ needs to produce the MSG_3 with valid credentials to U_i. But due to lack of knowledge on the shared secret CG_k and IN_j, ID_i, SK_{CG-BRC}, y, and NM_3 it is computationally expensive task for the attacker to impersonate IN_j in polynomial time from the trapped messages.

As a result, we infer that the proposed UAP-BCIoT resists all the above impersonation attacks.

2) Replay Attack: Consider that $\mathcal{A}$ captures all the transmitted messages $MSG_1 = \{A_3, HID_i, G_2, DID_{IN_j}, M_x, TS_1\}$, $MSG_2 = \{GI_1, GI_2, M_x, TS_2\}$, and $MSG_3 = \{DID^*_{IN_j}, NM_2, M_y, SKV_{ji}, TS_3\}$ between the participants during the login and authentication phase over the public channel. Now, $\mathcal{A}$ may try to replay the messages in order to extract some valuable information from the participants. The validation of the replayed messages will fail as each message is furnished with the participants current timestamp and random number, which will restrict $\mathcal{A}$ to prone the replay attack.

3) Privileged-Insider Attack: As a matter of fact, in reality, the BRC is assumed to be trusted and CG_k is semitrusted. However, due to the unpredictability the user's credentials are not stored any where. Also, the credentials received during the user's registration phase are masked to ensure the randomness. Therefore, $\mathcal{A}$ fails to extract the user's information such as identity, password and biometric information from the transmitted message $\{MID_i, MPW_i\}$ as $MID_i = h(ID_i \| b_i)$ and $MPW_i = h(PW_i \| \sigma_i)$. Thus, though the insider attacker exists in the system, he/she cannot achieve any valuable information as the credentials are computed using one-way hash function and it is also computationally expensive to get some information in polynomial time (see Definition 1). Hence, UAP-BCIoT resists privileged-insider attack.

4) Man-in-the-Middle Attack: Consider that $\mathcal{A}$ captures all the transmitted messages between the participants during the login and authentication phase over the public channel, where $MSG_1 = \{A_3, HID_i, G_2, DID_{IN_j}, M_x, TS_1\}$, $MSG_2 = \{GI_1, GI_2, M_x, TS_2\}$, and $MSG_3 = \{DID^*_{IN_j}, NM_2, M_y, SKV_{ji}, TS_3\}$. Now, $\mathcal{A}$ may try to modify the transmitted messages in order to make the participants believe that the received messages are from the legitimate participants. If $\mathcal{A}$ tries to modify the wadded MSG_1, $\mathcal{A}$ needs to modify A_3, M_x, and G_2 which necessitate the knowledge of MID_i, G_1, G_3, and A_2. The problem remains same with the other wadded messages MSG_2 and MSG_3 where $\mathcal{A}$ cannot modify them without the shared secret key between CG_k and IN_j, and between IN_j and U_i. Furthermore, due to the usage of random numbers and current timestamps, the attempt of this attack becomes impossible. Thus, UAP-BCIoT resists the man-in-the-middle attack.

5) Stolen Mobile Device Attack: Assume that the mobile device MD_i of a legal user U_i is lost/stolen by an attacker $\mathcal{A}$ who can extract the credentials stored on MD_i using the power analysis attacks [22]. However, $\mathcal{A}$ cannot gain any control over the stored credentials as each of the credentials is wadded with collision-resistant one-way hash function (see Definition 1). Also, the credentials received during the U_i's registration phase are masked as $\{MID_i, MPW_i\}$ to ensure the randomness. Therefore, $\mathcal{A}$ fails to extract the U_i's information, such as identity, password and biometric information from the stored information. Thus, UAP-BCIoT resists stolen mobile device attack.

6) Mutual Authentication: In UAP-BCIoT, on receiving the login request MSG_1, CG_k checks the authenticity of the participant U_i by verifying $A_3 \stackrel{?}{=} h((HID_i \oplus MID^*_i) \| MID^*_i \| TS_1 \| A_2)$. Upon successful validation, CG_k authenticates U_i. On receiving the message MSG_2, IN_j checks the authenticity of the participant CG_k by verifying $GI_2 \stackrel{?}{=} h(ID_{IN_j} \| MID_i \| ID_{CG_k} \| TS_2)$. On successful verification, IN_j authenticates U_i indirectly and CG_k directly. In addition, on receiving the response message MSG_3, U_i also checks the authenticity of the IN_j by verifying $NM_2 \stackrel{?}{=} h(MID^*_i \| ID_{IN_j} \| ID_{CG_k} \| M_x \| M_y \| TS_3)$. On successful verification, U_i authenticates CG_k indirectly and authenticates IN_j directly. Moreover, the session key verification happens at the end of U_i to ensure, both U_i and IN_j share the same session key. Thus, the above discussion shows the participants successfully achieve mutual authentication in UAP-BCIoT.

7) Ephemeral Secret Leakage Attack: Based on the CK-adversary model [23], an attacker $\mathcal{A}$ can compromise the session state and secret credentials apart from all the activities permitted under the DY model [21]. In UAP-BCIoT, if only the short term secrets (x, y) are compromised the session key between U_i and IN_j computed as $SK_{ij} = h(A_4 \| MID^*_i \| ID_{IN_j} \| M_x \| M_y) = h(NM_3 \| MID_i \| ID_{IN_j} \| M_x \| M_y) = SK_{ji}$ is not compromised. On the other hand, if only long-term secrets $(MID_i, ID_{CG_k}, ID_{IN_j})$ are compromised, the session key SK_{ij} is not also compromised due to computationally infeasibility of ECDDHP (see Definition 2) for deriving $(xy).P$ from M_x and M_y. Hence, without having both 'short term secrets and long-term secrets, it is computationally expensive task for $\mathcal{A}$ to derive the session key SK_{ij}. On the other side, the session key shared between the IoT node IN_j and CG_k is $SK_{kj} = h(TS_2 \| ID_{CG_k} \| MID^*_i \| h(SK_{CG-BRC} \| ID_{IN_j})) = h(TS_2 \| ID_{CG_k} \| MID_i \| IC_{j1}) = SK_{jk}$. However, without having the long-term secrets $(MID_i, ID_{CG_k}, ID_{IN_j}, SK_{CG-BRC})$, it also becomes computationally infeasible task to derive the session key SK_{kj} $(= SK_{jk})$. This shows that UAP-BCIoT is resilient against ESL attack.

8) Physical IoT Node Capture Attack: In an IoT-based ITS environment, it is not always possible to monitor the IoT nodes in 24×7 scenario. This renders the possibility of physical capture of some IoT nodes in the IoT-based ITS environment. Assume that an IoT node, say IN_j is physically compromised. This leads to compromise all the secret credentials (ID_{IN_j}, IC_{j1}) from the physically captured IN_j's memory, where $IC_{j1} = h(SK_{CG-BRC} \| ID_{IN_j})$. Since the identities generated for all the IoT nodes are unique, all the credentials

IC_{j1} for all IoT nodes IN_j are also distinct. This means that the information $(\text{ID}_{\text{IN}_j}, IC_{j1})$ are not useful for constructing the session keys SK_{ik} between a user U_i and other noncompromised IoT nodes IN_k in the IoT-based ITS environment. Therefore, even if some IoT nodes are physically captured, $\mathcal{A}$ cannot compromise the session keys established between the user U_i and other noncompromised IoT nodes IN_k. Hence, UAP-BCIoT is resilient against physical IoT node capture attack.

9) Anonymity and Untracability: Consider that $\mathcal{A}$ captures all the transmitted messages MSG_i $(i = 1, 2, 3)$ among the participants during the login and authentication phase over the public channel. But without the secret credentials x, y, MID_i, G_1, b, and X_{CG_k}, the identities of the participants $(\text{ID}_i, \text{ID}_{\text{CG}_k}, \text{ID}_{\text{IN}_j})$ cannot be extracted. It is also computationally expensive for $\mathcal{A}$ to derive the identities of the participants from the transmitted messages. Furthermore, each wadded message is dynamic in nature involving the randomness because of the involvement of random numbers and current timestamps. This shows that $\mathcal{A}$ cannot identify the actual identities of the participants, and also fails to trace the participants. Thus, UAP-BCIoT restricts traceability and also ensures anonymity.

VI. Formal Security Verification Through AVISPA Tool: Simulation Study

This section illustrates the simulation study of UAP-BCIoT through the formal security verification using the widely accepted AVISPA tool [6]. The simulation results of a security protocol tested under AVISPA tool assure whether "it is safe against active attacks, such as replay and man-in-the-middle attacks." In AVISPA, there are four backends, namely, on-the-fly model-checker (OFMC), constraint logic-based attack searcher (CL-AtSe), sat-based model-checker (SATMC), and tree automata based on automatic approximations for the analysis of security protocols (TA4SP). The tested security protocol is first implemented using the role-oriented language, called the high-level protocol specification language (HLPSL) [6]. The intermediate format (IF) is produced after translation of HLPSL code using the HLPSL2IF translator. Finally, the IF is given as an input to one of the available four backs to produce the output format (OF). When the analysis of a tested security protocol has been successful (by noticing an attack or not), the OF specifies definitely what is the result, and under what criteria it has been acquired. In OF, the following sections are there [6].

1) The first section (SUMMARY) indicates that "whether the tested protocol is safe, unsafe, or whether the analysis is inconclusive."
2) The second section (DETAILS) specifies "under what condition the tested protocol is declared safe or what conditions have been used for finding an attack, or finally why the analysis was inconclusive."
3) Other sections (PROTOCOL, GOAL, and BACKEND) are "the name of the protocol, the goal of the analysis, and the name of the backend used," respectively.

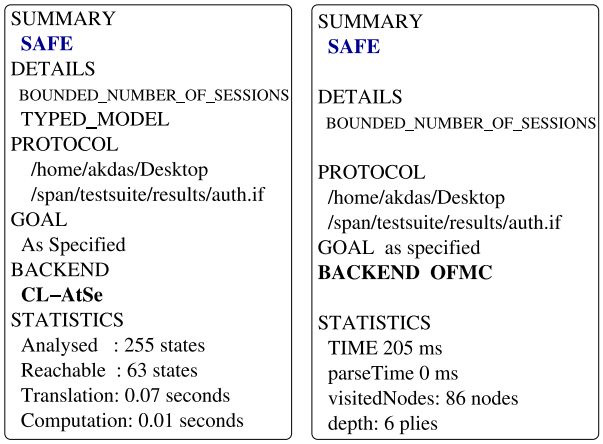


Fig. 6. Analysis of simulation results under CL-AtSe and OFMC backends.

4) At the end, "after some comments and statistics, the trace of an attack (if any) is also printed in the standard Alice-Bob format."

A detailed treatment on AVISPA and its HLPSL implementation can be also found in [6].

In UAP-BCIoT, three basic roles for U_i, CG_k, and IN_j are implemented. The composition roles (session and goal & environment) are always the mandatory roles which specify various scenarios involving the defined basic roles. In AVISPA, the executability check for nontrivial HLPSL specifications is an important part due to the following reason. There may be some modeling mistakes where a protocol model cannot execute to completion. As a consequence, the backends may not be able to search for an attack in case the protocol model cannot reach to a state where the attack can occur. It is worth noticing that an intruder (i) also participates in the execution of a protocol as a concrete session. AVISPA implements the DY model [21], and as a result, the backends are able to check replay and man-in-the-middle attacks. Under the broadly accepted SPAN (Security Protocol ANimator for AVISPA) tool [38], the simulation results illustrated in Fig. 6 ensure that both replay and man-in-the-middle attacks are protected in the proposed UAP-BCIoT.

VII. Comparative Analysis

A detailed comparative study among the proposed UAP-BCIoT and other relevant ECC-based authentication mechanisms in the IoT environment, such as the schemes of Li *et al.* [17], Porambage *et al.* [11], Porambage *et al.* [12], and Banerjee *et al.* [19], has been conducted based on the security & functionality features, computation costs and communication costs during the login and authentication phases. Note that Porambage *et al.*'s scheme [12] compromises two schemes (Scheme-1 and Scheme-2) that are briefly described in Section II. Both the schemes of Porambage *et al.* [11], [12] are based on the ECC cryptographic technique and also these are applicable for wireless sensor networks-based IoT applications, where a registered user can access real-time information directly from the IoT nodes in the IoT deployment. Li *et al.*'s scheme [17] is based on ECC cryptographic technique, while

TABLE IV
COMPARISON OF SECURITY AND FUNCTIONALITY FEATURES

Attributes	[17]	[11]	[12]	[19]	UAP-BCIoT
A_1: "Online/offline password guessing attack"	√	−	−	√	√
A_2: "Privileged-insider attack"	√	×	√	√	√
A_3: "User anonymity preservation"	√	×	×	×	√
A_4: "Traceability preservation"	√	√	×	√	√
A_5: "Stolen mobile device/ smart card attack"	√	−	−	√	√
A_6: "Man-in-the-middle attack"	√	×	√	√	√
A_7: "Replay attack"	√	×	×	√	√
A_8: "Impersonation attacks"	√	×	√	√	√
A_9: "Denial-of-service attack"	√	×	√	√	√
A_{10}: "Mutual authentication"	√	√	√	√	√
A_{11}: "IoT node capture attack"	√	×	√	√	√
A_{12}: "User mobile device revocation"	×	−	−	√	√
A_{13}: "Password/biometric update"	×	−	−	√	√
A_{14}: "Known session key attack"	×	×	×	√	√
A_{15}: "Formal security verification using AVISPA/ProVerif simulation"	√	√	×	√	√
A_{16}: "IoT node credential validation"	×	×	×	×	√
A_{17}: "Big Data analytics"	×	×	×	×	√

√: a scheme "supports an attribute or resists an attack"; ×: a scheme "does not support an attribute or it does not resist an attack"; −: not applicable in a scheme.

TABLE V
COMPARISON OF COMMUNICATION COSTS

Scheme	No. of messages	Communication cost (in bits)
Li *et al.* [17]	4	2720
Porambage *et al.* [11]	4	1344
Scheme-1 [12]	4	3360
Scheme-2 [12]	2	1136
Banerjee *et al.* [19] (without revocation)	3	2304
Banerjee *et al.* [19] (with revocation)	3	2560
UAP-BCIoT	3	2656

Banerjee *et al.*'s scheme [19] is based on the symmetric encryption/decryption technique and applicable for the IoT deployment.

A. Security and Functionality Features Comparison

In Table IV, the security and functionality features of UAP-BCIoT with other relevant schemes [11], [12], [17], and [19] have been compared with respect to fifteen attributes ($A_1 - A_{15}$). It is worth noting that UAP-BCIoT provides better security and more functionality attributes as compared to other existing schemes [11], [12], [17], [19]. Most importantly, our proposed scheme (UAP-BCIoT) only supports IoT node credential validation and big data analytics phases as discussed in Sections IV-I and IV-H, respectively, while none of other existing competing compared schemes does not support these important features.

B. Communication Cost Comparison

We assume identity, random nonce, timestamp, certificate [signature using elliptic-curve digital signature algorithm (ECDSA)] [39], hash output (if we apply SHA-1 as $h(\cdot)$ [29]), a ciphertext block (if AES-128 symmetric encryption) and message authentication code (MAC) require 160, 160, 32, 320, 160, 128, and 160 b, respectively. It is further assumed that the security of 160-b ECC is equivalent to that for 1024-bit RSA cryptosystem [40]. Therefore, an elliptic-curve point of the form $P = (P_x, P_y)$ demands $(160 + 160) = 320$ bits. In Table V, the communication overheads needed for UAP-BCIoT and other schemes [11], [12], [17] have been compared. In UAP-BCIoT, the messages MSG_1, MSG_2, and MSG_3 demand for $(160 + 160 + 320 + 160 + 320 + 32) = 1152$ b, $(160 + 160 + 320 + 32) = 672$ b, and $(160 + 160 + 320 + 160 + 32) = 832$ b, respectively, which together incur the cumulative communication cost as $(1152 + 672 + 832) = 2656$ bits. It is clear from Table V that UAP-BCIoT needs less cost as compared to the Scheme-1 [12] and Li *et al.*'s scheme [17]. Though the schemes of Porambage *et al.* [11] and Scheme-2 [12] demand less cost as compared to our UAP-BCIoT, our proposed scheme provides better security and more functionality attributes as compared to other schemes including these schemes.

TABLE VI
COMPUTATION COST COMPARISON

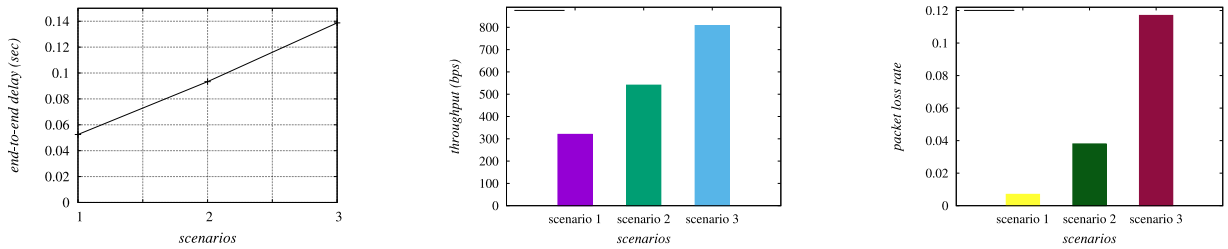
Scheme	Total computation cost	Approximate time (in milliseconds)
Li *et al.* [17]	$19T_h + 6T_{ecm}$	108.68
Porambage *et al.* [11]	$6T_h + 4T_{ecm} + 2T_{eca}$	79.12
Scheme-1 [12]	$18T_h + 15T_{ecm} + 4T_{eca}$	279.86
Scheme-2 [12]	$14T_h + 8T_{ecm} + 3T_{eca}$	154.48
Banerjee *et al.* [19]	$19T_h + 10T_{sed} + T_{fe}$	159.58
UAP-BCIoT	$35T_h + 11T_{ecm} + T_{fe} + 2T_{eca}$	225.20

C. Computation Cost Comparison

Based on the existing experimental results reported from [14], we consider T_{sed} (time required for symmetric encryption/decryption) ≈ 0.0087 s, T_h (time to execute one-way hash function) ≈ 0.00032 s, T_{ecm} (time to execute ECC point multiplication) ≈ 0.0171 s, T_{eca} (time to execute ECC point addition) ≈ 0.0044 s, and T_{fe} (time to execute fuzzy extractor *Gen*/*Rep* function) $\approx T_{ecm}$. In the test environment (CPU: 2.4 GHz, RAM: 4.0 G), the experiment was run 100 times in order to obtain the average approximate execution time. Comparative analysis on computation costs among UAP-BCIoT and other schemes tabulated in Table VI shows that the number of bits needed for transmission of messages during the login and authentication phases in UAP-BCIoT, and the schemes of Banerjee *et al.* [19], Li *et al.* [17], and Porambage *et al.* [11], [12] (Scheme-1 and Scheme-2) are 159.58, 108.68, 79.12, 279.86, 154.48 and 225.20 milliseconds, respectively. It is clear from Table VI that UAP-BCIoT performs better as compared to the Scheme-1 [12]. However, UAP-BCIoT provides better security and more functionality attributes as compared to other schemes [11], [12], [17].

VIII. PRACTICAL DEMONSTRATION: NS2 SIMULATION

The pragmatic study of UAP-BCIoT is performed with the help of widely used NS2 2.35 simulator [41]. For conducting the experimentation, we used the Ubuntu 18.04.4 LTS platform. We computed and analyzed some important network performance parameters, for instance, end-to-end delay (EED)



(a) (b) (c)

Fig. 7. Simulation results for (a) EED, (b) network throughput, and (c) packet loss rate.

TABLE VII
DETAILS OF SIMULATION PARAMETERS

Parameter	Description
Platform	Ubuntu 18.04 LTS
Scenarios taken	1, 2 and 3
Total users (U_i)	$3, 5, 8$ for scenarios $1, 2, 3$
Total cloud gateway nodes (CG_k)	1 for all scenarios
Total IoT nodes (IN_j)	50 for all scenarios
Simulation time	1800 seconds

(in seconds), "throughput (in bps)," and "packet loss rate" for the presented UAP-BCIoT.

A. Details of Simulation Parameters

Table VII consists of the summary of various simulation parameters. Simulation is conducted for 1800 s, i.e., 30 min. The remaining parameters are taken with their standard default values used in NS2. There are three different scenarios in the pragmatic study where one cloud gateway node CG_k and 50 IoT nodes IN_js in all scenarios. Furthermore, Scenarios 1 (Sc_1), 2 (Sc_2), and 3 (Sc_3) consist of three, five, and eight users, respectively. In all scenarios, different communicating parties exchange the following types of messages: 1) $\{A_3, HID_i, G_2, DID_{\text{IN}_j}, M_x, TS_1\}$ from U_i to CG_k; 2) $\{GI_1, GI_2, M_x, TS_2\}$ from CG_k to IN_j; and 3) $\{DID^*_{\text{IN}_j}, NM_2, M_y, SKV_{ji}, TS_3\}$ from IN_j to U_i, and they are of sizes 1152, 672, and 832 b, respectively.

B. Discussions on Obtained Results

We have computed and analyzed network performance parameters (i.e., EED (in seconds), throughput (in bps), and packet loss rate) for the proposed UAP-BCIoT.

1) Effect on End-to-End Delay: *EED* is the estimation of average time required by the data packets (messages) to reach at the destination point from the source point. *EED* can be computed by using the formula: $\sum_{i=1}^{\nu_{pkt}}(\delta_{RC_i}-\delta_{SN_i})/\nu_{pkt}$, where δ_{RC_i} and δ_{SN_i} are the receiving and sending time of a packet i, respectively. Here, ν_{pkt} represents the total number of packets. Fig. 7(a) contains the details of various values of *EED* under different scenarios for the proposed UAP-BCIoT. The *EED*s values are 0.05249, 0.09329 and 0.13871 s under scenarios: Sc_1, Sc_2 and Sc_3, respectively. It is noticed that the *EED* values increase with the increasing number of users (for example, from Sc_1 to Sc_2 and Sc_2 to Sc_3). It happens because the increment in the number of users originates with more number of exchanged messages, which further causes congestion. Therefore, *EED* increases from Sc_1 to Sc_2 and Sc_2 to Sc_3. Yet the increment in *EED* values is not that high as the proposed UAP-BCIoT is based on the lightweight cryptographic operations.

2) Effect on Throughput: The throughput is the estimation of the number of bits transmitted per unit time in a network communication. Fig. 7(b) consists of various values of throughput (in bps) of the proposed UAP-BCIoT for different considered scenarios. The throughput is estimated as $(\nu_r \times |\varpi|/\delta_D)$, where δ_D, $|\varpi|$, and ν_r represent the total time (in seconds), the size of a packet, and the total number of received packets, respectively. We have taken 1800 s as the simulation time, which is δ_D. The simulated values of throughput are 319.96, 540.82 and 808.09 bps for scenarios: Sc_1, Sc_2, and Sc_3, respectively. The throughput values increase from Sc_1 to Sc_2 and from Sc_2 to Sc_3. Since the scenarios: Sc_2 and Sc_3 contain increasing number of users, they cause the exchange of more messages.

3) Effect on Packet-Loss Rate: The packet-loss rate is the estimate of the total number of packets lost per unit time during a network communication. The values of the packet loss rate under different considered scenarios are provided in Fig. 7(c). The packet loss rate values are 0.007, 0.038 and 0.117 bps for scenarios: Sc_1, Sc_2, and Sc_3, respectively. The value of packet loss rate increases from Sc_1 to Sc_2 and also from Sc_2 to Sc_3." Since the Sc_2 and Sc_3 contain increasing number of users, they cause the exchange of more messages to incur congestion in the network. Thus, the packet-loss rate increases from Sc_1 to Sc_2 and from Sc_2 to Sc_3. However, increment in packet-loss rate is not that high as the proposed UAP-BCIoT is lightweight.

IX. CONCLUSION

In this work, an effective and robust three-factor user authentication scheme has been proposed for big data gathering in the IoT-based ITS environment (UAP-BCIoT). UAP-BCIoT permits an authorized registered user to access the real-time information directly from some designated IoT nodes. The fuzzy extractor technique was applied for local biometric verification, and the biometric secret key along with user's identity and password are used in UAP-BCIoT to provide more security. After the enrollment of IoT nodes and CG by the trusted BRC, and also registration process of user by the BRC, the user having the mobile device with necessary credentials

can authenticate a designated accessible IoT node via the CG for establishing a session key between them for maintaining secure communication. The data of IoT nodes can be transmitted to cloud servers in a secure way through the cloud gateway node using the authentication and key agreement mechanism. The proposed authentication and key agreement scheme (UAP-BCIoT) is useful in such scenarios because the real-time accessed data from the IoT nodes in the vehicles can be later securely stored at the cloud too. The stored data is then used for the big data analytics. A detailed security analysis based on the defined threat model, including the formal security analysis using ROR model, informal security analysis, and formal security verification under the AVSIPA software tool proved that UAP-BCIoT can defend various known attacks. Moreover, the conducted comparative study revealed that UAP-BCIoT provides a better tradeoff among the security and functionality features, communication, as well computation costs with relevant existing schemes. In addition, the practical demonstration of proposed UAP-BCIoT was also provided to measure its impact on the network performance parameters.

In the future, we would like to implement UAP-BCIoT including big data analytics in the real-world environment.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers and the Associate Editor for their valuable feedback on this article which helped them to improve its quality as well as presentation.

REFERENCES

[1] G. Glissa and A. Meddeb, "6LowPSec: An end-to-end security protocol for 6LoWPAN," *Ad Hoc Netw.*, vol. 82, pp. 100–112, Jan. 2019.

[2] P. Papadimitratos, A. L. Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, "Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation," *IEEE Commun. Mag.*, vol. 47, no. 11, pp. 84–95, Nov. 2009.

[3] N. M. S. Kumar, T. Eswari, P. Sampath, and S. Lavanya, "Predictive methodology for diabetic data analysis in big data," *Procedia Comput. Sci.*, vol. 50, pp. 203–208, 2015.

[4] S. Muthuramalingam, A. Bharathi, S. R. kumar, N. Gayathri, R. Sathiyaraj, and B. Balamurugan, *IoT Based Intelligent Transportation System (IoT-ITS) for Global Perspective: A Case Study*. Cham, Switzerland: Springer Int., 2019, pp. 279–300.

[5] M. Ge, H. Bangui, and B. Buhnova, "Big data for Internet of Things: A survey," *Future Gener. Comput. Syst.*, vol. 87, pp. 601–614, Oct. 2018.

[6] AVISPA. (2019). *Automated Validation of Internet Security Protocols and Applications*. Accessed: Feb. 2019. [Online]. Available: http://www.avispa-project.org/

[7] M. Abdalla, P. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proc. 8th Int. Workshop Theory Practice Public Key Cryptography (PKC)* vol. 3386. Les Diablerets, Switzerland, 2005, pp. 65–84.

[8] A. K. Das, S. Zeadally, and D. He, "Taxonomy and analysis of security protocols for Internet of Things," *Future Gener. Comput. Syst.*, vol. 89, pp. 110–125, Jun. 2018.

[9] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. Rodrigues, "Authentication in cloud-driven IoT-based big data environment: Survey and outlook," *J. Syst. Archit.*, vol. 97, pp. 185–196, Aug. 2019.

[10] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," *Ad Hoc Netw.*, vol. 20, pp. 96–112, Sep. 2014.

[11] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Istanbul, Turkey, 2014, pp. 2728–2733.

[12] P. Porambage, A. Braeken, C. Schmitt, A. Gurtov, M. Ylianttila, and B. Stiller, "Group key establishment for enabling secure multicast communication in wireless sensor networks deployed for IoT applications," *IEEE Access*, vol. 3, pp. 1503–1511, 2015.

[13] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Netw.*, vol. 36, pp. 152–176, Jan. 2016.

[14] S. Challa *et al.* "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, pp. 3028–3043, 2017.

[15] W.-L. Tai, Y.-F. Chang, and W.-H. Li, "An IoT notion-based authentication and key agreement scheme ensuring user anonymity for heterogeneous ad hoc wireless sensor networks," *J. Inf. Security Appl.*, vol. 34, pp. 133–141, Jun. 2017.

[16] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 269–282, Feb. 2018.

[17] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ECC-based provable secure authentication protocol with privacy preserving for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3599–3609, Aug. 2018.

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

[19] S. Banerjee *et al.*, "A provably-secure and lightweight anonymous user authenticated session key exchange scheme for Internet of Things deployment," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8739–8752, Oct. 2019.

[20] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's law in passwords," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2776–2791, Nov. 2017.

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

[22] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.

[23] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT'02)*, Amsterdam, The Netherlands, 2002, pp. 337–351.

[24] M. Wazid, A. K. Das, N. Kumar, and A. V. Vasilakos, "Design of secure key management and user authentication scheme for fog computing services," *Future Gener. Comput. Syst.*, vol. 91, pp. 475–492, Feb. 2019.

[25] A. Dua, N. Kumar, A. K. Das, and W. Susilo, "Secure message communication protocol among vehicles in smart city," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4359–4373, May 2018.

[26] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Trans. Depend. Secure Comput.*, vol. 17, no. 2, pp. 391–406, Mar./Apr. 2020.

[27] S. Challa, A. K. Das, P. Gope, N. Kumar, F. Wu, and A. V. Vasilakos, "Design and analysis of authenticated key agreement scheme in cloud-assisted cyber-physical systems," *Future Gener. Comput. Syst.*, vol. 108, pp. 1267–1286, Jul. 2020.

[28] M. Wazid, A. K. Das, V. K. Bhat, and A. V. Vasilakos, "LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment," *J. Netw. Comput. Appl.*, vol. 150, Jan. 2020, Art. no. 102496.

[29] *Secure Hash Standard*, document FIPS PUB 180-1, National Institute of Standards and Technology, U.S. Dept. Commerce, Washington, DC, USA, Apr. 1995. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[30] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. Adv. Cryptol. (Eurocrypt)*, vol. 3027. Interlaken, Switzerland, 2004, pp. 523–540.

[31] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, "Verification and validation techniques for streaming big data analytics in Internet of Things environment," *IET Netw.*, vol. 8, no. 3, pp. 155–163, 2019.

[32] Y. Sun, H. Song, A. J. Jara, and R. Bie, "Internet of Things and big data analytics for smart and connected communities," *IEEE Access*, vol. 4, pp. 766–773, 2016.

[33] M. Marjani *et al.*, "Big IoT data analytics: Architecture, opportunities, and open research challenges," *IEEE Access*, vol. 5, pp. 5247–5261, 2017.

[34] D. Wang, D. He, P. Wang, and C. H. Chu, "Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment," *IEEE Trans. Depend. Secure Comput.*, vol. 12, no. 4, pp. 428–442, Jul./Aug. 2015.
[35] S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay, and J. J. Rodrigues, "Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications," *IEEE Trans. Ind. Informat.*, vol. 15, no. 1, pp. 457–468, Jan. 2019.
[36] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6903–6916, Jul. 2019.
[37] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1953–1966, Sep. 2015.
[38] AVISPA. (2019). *SPAN, the Security Protocol ANimator for AVISPA*. Accessed: Feb. 2019. [Online]. Available: http://www.avispa-project.org/
[39] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Security*, vol. 1, no. 1, pp. 36–63, 2001.
[40] E. Barker, *Recommendation for Key Management*, document SP 800-57, NIST, Gaithersburg, MD, USA, Jan. 2016.
[41] *The Network Simulator-ns-2*. Accessed: Jun. 2020. [Online]. Available: https://www.isi.edu/nsnam/ns/

Jangirala Srinivas (Member, IEEE) received the B.Sc. and M.Sc. degrees from Kakatiya University, Warangal, India, in 2003 and 2008, respectively, the M.Tech. degree from IIT Kharagpur, Kharagpur, India, in 2011, and the Ph.D. degree from the Department of Mathematics, IIT Kharagpur, Kharagpur, in 2017.

He also worked as a Research Assistant with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India. He is currently working as an Assistant Professor with the Jindal Global Business School, O. P. Jindal Global University, Haryana, India. His research interests include blockchain technology and applications, information security, cryptocurrency, supplychain. He has authored 24 papers in international journals and conferences in his research areas.

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, Kharagpur, India, in 1998, 2000, and 2008, respectively.

He is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India. His research area cryptography, network security, blockchain, security in Internet of Things, Internet of Vehicles, Internet of Drones, smart grids, smart city, cloud/fog computing and industrial wireless sensor networks, intrusion detection, blockchain, and AI/ML security. He has authored over 240 papers in international journals and conferences in the above areas, including over 205 reputed journal papers.

Dr. Das was a recipient of the Institute Silver Medal from IIT Kharagpur. He is on the Editorial Board of IEEE SYSTEMS JOURNAL, *Journal of Network and Computer Applications* (Elsevier), *Computer Communications* (Elsevier), *IET Communications*, *KSII Transactions on Internet and Information Systems*, and *International Journal of Internet Technology and Secured Transactions* (Inderscience). He is a Guest Editor of *Computers & Electrical Engineering* (Elsevier) for the special issue on Big Data and IoT in e-healthcare, for *ICT Express* (Elsevier) for the special issue on Blockchain Technologies and Applications for 5G Enabled IoT and for Wireless Communications and Mobile Computing for the special issue on Security and Privacy for Smart Mobile Devices: Attacks, Challenges, and New Designs. He has served as a Program Committee Member in many international conferences. He also severed as one of the Technical Program Committee Chairs for the fisrt International Congress on Blockchain and Applications, Avila, Spain, June 2019, International Conference on Applied Soft Computing and Communication Networks, October 2020, Chennai, India, and second International Congress on Blockchain and Applications, L'Aquila, Italy, October 2020.

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 was working as an Assistant Professor with the Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, India. He is currently working as an Associate Professor with the Department of Computer Science and Engineering, Graphic Era University. He was also a Postdoctoral Researcher with the Cyber Security and Networks Lab, Innopolis University, Innopolis, Russia. His current research interests include security, remote user authentication, Internet of Things, and cloud computing. He has published more than 60 papers in international journals and conferences in the above areas.

Dr. Wazid was a recipient of the University Gold Medal and the Young Scientist Award by UCOST, Department of Science and Technology, Government of Uttarakhand, India. He has also received the recognition of "Best Reviewer of 2019" from *ICT Express* (Elsevier) Journal.

Athanasios V. Vasilakos (Senior Member, IEEE) received the Ph.D. degree from the University of Patras, Patras, Greece.

He is with the School of Electrical and Data Engineering, University of Technology Sydney, Sydney, NSW, Australia, the Department of Computer Science and Technology, Fuzhou University, Fuzhou, China, and the Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden. He has published over 700 technical research papers in leading journals and conferences in his areas of research.

Dr. Vasilakos served or is serving as an Editor for many technical journals, such as the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, IEEE TRANSACTIONS ON CLOUD COMPUTING, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON CYBERNETICS, IEEE TRANSACTIONS ON NANOBIOSCIENCE, IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE, IEEE TRANSACTIONS ON CLOUD COMPUTING, *IEEE Communication Magazine*, *ACM Transactions on Autonomous and Adaptive Systems*, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, and *ACM Transactions on Autonomous and Adaptive Systems*. He is Web of Science Highly Cited Researcher from 2017–2020. He is also the General Chair of the European Alliances for Innovation.