This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2941575, IEEE Access

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

An Authentic-Based Privacy Preservation Protocol for Smart e-Healthcare Systems in IoT

B D Deebak[1], Fadi Al-Turjman[2], Moayad Aloqaily[3], and Omar Alfandi[4]

[1]Vellore Institute of Technology, Vellore, India
[2]Antalya Bilim University, Antalya, Turkey
[3]Gnowit Inc., Ottawa, ON, Canada.
[4]Zayed University, UAE

Corresponding author: B D Deebak (e-mail: deebakbd@gmail.com).

ABSTRACT Emerging technologies rapidly change the essential qualities of modern societies in terms of smart environments. To utilize the surrounding environment data, tiny sensing devices and smart gateways are highly involved. It has been used to collect and analyze the real-time data remotely in all Industrial Internet of Things (IIoT). Since the IIoT environment gathers and transmits the data over insecure public networks, a promising solution known as authentication and key agreement (AKA) is preferred to prevent illegal access. In the medical industry, the Internet of Medical Things (IoM) has become an expert application system. It is used to gather and analyze the physiological parameters of patients. To practically examine the medical sensor-nodes, which are imbedded in the patient's body. It would in turn sense the patient medical information using smart portable devices. Since the patient information is so sensitive to reveal other than a medical professional, the security protection and privacy of medical data are becoming a challenging issue of the IoM. Thus, an anonymity-based user authentication protocol is preferred to resolve the privacy preservation issues in the IoM. In this paper, a Secure and Anonymous Biometric Based User Authentication Scheme (SAB-UAS) is proposed to ensure secure communication in healthcare applications. This paper also proves that an adversary cannot impersonate as a legitimate user to illegally access or revoke the smart handheld card. A formal analysis based on the random-oracle model and resource analysis is provided to show security and resource efficiencies in medical application systems. In addition, the proposed scheme takes a part of the performance analysis to show that it has high-security features to build smart healthcare application systems in the IoM. To this end, experimental analysis has been conducted for the analysis of network parameters using NS3 simulator. The collected results have shown superiority in terms of the packet delivery ratio, end-to-end delay, throughput rates, and routing overhead for the proposed SAB-UAS in comparison to other existing protocols.

INDEX TERMS Authentication and key agreement, Internet of Medical Things, security protection and privacy user authentication, random-oracle model and resource analysis, e-healthcare application, Biometric

I. INTRODUCTION

Internet of Things (IoT) composes of various physical sensors or devices/virtual objects that are interconnected to share information over the public networks. The physical objects or devices can be a sensor, smart device, camera, drone or vehicle, and the virtual objects can be a book, electronic ticket or wallet. In IoT, the connective things or objects should be made to be smart to-do an ingenious decision without human interference [1]. As a result, the IoT objective is to integrate a computer-based physical system to improve the accuracy of social-environmental systems. Gartner Inc. [2] predicts that there will be around 8.4 billion IoT devices to connect across the world. IoT devices can generally be a semi-structured or unstructured in nature [3], which may be an essential property of 5V big-data namely volume, velocity, variety, veracity and value. The generated data volume is stored in the cloud, i.e. an on-demand and effective storage medium [4]. In today's world, technological development adopts the quality IoT features to attain a high degree of production and complete the task via fewer attempts. And thus, our world is converging more towards the IIoT. IoT convergence can be applied to various industries, namely transportation, energy/utilities, logistics, manufacturing, mining, metals, oil, gas, and aviation [5].

In accordance with market analysis and academic experts, it can be defined as the next innovation wave to optimize the environmental resources. In the use of a sensor or virtual objects, IIoT advances intelligent decision-making and data

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2941575, IEEE Access

analytics to transform the industrial assets. Therefore, the industries connect the intelligent device or machine to predict that the IoT markets will extend to $123.89 billion by 2021 [6]. Lately, Advancement of wireless communication technologies has deeply been functioning for the evolution of various sensors-based application systems such as environmental test, automobile industries, electronic health care, military, Internet of connected vehicles [7], drone deployment, etc. [8].

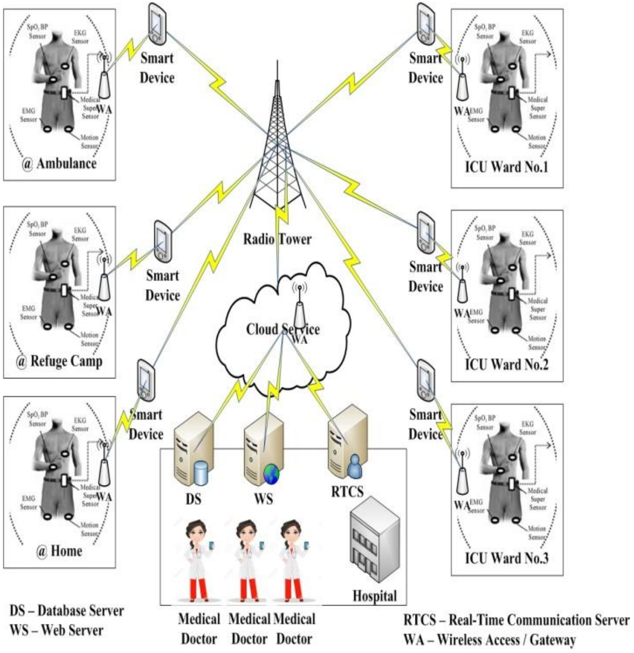

Fig. 1. A system model of Internet of Medical Things

An electronic healthcare system has a wireless medical sensor network, which has lightweight resources with limited memory, bandwidth, and processing power [9]. The medical sensors such as ECG, blood pressure, pulse oximeter, temperature, etc. are generally deployed in a patient's body to form a heterogeneous wireless body area network. They sense and collect the physiological information about patients to transmit over a wireless communication channel which is usually provided to medical professional smart devices, i.e. iPhone, Laptop, PDA, implantable medical-devices, etc. [9,10]. Therefore, it is claimed that the medical professional may read or consider the assessment for a broader examination as and when it is demanded to process.

A typical system model of IoM for hospital environment is shown in Fig. 1 as demonstrated in [11] to analyze the security and performance issues. This system includes patient, medical professional / practitioner, medical sensors, system database, gateway and server that are used to offer incredible application benefits namely large-scale medical monitoring, causality emergency medical tracking and responses. Since data transmission is insecure over public networks, the protection of the medical sensor is so significant to prevent data tampering. In healthcare application system, the security and privacy of patient's data are one of the biggest concern to adopt wireless communication technologies, namely wireless gateway access, mobile computing device and medical sensor [12]. Medical sensor nodes are deployed in the Patient's body to read the physiological information. A medical professional/expert can access the sensing data through the authenticated access of a wireless gateway. Upon mutual authentication, the communication entities such as medical sensor and experts share a secret session key to establish secure communication. As a result, it is addressing the issue of user authentication problem that becomes a significant research area in the field of wireless sensor networks (WSNs) [11-14]. Table I define the important abbreviations used in this paper.

Table I Important Abbreviation Used

Abbreviation	Description
IoT	Internet of Things
5V	Volume, Velocity, Variety, Veracity And Value
IIoT	Industrial Internet of Things
AKA	Authentication and Key Agreement
IoM	Internet of Medical Things
SAB-UAS	Secure and Anonymous Biometric Based User Authentication Scheme
ECG	Electrocardiogram
PDA	Personal Digital Assistant
WSN	Wireless Sensor Networks
RSA	Rivest–Shamir–Adleman
DH	Diffie-Hellman
DoS	Denial of Service
ECC	Elliptic Curve Cryptosystem
BAN	Burrows Abadi Needham
ECDF	Elliptic-Curve Discrete Logarithm
ECDH	Elliptic-Curve Diffie-Hellman
ECF	Elliptic-Curve Factorization
DDH	Decision Diffie-Hellman
WDH	Weak Diffie-Hellman
CFH	Collision-Free Hash
PDR	Packet Delivery Ratio
ETE	End-to-End
TTR	Throughput Transmission Rate
RTO	Routing Overhead

A. *MOTIVATIONS*

An extensive effort has been committed to the development of secure user authentication schemes; however, there is no significant outcome to achieve better security and privacy. As referred to [15], some security goals are afar to attain by the use of existing cryptosystems. It is evident that an improved or extended version of the authentication scheme is recommended to improve the security efficiencies of any application systems. In literature, very few papers have considered the systematic design and evaluation for security and performance analysis. On the other hand, most of the authentication schemes have found to be unsuitable for the achievement of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2941575, IEEE Access

security goals and its significant features. As a result, there is no distinctive quality of authentication scheme to provide a secure and efficient user authentication scheme.

Several improved versions of authentication schemes have been introduced for various application systems, however, most of the schemes have found to be unsuitable to claim the security goals. The crucial points lie in how to accomplish the goals such as providing two-factor security even if the smartcard is lost or tampered and securing password update. Huang et al. [14] have addressed more challenging issues. Lately, Madhusudhan et al. [15] have found a problem of intractability for the design techniques of two-factor cryptosystems. In the literature, two-factor user authentication guarantees that the user can choose his/her password invariably to draw password space P_S uniformly. Since this assumption is unrealistic, it may cause an effect of misconception. As an instance, the above assumption claims that the smartcard parameters have been extracted by an adversary A_{dv}.

A probability of A_{dv} success is precisely set as $(1\ P_S)$ in an attempt of one online-guessing attack. When a secure user authentication protocol is applied, a two-factor strategy P_S ensures that an active online-guessing is the best way to diffuse various attack vectors such as replay, parallel-session, offline password-guessing, etc. Specifically, A_{dv} the optimal benefit is meant to infiltrate the threat attacking on P_S, which is not larger than $Q_{Send} = P_S + \epsilon$, where Q_{Send} denotes the number of online impersonation attacks attempted by A_{dv} and ϵ denotes a negligible-value. On the other hand, user-chosen passwords are frequently far and wide from uniform distributed. In order to provide a defensive mechanism, the proposed SAB-UAS scheme introduces a fuzzy verifier, which can timely infer user's smartcard depravity. As a result, it can prevent an online-guessing attack to provide seemliness intractability addressed in [17].

B. MAJOR CONTRIBUTIONS

In this work, a substantial thought is made to investigate the underlying adversarial model that tries to eliminate the deficiencies such as redundancies, insufficiencies, ambiguities, etc. using the evaluation criteria set. As for systematic methodology, a broad set of 12 independent criteria is characterized to analyze the practical capabilities of adversary model. Though it is completely not available to examine, it is expected to provide a solid analysis of requirement definition. Thus, this paper presents a secure-anonymous biometric-based user authentication scheme (SAB-UAS) not only to perform smart revocation/reissue, but also to achieve better security efficiencies using a formal security model. In SAB-UAS, a long-standing usability-security conflict is provided to address the traditional optimal-bound security $Q_{Send} = P_S + \epsilon$. The major contributions are summarized as follows:

1. Initially, a systematic framework consisting of practical adversarial models and selection criteria is suggested to evaluate secure-anonymous biometric-based user authentication scheme.
2. Secondly, a defensive strategy of the fuzzy verifier is introduced to provide timely access, which is helpful to detect smartcard deprivation in order to prevent potential attacks and seemliness intractability.
3. Thirdly, the proposed SAB-UAS scheme proves that it can satisfy the selection criterion to show the strength of security efficiencies.
4. Lastly, the formal and the informal security analysis demonstrate that the proposed scheme can achieve better security and performance efficiencies to prove its significance for smart healthcare systems in comparison with other existing schemes [61-63].

C. PAPER ORGANIZATION

This paper organizes the sections as follows: Section II briefly explains the authentication schemes related to IoT and IIoT environment. Section III discusses the elliptic-curve cryptosystems, fuzzy extractor, threat assumption, and security properties to signify the use of proposed SAB-UAS scheme. Section IV presents a secure-anonymous biometric-based user authentication scheme (SAB-UAS) using a smartcard for smart electronic healthcare application systems. Section V demonstrates a formal proof using the random-oracle model, informal and performance analysis to prove the security efficiency of proposed SAB-UAS scheme. Section VI demonstrates the practical scenario of proposed SAB-UAS with other authentication protocols using NS3 simulation. Section VII concludes this research work.

II. RELATED WORKS

For data confidentiality and secure communication, various authentication schemes [11-14] have been introduced. However, a security issue in relation to password-based authentication is preserving a password table to verify whether the user is legitimate or not. Moreover, it requires an additional memory space to store the password database. For the easiness of storage overhead, several researchers have suggested an alternative solution of fingerprint or iris. As uniqueness, it is providing a storage benefit to operate a smartcard calculation at more than one security level. Watro [17] et al. introduced a secure authentication protocol based on RSA and DH for WSNs. Wong et al. [18] presented a hash-based dynamic authentication scheme to resist various potential attacks, namely man-in-the-middle, replay, forgery, and key impersonation. However, Das et al. [19] demonstrated that their schemes are susceptible to the privileged-insider attack and in addition, they proposed an improved version to achieve better security efficiencies.

Yoon and Kim [20] proposed a biometric-based user authentication scheme to prevent security vulnerabilities such as poor repairability, denial of service (DoS) and sensor impersonation attack. Choi et al. [21] shown that

Table II Summary of Technique Used, Drawbacks, Formal Analysis Model and Simulation Used of Existing Authentication Schemes

Existing Scheme	**Year of Publication**	**Technique Used**	**Drawback**	**Formal Analysis Model**	**Simulation Used**
Li et al. [28]	2018	Lightweight RFID Mutual Authentication [Reader With Cache]	It cannot be resilient to the potential attacks such as reader-impersonation, tag-forgery and message eavesdropping.	No	No
Li et al. [29]	2017	Improved Secure Authentication [With Data Encryption and User Anonymity]	It cannot be resilient to the potential attacks such as denial-of-service, privileged-insider and key impersonation	No	No
Li et al. [30]	2018	Secure 3PAKE Protocol Using Chebyshev Chaotic Maps [With Random Oracle Model]	It cannot be resilient to the various potential attacks such as password disclosure, offline password guessing and key impersonation.	No	No
Gope et al. [33]	2018	Lightweight Privacy Preservation Protocol [Using Physically Uncloneable Functions (PUFs)]	It may cause several key issues such as perfect secrecy, large computation and storage cost.	Yes	No
Al-Turjman et al. [34]	2017	Seamless Key Agreement Framework [For Mobile-Sink and IoT-Based Cloud-Centric Network]	It cannot be resilient to the various potential attacks such as denial-of-service, password disclosure, offline password guessing and key impersonation.	Partial	No
Deebak et al [35]	2019	Hash-Based RFID Authentication [For Context-Aware IoT]	It cannot be resilient to the potential attacks such as denial-of-service, privileged-insider and data forgery.	Yes	Yes
Wazid et al. [36]	2018	Secure Lightweight Three-Factor Remote User Authentication [Using Smartcard, Password and Personal Biometrics]	It cannot be resilient to the potential attacks such as smartcard forgery and message eavesdropping and denial-of-service.	Yes	No
Roy et al. [37]	2017	Anonymous User Authentication Using Chaotic Map [With Biometrics and Fuzzy Extractor]	It may cause several key issues such as partial perfect secrecy, large computation and storage cost.	Yes	No
Wazid et al. [38]	2017	Secure Authentication For Medicine Anti-Counterfeiting System	It cannot be resilient to the potential attacks such as smartcard forgery and message eavesdropping and denial-of-service.	Yes	No
Al-Turjman et al. [39]	2018	Seamless Identity Provisioning Framework [With Mutual Authentication Approach]	It cannot be resilient to the potential attacks such as smartcard forgery and message eavesdropping, man-in-the-middle and denial-of-service.	No	No

Yoon and Kim failed to provide the security issues, namely user verification problem, user anonymity, biometric recognition, session key exposure, DoS attack, key revocation, and perfect forward secrecy. For the betterment of security efficiencies, they have extended biometric-based user authentication scheme and also found that their schemes are more secure than the other authentication and key agreement schemes. Unfortunately, Park et al. [22] shown that Choi et al. scheme is still insecure to key impersonation attack. Since WSNs are dealing with various environmental systems, any adversaries can physically infer or capture the sensor information from the sensor memory.

Using extract information of capture sensor node, an adversary may try to damage the entire medical sensor networks. As a consequence, it is measured as potential vulnerabilities for WSNs and Medical Sensor Networks as well. At first, Lamport [23] introduced the password-based authentication protocol. In the past, several authentication protocols have been proposed [24-39]. Chang et al. [24] applied elliptic-curve cryptosystem to design a lightweight authentication protocol. They developed an ECC-based authentication to achieve the property of forward secrecy. Yeh et al. [25] constructed a two-factor authentication scheme based ECC for WSNs. However, their scheme could not achieve the primary goal of security requirement i.e. proper mutual authentication. Additionally, Shi et al. [26] found that the Yeh et al scheme is not secure. Later, Choi et al. [27] demonstrated that Shi et al. scheme is susceptible to secure key sharing, stolen smartcard, and sensor-energy exhaustion attack. The attack known as the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2941575, IEEE Access

sensory - energy plays a crucial role to apply energy consumption issue to limit the lifetime of a sensor node. To address the issue of sensor-energy exhaustion, Choi et al. enhanced the Shi et al. scheme. However, their scheme could not preserve user anonymity and untraceability of communication entities. Li et al. [27] presented an RFID-based authentication protocol for IoT. Their protocol supports an explicit mutual authentication to protect the privacy of real-time entities, i.e. reader, tag and database server. In addition, Li et al. [28] extended their authentication protocol to overcome the security drawbacks of previous mechanism, i.e. IoT based medical-care. This improved version provides better client anonymity to prevent replay and data disclosure attack. Later, Li et al. [30] developed a three-party user authentication protocol, which applies the Chebyshev and Chaotic-Map to prove the property of client anonymity. Hameed et al. [31] presented a security protocol based on integrity mechanism to handle the data integrity in IoT-based WSNs through the knowledge of gateway access i.e. base station. Al-Turjman et al. [32] constructed a cloud-integrated architecture to support mobile-edge, IoT and cloud computing services such as scalability, reliability and feature adaptability.

Al-Turjman et al. [34] designed seamless key agreement framework in IoT based cloud-centric network. Deebak et al. [35] presented a hash-based RFID authentication for context-aware IoT. Furthermore, Li et al. [37] developed an ECC-based authentication protocol for IIoT environment, which applies the biometric-key features to authenticate the service access. Challa et al. [1] presented an ECC-based user authentication mechanism for future IoT applications. However, their scheme consumes more computation and communication overhead in comparison with non-ECC based authentication mechanism. Wazid et al. [36] developed a secure lightweight authentication for IoT networks. Their scheme uses biometric, smart card and password as a three-factor to comply with key agreement properties. Later, Roy et al. [37] proposed a new user authentication protocol for crowdsourcing IoT. Their scheme claims the user anonymity in the use of biometric - templates. Wazid et al. [38] built a new authentication mechanism for medical counterfeit systems that uses this scheme to verify the authenticity of pharmaceutical i.e. dosage forms. Al-Turjman et al. [39] proposed a seamless mutual authentication protocol for IIoT to claim the feature of context-sensitive awareness. From the literature, the security features and its related drawbacks were studied well. Accordingly, a secure-anonymous biometric-based user authentication scheme (SAB-UAS) is presented to suit the IIoT environment. Table II summarizes the technique used, drawback, formal analysis and simulation used of existing authentication schemes.

III. SECURITY MODEL & ASSUMPTIONS

This section discusses the elliptic-curve cryptosystem, fuzzy extractors, threat assumption, and security properties.

A. ELLIPTIC-CURVE CRYPTOSYSTEM

At first, Koblitz [40] and Miller [41] have proposed this cryptosystem. It is widely used in several user authentication schemes [4-12] to provide better security efficiency. An elliptic-curve E_C is represented over a field $K \neq 2 \, or \, 3$ of the characteristics to set the solution $(x, y) \in K^2$ to the solved equation as follows:

$$Y^2 = x^3 + ax + b \, , \forall \, a, b \in K \tag{1}$$

Where $4a^3 + 27b^2 \neq 0$

Assume that the elliptic-curve cryptosystem is based on $G_F(q)$ that can translate the systems using elliptic-curve group EC_g. It is defined over $G_F(q)$ to consider k times of P additional points i.e. for the scalar point multiplications $KP = (P + P + \cdots + P, K \; times)$. For given E_C, two points such as $P, Q \in E_C$ are defined over $G_F(q)$ that is used to find an integer value x such that $Q = x.P$, if any value of x exists. Importantly, this strategy is proven to be intractable than discrete logarithm. The definitions of E_C can be referred in [14]. The most significant computational problems based on E_C are given in below:

Definition 1: In elliptic-curve discrete logarithm (ECDF) problem, two given elements $Q, R \in G_P$ are used to find an integer value $k \in [1, N-1]$ such that $R = k.Q$.

Definition 2: In the elliptic-curve Diffie-Hellman (ECDH) problem, three given elements (P, aP, bP) for any $a, b \in [1, N-1]$ are used to find the computation of abP, which is extremely hard for the elliptic group G_P.

Definition 3: In the elliptic-curve factorization (ECF) problem, two given elements $P, Q \in G_P$, where $Q = sP + tP$ and $(s, t) \in [1, N-1]$ are used to find the computation of sP and tP that is impossible to calculate in practice.

Definition 4: In decision Diffie-Hellman (DDH) problem, four given elements (P, aP, bP, cP) for any $(a, b, c) \in [1, N-1]$ are used to decide whether $cP = abP$ i.e. $ab \; mod \; P$ or not.

Definition 5: In a weak Diffie-Hellman (WDH) problem, three given elements $(P, Q, kP)$are used to compute kQ, $Q \in G_P$ for any $k \in [1, N-1]$ that is practically hard to determine.

Definition 6: In a collision-free hash (CFH) problem, a given hash-value $H(.)$ is very hard to invert when there is computationally infeasible to determine the input x such that $H(a) = h$.

A collision resistant hashing i.e. strong collision-free H is one, which is computationally infeasible to determine any two message transmission a and b such that $H(a) = H(b)$.

B. FUZZY EXTRACTOR

This subsection discusses the fundamental concepts of a biometric-based fuzzy extractor, which translates the biometric data into random values. As referred to [42], two formal procedure such as $\{G_{EN}, R_{EP}\}$ are considered for the fuzzy extractor. The procedural mechanism of $\{G_{EN}, R_{EP}\}$ is demonstrated as follows:

1. $G_{EN}(B_{IO}) \rightarrow \langle R, P \rangle$; and
2. $R_{EP}(B^*_{IO}, P) = R$, if B^*_{IO} is closely associated with B_{IO}

G_{EN} is a probabilistic function, which has a biometric input-output B_{IO} to extract the string $R \in \{0,1\}^l$ and its auxiliary string $P \in \{0,1\}^*$. R_{EP} is a deterministic reproduction, which is used to recover string R from auxiliary string P i.e. any vector B^*_{IO} closed to B_{IO}. The details of fuzzy extraction are also referred to [43].

C. THREAT ASSUMPTION

Dolev-Yao [42] and other threat models [44] is basically introduced to consider a threat of side-channel attack that constructs the threat assumptions. They are as follows:

A. An adversary A_{dv} can either be a sensor node, medical professional/expert or wireless gateway. In addition, any registered / legitimate user can also be possible to act as an adversary.

B. An adversary A_{dv} can overhear any communication over public insecure networks. Therefore, any data transmission can be leaked or captured between the communication entities such as sensor node, medical professional/expert or wireless gateway.

C. Importantly, an adversary A_{dv} may alter or delete or reroute the captured data.

D. An adversary A_{dv} may extract the information from smartcard SM_c to analyze the card power storage capacity.

In the conventional password authentication and key agreement (PAKA) protocol, A_{dv} is modeled to provide complete control over the communication channel between the real-time communication entities [45]. To characterize the qualities of forward-secrecy, A_{dv} may allow corrupting validity of communication parties to infer the long-term secret key. In addition, A_{dv} may obtain previous session keys in order to examine improper erasure. Recent analysis has proven that the extraction of security parameters could be deduced to experience power-analysis attack], software-loophole [46] and reverse engineering. The leakage of sensitive information may lead to security vulnerabilities such as offline password-guessing [34] and impersonation attack [35]. It is also evident that the stored session key in smartcard may be intercepted to experience malicious card-reader attack [14]. However, the attacker can intercept the storage key via card-reader to read the user's secret information through stolen or lost smartcard.

This may enable the attackers to intercept any secure authentication scheme, though it adheres with extreme adversary principles [47]. It uses robust security to protect against adversarial activities that would trivially break any types of user authentication schemes. The above treatment is as follows: 1. the malicious user may break terminal access to underway an attack of side-channel; and 2. an attacker may leak the sensitive information of legal user within a short time interval. This analysis tries to invalidate overly-conservative proposition that may simply presume a smartcard to be an external memory card using an embedded microcontroller to perform a cost-effective operation, supported by security schemes. As memory-card based authentication scheme is completely insecure over public networks, all the memory-card based authentication schemes [16] were truly insecure over un-trusted terminals. Therefore, the conditional assumption of non-tamper resistive is more secured than extreme assumption referred to [17].

In SAB-UAS scheme, the capabilities of A_{dv} are summarized in Section II-B. The previous works provide a new insight to fairly evaluate the integrity of the proposed scheme. Wang et al. [48] introduced three types of security model such as Type-I, Type-II and Type-III. Of which Type-III is more influential to make use in practice. The brief descriptions are as follows:

Type – I: A_{dv} has a full-control of a communication channel, which is inconsistent.

Type – II: Smartcard is non-tampered resistant and user's password may be secretly listened over a communication channel using malicious card-reader by A_{dv}. The former is more consistent than the latter assumption.

Type – III: Smartcard has no security protection i.e. A_{dv} may distribute numerous queries to learn useful information of users using the malicious card-reader attack.

In regard to threat assumption C, it is argued that this assumption might not be of much practical importance to validate whether it is practically applicable or not to ensure its security relevance. On the other hand, the input password is verified before the execution of smartcard to learn useful information of corresponding remote-server that may lock the legal user account. If the above verification exists, then A_{dv} can always detect a user's password using a malicious card –reader. The key conflict is that A_{dv} of Type-III is not exclusively defined in threat assumption C and D. As referred in [48], this may minimally assume the counter protection to infer whether the lock time-period exceeds the threshold limit or not. According to the above verification, the proposed SAB-UAS model is very close to Type-III model in [49]. As a result, Type-III may not provide the security features such as forward-secrecy and known-key attack. According to Yang et al. [16], the proposed SAB-UAS has explicitly considered the malicious card-reader and A_{dv} is further specified with threat assumptions C and D.

In SAB-UAS A_{dv} model, it is assumed to be able to offline-guessing that is enumerated of $\{\mathrm{U_{ID}}, \mathrm{Ad_i}\}$ pair in the product of Cartesian $\{D_{ID} \times D_{AD}\}$ with polynomial time. It is enabled to deal with potential security features [34-37] such as resilient to offline-password guessing, undetectable online-password guessing, etc. Note that the threat assumption of B has yet been explicitly made in [34], which do not consider the security feature of user anonymity, whereas the proposed SAB-UAS model becomes stronger in practical aspect to incorporate previous and new assumption to provide a robust and secure authentication protocol.

D. SECURITY PROPERTIES

As referred in Yang et al. [16], the constructive analysis shows that the smartcard-based user authentication schemes have a common set of security properties to adopt the efficiencies of user authentication protocols. Madhusudhan and Mittal [15] demonstrated that an earlier set of security properties has ambiguities and redundancies, and thus they presented nine different sets of security goals along with ten desirable features. Since the security goals are based on the assumption of non-tamper resistance, their authentication scheme is set to be superior. However, it is still having the challenging issues to notice inherent security conflicts among set criteria. The security properties are as follows:

- **C.1 No Password Verifier-Table:** The server system does not maintain a verifier database to store user-password or derive a value of user passwords.
- **C.2 Password Friendliness:** The user passwords are memorable and can be opted generously to change user passwords.
- **C.3 No-Password Exposure:** The user passwords cannot be derived by the server administrator.
- **C.4 No Smartcard Loss Attack:** The scheme is completely free from smartcard loss attack i.e. unauthorized user acquiring a legal user card should not be able to change the password of smartcard easily or recover the victim's password by means of online, offline, hybrid password guessing or key impersonate attack to login in to the server systems, even if the smartcard is obtained or revealed to incur the secret-data.
- **C.5 Resilient To Known-Key Attack:** The scheme can be resilient to various potential attacks comprising of offline password-guessing, replay, parallel-guessing, de-synchronization, stolen-verifier, key-impersonation, unknown key-share, and key-control and known-key.
- **C.6 Sound Repairability:** The smartcard tries to provide smartcard revocation with reasonable repairability i.e. a legitimate user may revoke his/her smartcard without changing their identities.
- **C.7 Provision of User Key-Agreement:** The client and server can establish a common secret session-key for secure data communication between the real-time entities during the system authentication phase.
- **C.8 No Clock Synchronization:** The scheme is not easily prone time delay and synchronization i.e. the server does not need to synchronize its clock time with the input devices utilized by smartcard and vice versa.
- **C.9 Timely Based Typo-Detection:** The user can timely notify if he/she enters a wrong password by fault when login being accessed.
- **C.10 Proper Mutual Authentication:** The user and server can mutually verify the authentication of each other.
- **C.11 User Anonymity:** The authentication scheme can defend or protect the user activities to save from intractability.
- **C.12 Forward - Secrecy:** The scheme can try to achieve the property of perfect forward secrecy.

It is evidently pointing out that criterion set – C4 provides the attacking scenario where A_{dv} has acquired the smartcard access while C5 has no gain of access to victim's smartcard. The criterion set - C4 assumes a traditional smartcard reissue to reveal user's smartcard access using the random-oracle model. The criterion set – C5 is completely based on basic attacks [15,16] that a password related authentication scheme is well guarded on new attack vectors e.g. stolen verifier addressed in two-factor authentication systems. It is demonstrated that the criterion is set to eliminate redundancies and ambiguities of the traditional authentication system in order to facilitate concreteness based cryptanalysis. Further, the efficiency of the proposed authentication scheme may be contingent upon the implementation of real-time environmental systems. An extensive comparison proves that the proposed adversarial model is so hard and the criterion sets are more concrete and comprehensive in comparison with existing schemes.

Table III Important Notations of SAB-UAS Scheme

Notation	Description
M_E	Medical Expert
WG_{Ac}	Wireless Gateway Access
MS_j	Medical Sensor
$m_x \ and \ m_y$	Master Key
$\mathrm{U_{ID}}$	User Identity
$\mathrm{BT_i}$	Biometric Template
SM_I	Smart Card
$\mathrm{C_R}$	Card Reader
r_1 and r_2	Random Number
TS_i	Current Timestamp
$\mathrm{U_{sr}}$	User
US_K	User Session Key
$H(.)$	Collision free one-way hashing
$\mathrm{G_{EN}(BT_i)}$	One part of fuzzy extraction with biometric-key $\mathrm{R_i}$ and string helper $\mathrm{P_i}$
$\mathrm{R_{EP}\left(B^*_{IO_i}, P_i\right)}$	One part of fuzzy extraction with biometric-key $\mathrm{R_i}$ in $\mathrm{G_{EN}(BT_i)}$
$\rightarrow$	Insecure Channel
$\|$	String Concatenation
$\oplus$	Bitwise XOR operation

IV. PROPOSED SAB-UAS SCHEME

This section presents a secure-anonymous biometric-based user authentication scheme (SAB-UAS) using smartcard. In SAB-UAS, three communication entities namely medical expert M_E, wireless gateway access WG_{Ac} and medical sensor MS_j. WG_{Ac} generates two master keys such as $m_x \ and \ m_y$ and transmits a long-term secret key $H\left(S_{ID_j} \parallel m_y\right)$ to M_S before the SAB-UAs scheme initiates its execution process. Then, WG_{Ac} tries to compute $m_x.P$, which is considered as a gateway's public key. The proposed SAB-UAS scheme is composed of three phases namely user registration, system login, authentication and revocation/reissue. The important notation of SAB-UAS is shown in Table III.

A. USER REGISTRATION PHASE

This phase chooses a user identity U_{ID} that imprints a biometric template BT_i on U_{sr} to perform the following execution.

Step1: M_S initiates BT_i to extract $\langle R_i, P_i\rangle$ from $G_{EN}(BT_i) \rightarrow \langle R_i, P_i\rangle$ and then stores the values P_i in the memory storage. Upon P_i storage, M_S sends $\langle U_{ID}, Ad_i = H(R_i)\rangle$ to WG_{Ac} over a secure communication channel.

Step2: After receiving the registration request $\langle U_{ID}, Ad_i\rangle$ from M_S, WG_{Ac} computes the user authentication parameters that are as follows:

$$C_I = H(U_{ID} \parallel m_x \parallel m_y); \tag{2}$$

$$MS_I = H(C_I) \oplus Ad_i; \tag{3}$$

$$N_I = m_x \oplus C_I \oplus m_y; \tag{4}$$

$$VR_I = H(U_{ID} \parallel Ad_i) \tag{5}$$

Step3: WG_{Ac} stacks the user authentication parameters namely MS_I, N_I, VR_I and $H(.)$ into smartcard SM_I. WG_{Ac} then issues SM_I to M_S over a secure communication channel.

Step4: Finally, M_S stores P_i into smartcard.

B. SYSTEM LOGIN AND AUTHENTICATION PHASE

This phase performs a login phase for U_{sr}; and thus the entities such as WG_{Ac}, U_{sr} and MS_j use a common session key to authenticate each other. The authentication step between U_{sr} and MS_j are as follows:

Step1: U_{sr} inserts his/her SM into the card-reader C_R that reads the user identity U_{ID} to imprint his/her biometric information B^*_{IO} at M_S.

Step2: M_S then initiates B^*_{IO} to extract R_i from $R_{EP}(B^*_{IO_i}, P_i) \rightarrow \langle R_i\rangle$. Then, SM_I computes ${Ad_i}^*$ and ${VR_I}^*$ using a fuzzy extractor. Lastly, it compares ${VR_I}^*$ with VR_I that is as follows:

$R^*_i = R_{EP}(B^*_{IO_i}, P_i)$; ${Ad_i}^* = H(R^*_i)$; ${VR_I}^* = H(U_{ID} \parallel {Ad_i}^*)$; then Verifies, whether $VR_I == {VR_I}^*$ or not

Step3: SM_I generates two random numbers r_1 and r_2 to compute:

$$Y_i = r_1 \times P; \tag{6}$$

$$H(C_I) = MS_I \oplus {Ad_i}^*; \tag{7}$$

$$AD_i = U_{ID} \oplus H(r_2); \tag{8}$$

$$MS_1 = r_2 \oplus H(C_I); \tag{9}$$

$$MS_2 = H(AD_i \parallel H(C_I) \parallel Y_i \parallel r_2 \parallel TS_i) \tag{10}$$

$$MS_3 = N_i \oplus (r_1 \times xP) \tag{11}$$

Where TS_i is the current timestamp. U_{sr} sends the login request $\{AD_i, Y_i, MS_1, MS_2, MS_3, TS_i\}$ to WG_{Ac}.

Step4: After receiving a login request from U_{sr}, WG_{Ac} tries to retrieve TS' and verifies $(TS' - TS_i) \leq \Delta TS$. If the verification is valid, then WG_{Ac} computes C^*_I, r^*_2, ID^*_i and MS^*_2 to compare C^*_I with $H(ID^*_i \parallel m_x \parallel m_y)$. The comparison of MS^*_2 with MS_2 is as follows:

$$C^*_I = MS_3 \oplus (m_x \times Y_i) \oplus m_x \oplus m_y; \; r^*_2 = MS_1 \oplus H(r^*_2); \tag{12}$$

$$ID^*_i = AD_i \oplus H(r^*_2) \tag{13}$$

After the successful generation of C^*_I, the expression $H(ID^*_i \parallel m_x \parallel m_y)$ is examined to check whether it is valid or not. Then, the generated MS^*_2 is validated with MS_2 to analyze its equality measure. If the above analysis is valid, then WG_{Ac} verifies the legitimacy of U_{sr}.

Step5: WG_{Ac} tries to compute the parameters such as K_g, C_g and $W_g$to validate whether the communication is authenticated or not between U_{sr} and MS_j. The expressions are as follows:

$$K_g = H(H(SD_j \parallel m_y) \parallel TS_g) \tag{14}$$

$$C_g = EC_{kg}(AD_i \parallel r_2 \parallel Y_i); \tag{15}$$

$$W_g = H(H(SD_j \parallel m_y) \parallel AD_i \parallel C_g \parallel TS_g) \tag{16}$$

Where TS_g is the current data timestamp. WG_{Ac} then tries to send the user authentication message $\{AD_i, C_g, TS_g, W_g\}$ to MS_j.

Step6: After the successful authentication message from WG_{Ac}, MS_j tries to retrieve TS'' in order to verify whether $(TS'' - TS_g) \leq \Delta TS$. If the verification holds, then MS_j examines the W_g validation to compare with $H(H(SD_j \parallel m_y) \parallel AD_i \parallel C_g \parallel TS_g)$ to verify the legitimacy of WG_{Ac}. Then, MS_j checks whether AD_i equates with AD^*_i or not to execute the following equation:

$$K^*_g = H(H(SD_j \parallel m_x) \parallel TS_g) \tag{17}$$

$${D_{Kg}}^* = AD^*_i \parallel r^*_2 \parallel Y^*_i \tag{18}$$

After a successful generation of K^*_g and D_{Kg}, AD_i compares with AD^*_i to validate the user authentication message.

Step7: MS_j generates a random number r_n that computes KS_U, Z_i, R_M and Vf_s to create a user session key US_K. The computation is as follows:

$$KS_U = r_n \times Y^*_i; \; Z_i = r_n \times P \tag{19}$$

$$US_K = H(AD_i \parallel KS_U \parallel TS) \tag{20}$$

$$R_M = \text{Query Response of } U_{sr} \tag{21}$$

$$Vf_s = H(AD_i \parallel r^*_2 \parallel Z_i \parallel US_K \parallel R_M \parallel TS) \tag{22}$$

Where TS is the current data timestamp. MS_j sends the communication parameters $\{R_M, Z_i, Vf_s, TS\}$ to U_{sr}.

Step8: After receiving the message $\{R_M, Z_i, Vf_s, TS\}$ from MS_j, U_{sr} computes US_K to validate whether ${Vf_s}^*$equates Vf_s or not. The computation is as follows:

$$KS_U = r_1 \times Z_i; \; US_K = H(AD_i \parallel KS_U \parallel TS) \tag{23}$$

$${Vf_s}^* = H(AD_i \parallel r_2 \parallel Z_i \parallel US_K \parallel R_M \parallel TS) \tag{24}$$

Lastly, the legitimate user U_{sr} computes KS_U and US_K to establish a secure communication US_K.

C. REVOCATION / REISSUE PHASE

To compensate the smart card loss or long-term key disclosure, the loss or tampered smartcard should be periodically revoked or reissued at a cyclic basis.

Step1: Assume that U_{sr} wishes to revoke his/her SM. To execute this scenario, he/she should insert their SM_I to generate a new identity ${U_{ID}}^*$ from the previous identity U_{ID} to prevent the adversaries act. Then, the successful update of ${U_{ID}}^*$ imprints the user biometric $B^*_{IO_i}$ on MS_j.

Step2: $\mathrm{MS_j}$ initiates $\mathrm{B^*_{IO_i}}$ to extract $\mathrm{R_i}$ from $\mathrm{R_{EP}}\left(\mathrm{B^*_{IO_i}}, \mathrm{P_i}\right) \rightarrow \langle \mathrm{R_i} \rangle$. Subsequently, $\mathrm{SM_I}$computes $\mathrm{Ad_i}^*$ and $\mathrm{VR_I}^*$ using a fuzzy extractor.

$\mathrm{R_i} = \mathrm{R_{EP}}\left(\mathrm{B^*_{IO_i}}, \mathrm{P_i}\right)$; and $\mathrm{Ad_i} = \mathrm{H}(\mathrm{R^*_i})$

Step3: $\mathrm{U_{sr}}$ computes $\mathrm{Z_i} = \mathrm{U_{ID_i}} \oplus \mathrm{MS_i}$ to send the revocation/reissuing request message parameters $\left\{\mathrm{U_{ID_i}}, \mathrm{U_{ID_i}}^*, \mathrm{Ad_i}, \mathrm{Z_i}\right\}$ via $\mathrm{WG_{Ac}}$over a secure communication channel.

Step4: $\mathrm{WG_{Ac}}$ initially validates whether $\mathrm{U_{ID}}$ is similar to $\mathrm{U_{ID_i}}^*$ or not. If the similarity is not held, then $\mathrm{WG_{Ac}}$ tries to compute $\mathrm{MS^*_i}$and $\mathrm{Z^*_i}$ to validate the legitimacy of user $\mathrm{U_{sr}}$. The computation is as follows:

$\mathrm{C^*_I} = \mathrm{H}\left(\mathrm{U^*_{ID}} \parallel \mathrm{m_x} \parallel \mathrm{m_y}\right)$; and $\mathrm{Z^*_i} = \mathrm{U_{ID}} \oplus \mathrm{H}(\mathrm{C_I}) \oplus \mathrm{Ad_i}$.

The verification of $\mathrm{Z^*_i}$ with $\mathrm{Z_i}$ is employed to prove user legitimacy.

Step5: if the user legitimacy holds, $\mathrm{WG_{Ac}}$ revokes $\mathrm{U_{ID_i}}$ and update the same in the revocation lookup table. Consequently, $\mathrm{WG_{Ac}}$determines new computation parameters $\{\mathrm{Vf_i}, \mathrm{N_i}, \mathrm{C_I}\}$. The expressions are as follows:

$\mathrm{C_I} = \mathrm{H}\left(\mathrm{U_{ID}} \parallel \mathrm{m_x} \parallel \mathrm{m_y}\right)$; $\mathrm{MS_i} = \mathrm{H}(\mathrm{C_I}) \oplus \mathrm{Ad_i}$

$\mathrm{N_i} = \mathrm{m_x} \oplus \mathrm{C_I} \oplus \mathrm{m_y}$; $\mathrm{Vf_i} = \mathrm{H}(\mathrm{U^*_{ID}} \parallel \mathrm{Ad_i})$

Step6: $\mathrm{WG_{Ac}}$stacks $\mathrm{H}(.)$ and new authentic parameters $\{\mathrm{MS_i}, \mathrm{N_i}, \mathrm{Vf_i}, \mathrm{H}(.)\}$ in the storage of smartcard $\mathrm{SM_I}$. Then, $\mathrm{WG_{Ac}}$newly issue $\mathrm{SM_I}$ to $\mathrm{U_{sr}}$ through a secure communication channel.

Step7: Finally, $\mathrm{U_{sr}}$ stores the details of $\mathrm{P_i}$ in to the smartcard SM.

V. FORMAL SECURITY ANALYSIS OF PROPOSED SAB-UAS

This section demonstrates a formal proof using the random-oracle model that proves the security efficiency of proposed SAB-UAS scheme. A collision-free one-way hash function is considered to specify the significance of random value r_2 and master secret session-keys m_x and m_y of WG_{Ac}.

Assume that a function of collision-free one-way hashing is defined as: $f: \{0,1\}^* \rightarrow \{0,1\}^n$. It has an input binary string $\mathrm{a} \in \{0,1\}^*$, which has a random binary to produce a length of $H(a) \in \{0,1\}^n$. It can satisfy the requirements as follows:

Given that $b \in B$, but it couldn't find the computational of $a \in A$ such that $b = H(a)$

Given that $a \in A$, but it couldn't find the computational of $a' \neq a \in A$ such that $H(a') = H(a)$

It is not fortunate that the computation couldn't determine about a string pair $(a', a) \in A' \times A$ with $a' \neq a \in A$ such that $H(a') = H(a)$.

Theorem 1: It is assumed that the collision-free one-way hash function $H(.)$ closely represents a formal random based oracle model. The proposed SAB-UAS scheme distinctively proves that the secure session key US_K protects the sensitive information including user identity $\mathrm{U_{ID}}$, random binary-string r_2 and master secret-key m_x and m_y of WG_{Ac} to prevent any adversaries.

TABLE IV: ALGORITHM $Exp^{SAB-UAS}_{Hash,Ad}$

```
Eavesdropping of user login request message
    $\langle Ad_i, Y_i, MS_1, MS_2, MS_3, TS_i \rangle$ during the system login phase
Call Random-Oracle Model to Reveal: let
    $\langle Ad^*_i, H(C_I)^*, MS^*_1, r^*_2, TS^*_i \rangle \leftarrow Reveal\ (MS_2)$
If $Ad_i{}^* == Ad_i$ then
    Accept $\langle H(C_I)^*, MS^*_1, r^*_2, TS^*_i \rangle$ as a corrective format of $U_{sr}$.
    Call Random-Oracle Model to Reveal: let
    $(C^*_I) \leftarrow Reveal\ (H(C_I)^*)$
    Call Random-Oracle Model to Reveal: let
    $(C^{**}_I) \leftarrow Reveal\ (MS_1 \oplus r_2)$
        If $(C^*_I == C^{**}_I)$ then
        Accept $C_I$ as a corrective format of $U_{sr}$.
        Call Random-Oracle Model to Reveal: let
            $\langle \mathrm{U_{ID}}^*, \mathrm{m^*_x}, \mathrm{m^*_y} \rangle \leftarrow Reveal(C_I)$
        Compute $\mathrm{U_{ID}}^{**} = \mathrm{Ad_i} \oplus \mathrm{H}(\mathrm{r_2})$
            If $(\mathrm{U_{ID}}^* == \mathrm{U_{ID}}^{**})$ then
            Accept $\langle \mathrm{m^*_x}, \mathrm{m^*_y} \rangle$ as the proper secret key
                $\langle m_x, m_y \rangle$ of $WG_{Ac}$
                Return 1 $\langle For\ Success \rangle$
                    Else
                Return 0 $\langle For\ Failure \rangle$
        Else
            Return 0
        End If
    Else
        Return 0
End If
```

Proof: A formal random-oracle model can remove the input key m_x for the given hash function $b = H(a)$ without key failure. A_{dv} runs the executable programs as shown in Table IV. A function $Exp^{SAB-UAS}_{Hash,Ad}$represents a proposed SAB-UAS scheme that defines a success probability.

A success probability of $Exp^{SAB-UAS}_{Hash,Ad}$ is defined as $Success^{SAB-UAS}_{Hash,Ad} = \left|Pr\left[Exp^{SAB-UAS}_{Hash,Ad} = 1\right] - 1\right|$, where $Pr(.)$ represents a probability of $Exp^{SAB-UAS}_{Hash,Ad}$. The adversarial function of this algorithm is written as $Adv^{SAB-UAS}_{Hash,Ad}\left(e_t, Q_{uery}\right)$, where e_t is the time of execution and $Q_{uery}$is the executable number of queries. Assume that A_{dv} has the capabilities to work out the hash functioning problem provided in Definition6, where he/she can immediately try to retrieve the parameters such as user identity $\mathrm{U_{ID}}$, random binary-string r_2 and master secret-key m_x and m_y of WG_{Ac}. In this case, A_{dv} may wish to detect the complete communication between U_{sr} and WG_{Ac}. However, the input inversion from the given hashing is computationally not possible i.e. $Adv^{SAB-UAS}_{Hash,Ad}(e_t) \leq \epsilon, \forall\, \epsilon > 0$.

Therefore, $Adv^{SAB-UAS}_{Hash,Ad}\left(e_t, Q_{uery}\right) \leq \epsilon$ depends on $Adv^{SAB-UAS}_{Hash,Ad}(e_t)$. As A_{dv} has less possibility to detect the complete connection setup between U_{sr} and WG_{Ac}, the proposed SAB-UAS scheme distinctively proves that the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2941575, IEEE Access

secure session key US_K protects the sensitive information from A_{dv} to retrieve $\{\mathrm{U_{ID}}, \mathrm{r_2}, \mathrm{m_x}, \mathrm{m_y}\}$. Hence, the proposed SAB-UAS claims to achieve better security efficiencies.

TABLE V IMPORTANT BAN LOGIC NOTATION

Notation	Description
$P\| \equiv X$	Proposition P believes X that prove formula X is true
$\#\langle X \rangle$	Formula X is true
$P \Longrightarrow X$	Proposition P has a jurisdiction over a formula X
$P \lhd X$	Proposition P has complete control over the formula X. This has reasoning over certificate authorities.
$X: P\|\sim X$	Proposition P has once said the execution of previous protocols that use earlier messages to examine the current protocol.
$\langle X, Y \rangle$	X or Y is a part of $\langle X, Y \rangle$
$\langle X \rangle_Y$	$\langle X \rangle$ combines with Y
$(X)_K$	(X) is a key hashing function K
$P \overset{K}{\rightarrow} Q$	P and Q uses secret session-key K to establish a real-time communication
US_K	A secret session-key is used to authenticate a session
$\dfrac{P\| \equiv P \overset{K}{\leftrightarrow} Q, P \lhd \langle X \rangle_K}{P\| \equiv Q\|\sim X}$	A rule of message-meaning
$\dfrac{P\| \equiv \#(X)}{P\| \equiv \#(X, Y)}$	A rule of freshness concatenation
$\dfrac{P\| \equiv \#(X), P\| \equiv Q\|\sim X}{P\| \equiv Q\| \equiv X}$	A rule of nonce verification
$\dfrac{P\| \equiv Q \Rightarrow X, P\| \equiv Q\| \equiv X}{P\| \equiv X}$	A rule of jurisdiction

A. SECURITY PROOF BASED BAN LOGIC

This subsection uses Burrows Abadi Needham (BAN) logic [50] to demonstrate that the proposed SAB-UAS scheme is completely valid and practically efficient to prevent known-key attacks in order to satisfy the security efficiency of e-healthcare systems. This model has become a well-known formal cryptographic protocol that is widely used to analyze the authentication scheme. The important notations and BAN logical postulates are described in Table V. According to analytical BAN logical procedure, the proposed SAB-UAS scheme shall assure the below goals:

1. $\mathrm{Goal_1}: \mathrm{Usr_i}| \equiv \left(\mathrm{Usr_i} \overset{\mathrm{US_K}}{\longleftrightarrow} \mathrm{WG_{Ac}}\right)$
2. $\mathrm{Goal_2}: \mathrm{Usr_i}| \equiv \mathrm{WG_{Ac}}| \equiv \left(\mathrm{Usr_i} \overset{\mathrm{US_K}}{\longleftrightarrow} \mathrm{WG_{Ac}}\right)$
3. $\mathrm{Goal_3}: \mathrm{WG_{Ac}}| \equiv \left(\mathrm{Usr_i} \overset{\mathrm{US_K}}{\longleftrightarrow} \mathrm{WG_{Ac}}\right)$
4. $\mathrm{Goal_4}: \mathrm{WG_{Ac}}| \equiv \mathrm{Usr_i}| \equiv \left(\mathrm{Usr_i} \overset{\mathrm{US_K}}{\longleftrightarrow} \mathrm{WG_{Ac}}\right)$

Initially, the proposed SAB-UAS scheme is transformed to idealize the message transmissions that are as follows:

1. $\mathrm{M_{sg}1}: \mathrm{Usr_i} \rightarrow \mathrm{D_C}: \{\mathrm{U_{ID_i}}, \mathrm{X}\}_{\mathrm{H}\left(\mathrm{U_{ID_j}} \| \mathrm{m_y}\right)}$
2. $\mathrm{M_{sg}2}: \mathrm{Usr_i} \rightarrow \mathrm{D_C}: \left\{\mathrm{U_{ID_i}}, \mathrm{X}, \mathrm{S_{ID_j}}, \mathrm{Y}\right\}_{\mathrm{H}\left(\mathrm{S_{ID_j}} \| \mathrm{m_y}\right)}$
3. $\mathrm{M_{sg}3}: \mathrm{D_C} \rightarrow$
   $\mathrm{Usr_i}: \langle \mathrm{U_{ID_j}}, \mathrm{S_{ID_j}}, \mathrm{X}, \mathrm{Y}, \mathrm{Usr_i} \overset{\mathrm{Y}}{\leftrightarrow} \mathrm{WG_{Ac}} \rangle_{\mathrm{H}\left(\mathrm{U_{ID_j}} \| \mathrm{m_y}\right)}$
4. $\mathrm{M_{sg}4}: \mathrm{D_C} \rightarrow \mathrm{WG_{Ac}}: \langle \mathrm{U_{ID_j}}, \mathrm{S_{ID_j}}, \mathrm{X}, \mathrm{Y}, \mathrm{Usr_i}$
   $\overset{\mathrm{X}}{\leftrightarrow} \mathrm{WG_{Ac}} \rangle_{\mathrm{H}\left(\mathrm{S_{ID_j}} \| \mathrm{m_y}\right)}$
5. $\mathrm{M_{sg}5}: \mathrm{WG_{Ac}} \rightarrow \mathrm{Usr_i}: \langle \mathrm{U_{ID_j}}, \mathrm{S_{ID_j}}, \mathrm{X}, \mathrm{Y}, \mathrm{Usr_i}$
   $\overset{\mathrm{US_K}}{\longleftrightarrow} \mathrm{WG_{Ac}} \rangle_{\mathrm{US_K}}$
6. $\mathrm{M_{sg}6}: \mathrm{Usr_i} \rightarrow \mathrm{WG_{Ac}}: \langle \mathrm{S_{ID_j}}, \mathrm{U_{ID_j}}, \mathrm{X}, \mathrm{Y}, \mathrm{Usr_i}$
   $\overset{\mathrm{US_K}}{\longleftrightarrow} \mathrm{WG_{Ac}} \rangle_{\mathrm{US_K}}$

Secondly, the following assumptions are made to initiate and analyze the proposed SAB-UAS scheme:

$\mathrm{Asgn_1}: \mathrm{Usr_i}| \equiv \neq (\mathrm{X})$
$\mathrm{Asgn_2}: \mathrm{WG_{Ac}}| \equiv \neq (\mathrm{Y})$
$\mathrm{Asgn_3}: \mathrm{Usr_i}| \equiv \ \mathrm{Usr_i} \xleftrightarrow{\mathrm{H}\left(\mathrm{U_{ID_j}} \| \mathrm{m_y}\right)} \mathrm{D_C}$
$\mathrm{Asgn_4}: \mathrm{D_C}| \equiv \ \mathrm{Usr_i} \xleftrightarrow{\mathrm{H}\left(\mathrm{U_{ID_j}} \| \mathrm{m_y}\right)} \mathrm{D_C}$
$\mathrm{Asgn_5}: \mathrm{WG_{Ac}}| \equiv \ \mathrm{WG_{Ac}} \xleftrightarrow{\mathrm{H}\left(\mathrm{S_{ID_j}} \| \mathrm{m_y}\right)} \mathrm{D_C}$
$\mathrm{Asgn_6}: \mathrm{D_C}| \equiv \ \mathrm{WG_{Ac}} \xleftrightarrow{\mathrm{H}\left(\mathrm{S_{ID_j}} \| \mathrm{m_y}\right)} \mathrm{D_C}$
$\mathrm{Asgn_7}: \mathrm{Usr_i}| \equiv \ \mathrm{D_C} \Longrightarrow \left(\mathrm{Usr_i} \overset{\mathrm{Y}}{\leftrightarrow} \mathrm{WG_{Ac}}\right)$
$\mathrm{Asgn_8}: \mathrm{WG_{Ac}}| \equiv \ \mathrm{D_C} \Longrightarrow \left(\mathrm{Usr_i} \overset{\mathrm{X}}{\leftrightarrow} \mathrm{WG_{Ac}}\right)$
$\mathrm{Asgn_9}: \mathrm{WG_{Ac}}| \equiv \ \mathrm{Usr_i} \Longrightarrow \left(\mathrm{Usr_i} \overset{\mathrm{US_K}}{\longleftrightarrow} \mathrm{WG_{Ac}}\right)$
$\mathrm{Asgn_{10}}: \mathrm{Usr_i}| \equiv \ \mathrm{WG_{Ac}} \Longrightarrow \left(\mathrm{Usr_i} \overset{\mathrm{US_K}}{\longleftrightarrow} \mathrm{WG_{Ac}}\right)$

Thirdly, the idealized form of the proposed SAB-UAS scheme is analyzed using BAN-logic rules and assumptions. The proofs of statements are as follows:

According to $\mathrm{M_{sg}1}$, the expression could be:

$\mathrm{WG_{Ac_1}}: \mathrm{D_C} \lhd \ \{\mathrm{U_{ID_i}}, \mathrm{X}\}_{\mathrm{H}\left(\mathrm{U_{ID_j}} \| \mathrm{m_y}\right)}$

According to $\mathrm{Asgn_4}$, a rule of message-meaning is applied to obtain:

$\mathrm{WG_{Ac_2}}: \mathrm{D_C}| \equiv \ \mathrm{Usr_i}|\sim\left(\mathrm{U_{ID_i}}, \mathrm{X}\right)$

According to $\mathrm{M_{sg}2}$, the expression could be:

$\mathrm{WG_{Ac_3}}: \mathrm{D_C} \lhd \ \left\{\mathrm{U_{ID_i}}, \mathrm{X}, \mathrm{S_{ID_j}}, \mathrm{Y}\right\}_{\mathrm{H}\left(\mathrm{S_{ID_j}} \| \mathrm{m_y}\right)}$

According to $\mathrm{Asgn_6}$, a rule of message-meaning is applied to obtain:

$\mathrm{WG_{Ac_4}}: \mathrm{D_C}| \equiv \mathrm{WG_{Ac}}|\sim\left\{\mathrm{U_{ID_i}}, \mathrm{X}, \mathrm{S_{ID_j}}, \mathrm{Y}\right\}$

According to $\mathrm{M_{sg}3}$, the expression could be:

$\mathrm{WG_{Ac_5}}: \mathrm{Usr_i} \lhd \langle \mathrm{U_{ID_j}}, \mathrm{S_{ID_j}}, \mathrm{X}, \mathrm{Y}, \mathrm{Usr_i} \overset{\mathrm{Y}}{\leftrightarrow} \mathrm{WG_{Ac}} \rangle_{\mathrm{H}\left(\mathrm{U_{ID_j}} \| \mathrm{m_y}\right)}$

According to $\mathrm{Asgn_4}$, a rule of message-meaning is applied to obtain:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2941575, IEEE Access

$$\mathrm{WG_{Ac_6}: Usr_i| \equiv D_C|\sim \langle U_{ID_j}, S_{ID_j}, X, Y, Usr_i \overset{X}{\leftrightarrow} WG_{Ac}\rangle_{H\left(S_{ID_j}\|m_y\right)}}$$

According to $\mathrm{Asgn_3}$, a rule of message-meaning is applied to obtain:

$$\mathrm{WG_{Ac_7}: Usr_i| \equiv D_C| \equiv \langle U_{ID_j}, S_{ID_j}, X, Y, Usr_i \overset{X}{\leftrightarrow} WG_{Ac}\rangle_{H\left(S_{ID_j}\|m_y\right)}}$$

According to $\mathrm{WG_{Ac_7}}$, a rule of BAN-logic is applied to break the conjunction to produce:

$$\mathrm{WG_{Ac_8}: Usr_i| \equiv D_C| \equiv Usr_i \overset{Y}{\leftrightarrow} WG_{Ac}}$$

According to $\mathrm{Asgn_7}$, a rule of jurisdiction is applied to obtain:

$$\mathrm{WG_{Ac_9}: Usr_i| \equiv\ Usr_i \overset{Y}{\leftrightarrow} WG_{Ac}}$$

According to $\mathrm{US_K = x \times Y = xy \times P}$, the expression could be:

$$\mathrm{WG_{Ac_{10}}: Usr_i| \equiv\ Usr_i \overset{Y}{\leftrightarrow} WG_{Ac}}$$

⟨Goal 1⟩

According to $\mathrm{M_{sg}4}$, the expression could be:

$$\mathrm{WG_{Ac_{11}}: WG_{Ac} \lhd \langle U_{ID_j}, S_{ID_j}, X, Y, Usr_i \overset{X}{\leftrightarrow} WG_{Ac}\rangle_{H\left(S_{ID_j}\|m_y\right)}}$$

According to $\mathrm{Asgn_5}$, a rule of message-meaning is applied to obtain:

$$\mathrm{WG_{Ac_{12}}: WG_{Ac}| \equiv D_C|\sim\ \langle U_{ID_j}, S_{ID_j}, X, Y, Usr_i \overset{X}{\leftrightarrow} WG_{Ac}\rangle}$$

According to $\mathrm{Asgn_2}$, a rule of BAN-logic is applied to break the conjunction to produce:

$$\mathrm{WG_{Ac_{13}}: WG_{Ac}| \equiv D_C| \equiv Usr_i \overset{X}{\leftrightarrow} WG_{Ac}}$$

According to $\mathrm{Asgn_8}$, a rule of jurisdiction is applied to obtain:

$$\mathrm{WG_{Ac_{14}}: WG_{Ac}| \equiv Usr_i \overset{X}{\leftrightarrow} WG_{Ac}}$$

According to $\mathrm{US_K = y \times X = xy \times P}$, the expression could be:

$$\mathrm{WG_{Ac_{16}}: WG_{Ac}| \equiv Usr_i \overset{US_K}{\longleftrightarrow} WG_{Ac}}$$

⟨Goal 3⟩

According to $\mathrm{M_{sg}5}$, the expression could be:

$$\mathrm{WG_{Ac_{17}}: Usr_i \lhd\ \langle U_{ID_j}, S_{ID_j}, X, Y, Usr_i \overset{US_K}{\longleftrightarrow} WG_{Ac}\rangle_{US_K}}$$

According to $\mathrm{WG_{Ac_{10}}}$, a rule of message-meaning is applied to obtain:

$$\mathrm{WG_{Ac_{18}}: Usr_i| \equiv\ WG_{Ac}|\sim \langle U_{ID_j}, S_{ID_j}, X, Y, Usr_i \overset{US_K}{\longleftrightarrow} WG_{Ac}\rangle}$$

According to $\mathrm{Asgn_1}$, a rule of freshness concatenation is applied to obtain:

$$\mathrm{WG_{Ac_{19}}: Usr_i| \equiv WG_{Ac}| \equiv \langle U_{ID_j}, S_{ID_j}, X, Y, Usr_i \overset{US_K}{\longleftrightarrow} WG_{Ac}\rangle}$$

According to $\mathrm{WG_{Ac_{19}}}$, a rule of BAN-logic is applied to break the conjunction to produce:

$$\mathrm{WG_{Ac_{20}}:\ Usr_i| \equiv WG_{Ac}| \equiv Usr_i \overset{US_K}{\longleftrightarrow} WG_{Ac}}$$

⟨Goal 2⟩

According to $\mathrm{M_{sg}6}$, the expression could be:

$$\mathrm{WG_{Ac_{21}}: WG_{Ac} \lhd\ \langle U_{ID_j}, S_{ID_j}, X, Y, Usr_i \overset{US_K}{\longleftrightarrow} WG_{Ac}\rangle_{US_K}}$$

According to $\mathrm{WG_{Ac_{16}}}$, a rule of message-meaning is applied to obtain:

$$\mathrm{WG_{Ac_{22}}: WG_{Ac}| \equiv Usr_i|\sim\ \langle U_{ID_j}, S_{ID_j}, X, Y, Usr_i \overset{US_K}{\longleftrightarrow} WG_{Ac}\rangle}$$

According to $\mathrm{Asgn_2}$, a rule of freshness concatenation is applied to obtain:

$$\mathrm{WG_{Ac_{23}}: WG_{Ac}| \equiv Usr_i| \equiv \langle U_{ID_j}, S_{ID_j}, X, Y, Usr_i \overset{US_K}{\longleftrightarrow} WG_{Ac}\rangle}$$

According to $\mathrm{WG_{Ac_{23}}}$, a rule of BAN-logic is applied to break the conjunction to produce:

$$\mathrm{WG_{Ac_{24}}: WG_{Ac}| \equiv Usr_i| \equiv Usr_i \overset{US_K}{\longleftrightarrow} WG_{Ac}}$$

⟨Goal 4⟩

According to ⟨Goal 1⟩, ⟨Goal 2⟩, ⟨Goal 3⟩ and ⟨Goal 4⟩, both $\mathrm{Usr_i}$ and $\mathrm{WG_{Ac}}$ is believed that the secure session key $\mathrm{US_K = xyP}$ is mutually shared between $\mathrm{Usr_i}$ and $\mathrm{WG_{Ac}}$ to adhere to a property of known-key security. Table III describes the important notation of BAN logic.

B. IN-FORMAL SECURITY ANALYSIS

This subsection shows that the proposed SAB-UAS scheme has resiliencies to withstand various potential attacks to achieve better security efficiencies.

Resilient to Privileged-Insider Attack: This attack uses $\mathrm{WG_{Ac}}$to collect the user credentials from data-center $\mathrm{D_C}$ that tries to obtain access to the legitimate user. To resist privileged-insider attack, the credentials of the proposed SAB-UAS scheme $\mathrm{\langle U_{ID}, Ad_i\rangle}$ are securely transmitted. It is masked with a one-way hash function to generate a long-term secret key $\mathrm{H\left(S_{ID_j} \| m_y\right)}$. Moreover, the master keys such as $\mathrm{m_x}$ and $\mathrm{m_y}$ use biometric template $\mathrm{BT_i}$ on $\mathrm{U_{sr}}$ to extract $\mathrm{\langle R_i, P_i\rangle}$ from $\mathrm{G_{EN}(BT_i) \to \langle R_i, P_i\rangle}$ that stores values of $\mathrm{P_i}$ in storage-memory. Assume that legitimate user has lost his/her smartcard $\mathrm{SM_i}$ and $\mathrm{A_{dv}}$ tries to extract the legal information of $\mathrm{U_{sr}}$ such as $\mathrm{\langle MS_I, N_I, VR_I, H(.)\ \rangle}$ using a power-analysis mechanism. However, $\mathrm{A_{dv}}$ cannot infer or extract secret session-key to perform parallel-guessing attack as the master keys such as $\mathrm{m_x}$ and $\mathrm{m_y}$ are not known. Hence, the proposed SAB-UAS scheme claims the resiliency of privileged-insider attack.

Resilient to Stolen Smartcard Attack: Assume that smartcard SM of $\mathrm{U_{sr}}$ maybe stolen or lost. $\mathrm{A_{dv}}$ tries to extract $\mathrm{U_{sr}}$ credential information namely $\mathrm{\langle MS_I, N_I, VR_I, H(.)\ \rangle}$, where $\mathrm{C_I = H\left(U_{ID} \| m_x \| m_y\right)}$; $\mathrm{MS_I = H(C_I) \oplus Ad_i}$; $\mathrm{N_I = m_x \oplus C_I \oplus m_y}$; $\mathrm{VR_I = H\left(U_{ID} \| Ad_i\right)}$ using a power-analysis mechanism. It is evident that $\mathrm{U_{sr}}$ credential information is completely protected using master secret keys $\mathrm{\langle m_x,\ m_y\rangle}$ and biometric template $\mathrm{BT_i}$. Since key-replication or parallel-guessing is computationally hard, key-inference or credential derivative is impracticable. Hence, the proposed SAB-UAS scheme claims the resiliency of stolen smartcard attack.

Resilient to Stolen-Verifier Attack: Assume that $\mathrm{A_{dv}}$ tries to steal $\mathrm{U_{sr}}$ credentials that temporally store information in $\mathrm{WG_{Ac}}$ to perform malicious activities. However, in the proposed SAB-UAS scheme, $\mathrm{WG_{Ac}}$ does not allow $\mathrm{A_{dv}}$ to infer the sensitive information of $\mathrm{U_{sr}}$

related to user identity U_{ID} and biometric template BT_i. Hence, the proposed SAB-UAS scheme claims the resiliency of stolen-verifier attack.

User-Anonymity Preservation: In security application systems, user-anonymity plays a vital role. Therefore, it is highly demanded to strengthen wireless communication technologies and pervasive computing. To protect user identity U_{ID}, the proposed SAB-UAS scheme securely keeps U_{sr} secret information, biometric template and master key $\langle m_x, m_y \rangle$. In addition, it is evident that the transmission messages of proposed SAB-UAS scheme preserve biometric template and master key $\langle m_x, m_y \rangle$ using symmetric-key encryption. Hence, in the proposed SAB-UAS scheme, user identity U_{ID} the derivation is computationally impracticable to achieve the property of user-anonymity preservation.

Password Friendliness: In proposed SAB-UAS scheme, U_{sr} freely chooses his/her secret session-key US_K to register or modify at D_C. Moreover, the proposed SAB-UAS scheme supports revocation/reissue of smartcard SM through the knowledge of D_C. Hence, the proposed scheme claims better user efficiency and friendliness.

Resilient to User-Forgery Attack: Assume that A_{dv} wishes to forge a message MS_1 to deduce the key elements such as $\langle r_2, U_{ID}, m_x, m_y \rangle$. As Ad_i is directly associated with master-key $\langle m_x, m_y \rangle$, A_{dv} cannot easily infer the collective information of message transmission $MS_I = H(C_I) \oplus Ad_i$. Hence, the proposed SAB-UAS scheme can be resilient to user-forgery attack.

Resilient to Sensor-Capture Attack: In the proposed SAB-UAS scheme, A_{dv} tries to seize the control of some sensor nodes MS_j that establishes the communication with U_{sr}. However, A_{dv} cannot easily capture or forge message transmission MS_3 as it is built or constructed using N_i. Moreover, MS_j shares a common session-key US_K with WG_{Ac}, which is not at all related to KS_U. Therefore, the proposed SAB-UAS scheme claims that A_{dv} couldn't exploit this attack successfully.

Resilient to Gateway-Forgery Attack: This attack has an ability to forge message transmission MS_1 or MS_2. In order to fabricate the message transmission MS_1, a critical parameter known as US_K is extremely subjective that tries to infer the messages namely MS_1 and MS_3. Unfortunately, the master keys $\langle m_x, m_y \rangle$ cannot be forged simultaneously to verify the session key KS_U of WG_{Ac}. Hence, the proposed scheme is resilient to gateway-forgery attack.

Resilient to Known-Key Attack: This attack realizes that the disclosure of session-key will have an effect on the security of the secret key. In the proposed SAB-UAS scheme, a secret session-key $US_K = H(AD_i \parallel KS_U \parallel TS)$ is derived from $KS_U = r_1 \times Z_i$, where $Z_i = r_n \times P$. This computation proves that U_{sr} session-key is generated independently to claim that the revelation of US_K has no authority on the exploitation of other sessions keys. Hence, the proposed scheme can be resilient to known-key attack.

Resilient to Offline-Guessing Attack: A three-factor authentication scheme ensures that even if A_{dv} infers the information of any two-communication parties, he/she may not be able to break up the remote server systems. In this scheme, A_{dv} tries to gather the parameters such as biometric and password, however, he/she could not acquire a possible computation of Y_i to build a legal login request message. Similarly, A_{dv} tries to gather the parameters such as password and smartcard, nonetheless, he/she cannot either perform a proper computation of Y_i nor predict the biometric information. Hence, it could not execute the offline-guessing attack. Also, A_{dv} tries to gather the parameters such as biometric and smartcard, nonetheless, he/she may have a chance to explore an offline guessing attack by means of MS_I or BT_i to verify the correctness of guessing value.

Assume that A_{dv} exploits BT_i to explore the offline guessing attack and its execution steps as follows: A_{dv} hypothecates U_{ID} and Ad_i into $U_{ID}{}^*$ and $Ad_i{}^*$ respectively. This hypothecation computes $R_i^* = R_{EP}(B_{IO_i}^*, P_i)$; $Ad_i{}^* = H(R_i^*)$; and $VR_I{}^* = H(U_{ID} \parallel Ad_i{}^*)$ to check whether $VR_I == VR_I{}^*$ or not. However, A_{dv} cannot infer a proper U_{ID} and Ad_i to send a login request to WG_{Ac} without the knowledge of P_i. Thus, the proposed scheme claims that it can be resilient to offline-guessing attack.

Property of Mutual Authentication and Key Agreement: In proposed SAB-UAS scheme, it is observed that U_{sr} and WG_{Ac} should respond to MS_j. Specifically, WG_{Ac}uses a long-term secret value S_{ID_j} to generate a correct message transmission $MS_I = H(C_I) \oplus Ad_i$, where $Ad_i = H(R_i)$ and it is validated using U_{sr}. In another way, U_{sr} applies $C_I = H(U_{ID} \parallel m_x \parallel m_y)$ and $AD_i = U_{ID} \oplus H(r_2)$ to generate a corrective response-value MS_3 that is verified using WG_{Ac}. This verification shows that U_{sr} and WG_{Ac} mutually passes the authenticated message transmission to exchange the messages of MS_j. Hence, the proposed scheme claims to achieve the property of mutual authentication.

With a generation of session-key, it is observed that U_{sr} and WG_{Ac} plays a vital role to contribute to the generation of session-key namely $\langle m_x, m_y \rangle$. This has a logical consequence that neither any U_{sr} can generate or control his/her session-key, nor any session-key can be adequate to produce random-key if any of the U_{sr} be able to construct a sufficient random input-keys. Hence, the proposed scheme claims the preservation of key agreement.

Property of Perfect Forward Secrecy: In proposed SAB-UAS scheme, a property of perfect forward-secrecy necessitates a long-term secret information $\langle S_{ID_j} \rangle$ to be highly secured between U_{sr} and WG_{Ac}that ensures all the previous key establishments are well protected. Based on the Diffie-Hellman protocol, the proposed scheme claims to achieve better forward secrecy. With the secret-key information of U_{sr} and WG_{Ac}, A_{dv} tries to recover $US_K = H(AD_i \parallel KS_U \parallel TS)$. However, from the specific feature of intractability based on the Diffie-Hellman problem, the proposed scheme claims that it is impracticable for A_{dv} to

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2941575, IEEE Access

compute $KS_U = r_n \times Y_i^*$.

C. RESOURCE EFFICIENCY ANALYSIS

This subsection estimates various resource efficiencies such as storage, computation, and communication of proposed SAB-UAS scheme. The analysis details are as follows:

Analyzing Storage Efficiency: In order to analyze storage overhead, the communication messages of a user U_{sr} and smartcard $SM_I$are chosen. Particularly, if we apply $SHA-1$, byte-length of 20 is set to the following parameters namely random number $r_1$and r_2, user identity U_{ID} and hash-resistant function, whereas byte-length of data timestamp is 2. Therefore, the proposed SAB-UAS claims that the total storage data length can easily be calculated for C_I, MS_I, N_I and VR_I. In respect of storage, the saved messages require 80 bytes.

Analyzing Communication Efficiency: In order to examine communication overhead, U_{sr} login request message $\{AD_i, Y_i, MS_1, MS_2, MS_3, TS_i\}$ is considered, which is later submitted to WG_{Ac}in turn to process the login. According to the above assumption of byte-length, the message length of U_{sr} is 102 bytes. Similarly, the byte-length of WG_{Ac}computation and U_{sr} the response is calculated and its summation is $30 + 20 = 50$ bytes during the system authentication phase. Thus, the system login and authentication phase of SAB-UAS scheme are totaled into $102 + 50 = 152$ bytes.

Analyzing Computation Efficiency: In order to realize the complexity of computational efficiency, the frequency of hash resistant function is considered. Importantly, the computation time of the X-OR operation is practically ignored as it has less time to execute the process. As referred in [34], the environment of 2.20 GHz CPU and 2 GB RAM consumes 0.0023 ms to execute the hash resistant function on an average. Therefore, the proposed SAB-UAS scheme claims that the execution times of hash function in system login and authentication phases are 7 and 13 times respectively. The calculation shows that the computation cost of SAB-UAS is recorded into $0.0161 + 0.0299 = 0.046$ ms.

D. COMPARISON OF PERFORMANCE EFFICIENCY

As from Table VI, the time cost of various authentication phases is compared in terms of T_{CM} denotes one-way chaotic map function, T_{SED} denotes symmetric encryption / decryption and T_{hash} denotes one-way hashing function respectively. Importantly, T_{hash} is examined using SHA 1. A test platform used in [52] is also applied to examine the computation parameters such as $T_{CM} = 127.042$ µs, $T_{SED} = 21.4835$µs and $T_{hash} = 21.4835$µs. It is supposed that all the authentication schemes including timestamps, random-integers, a hashing function, wireless gateway access, and medical-sensor node are set the key size as 160 bits. However, the chaotic map results in the key size of 1024 bits long as it is capable to perform modular prime in order to provide more security. In [53], it is discussed that the basis of communication cost is more non-trivial. A detailed hypothesis shows that the user identities, timestamps, and random integers are assigned to be 32 bits or only 4 bytes.

TABLE VI PERFORMANCE EFFICIENCIES OF EXISTING AUTHENTICATION SCHEMES

Existing Scheme / Properties	Kumari et al. [54]	Gope et al. [55]	Wu et al. [56]	Proposed Scheme
Execution Time for U_{sr} (µs)	10 T_{hash} = 0.328	7 T_{hash} = 0.2296	11 T_{hash} = 0.3608	9 T_{hash} = 0.2908
Execution Time for WG_{Ac} (µs)	8 T_{hash} = 0.2624	9 T_{hash} = 0.2952	10 T_{hash} = 0.5576	7 T_{hash} = 0.2296
Execution Time for MS_j	6 T_{hash} = 0.1968	3 T_{hash} = 0.984	6 T_{hash} = 0.1968	3 T_{hash} = 0.984
Communication Cost (bits)	3040	2400	2720	1216

Generally, the storage character of user identity cannot be less than six characters. Since DES is widely known to be insecure [53], a key size 56 bits is even not considered as a secure key length. The performance analysis demonstrates that the execution times of the proposed scheme have less cost in comparison with other existing schemes [54-56] for the communication entities namely U_{sr}, WG_{Ac} and MS_j. After all, the proposed SAB-UAS scheme is claimed to be robust and secure in order to realize in practice. However, Gope et al. [55] are completely impracticable as it is susceptible to a de-synchronization attack. In the wireless environment, even if none of the adversaries try to block the data packets, then the loss of data packet cannot be occurred between U_{sr}, WG_{Ac} and MS_j. It is appeared to be a problem of de-synchronization. Assume that the proposed SAB-UAS scheme has last message confirmation, which is blocked or stolen due to time overdue. Then, WG_{Ac}cannot modify or replace the parameter pair $\langle U_{ID}, Ad_i \rangle$ to make the data more inconsistent between U_{sr} and WG_{Ac}.

VI. PRACTICAL EXAMINATION USING NS3

This section demonstrates the practical implementation of proposed SAB-UAS using NS3 simulation [57] to examine the network parameters such as packet delivery ratio, end-to-end communication delay $\langle s \rangle$, throughput rate of data transmission $\langle bps \rangle$, and routing overhead $\langle packets \rangle$. For the analysis of the above parameters, a widely accepted version known as NS-3.28 has been installed on the platform of Ubuntu-14.04 LTS [58]. Table V shows the important parameters used in NS3 simulation that assumes a network coverage area as $80 \times 80\, m^2$ to examine the medical sensor and device controller node with a distance of 25 meters and 50 meters respectively, considered in [55]. A communication standard known as IEEE-802.15.4 is used as media access control to simulate the network duration $\approx 1800\,s$ i.e. 30 minutes. Because of network nature i.e. Ad hoc, optimized link state routing (OLSR) is preferred. It is used to provide dynamic discovery that invokes proactive routing to maintain the distribution table between the communication entities. Table VII represents the important notation used in simulation.

TABLE VII IMPORTANT SIMULATION PARAMETERS

Parameter	Description
Network Platform	Ubuntu-14.04 LTS
NS3 Version	NS-3.28
Routing Protocol	Optimized Link State Routing (OLSR), Adversarial Model
Number of communication nodes	⟨3,5,9⟩
Number of device controller nodes	⟨3⟩
Number of medical sensor node	⟨160⟩
Number of Malicious Node	20
Execution Time	⟨1800⟩ s
Network coverage area	$80\ \times 80\ m^2$
Data packet size	144 bits, 80 bits, and 64 bits
Wireless gateway $\mathrm{WG_{Ac}}$ location	$50\ \times 25\ m^2$
Traffic Type	UDP/TCP
Time Interval	$4\ s$
Mobility	$\approx\ 2\ to\ 50\ m/s$

To investigate the network metrics, the sensor nodes are implanted in rectangular form. It has ⟨20⟩ sensors in a row, which subsequently adds more concurrent rows for every execution scenario restricting the sensor quantity to be ⟨160⟩ nos i.e. row size ⟨8⟩. To explore a basic network scenario, three device controller, one wireless gateway and three patients with five medical sensors were considered. This is to note that the wireless gateway access $\mathrm{WG_{Ac}}$ is not considered in [42] to inspect the data aggregation and reliable data transmission. The description of a network scenario is as follows: Scenario: This scenario deploys⟨3,5,9⟩ $\mathrm{U_{sr}}$, ⟨1⟩ $\mathrm{WG_{Ac}}$, ⟨3⟩ M_S and ⟨160⟩ $\mathrm{MS_j}$. For the above scenario, three data transmission messages such as $\langle MS_1, MS_2, TS_1\rangle$ from $\mathrm{U_{sr}}$ to $\mathrm{WG_{Ac}}$, $\langle MS_3, MS_4, TS_2\rangle$ from $\mathrm{WG_{Ac}}$ to M_S and $\langle MS_5, TS_3\rangle$ from M_S to $\mathrm{U_{sr}}$ are considered with the packet size of 512 bits, 512 bits, and 192 bits to examine the network parameters. Each $\mathrm{U_{sr}}$ starts randomly to exchange the message i.e. for every $4\ s$. Importantly, according to the adversarial module, ⟨20⟩ malicious nodes are randomly assigned to perform various misbehavior in packet routing include send and receive messages.

Analysis of packet delivery ratio (PDR): It is a highly essential factor to measure the performance of routing protocol in any communication networks. In the use of packet size, availability of nodes, transmission range and coverage area, this analysis was performed. This communication metric defines the successful receiving packet delivery ratio at the sink node. From Fig.2, it is evident that the PDR ratio of proposed SAB-UAS slightly deteriorates when the number of sensors grows larger. Specifically, from the addition of row i.e. 30 to 45, there was a slight deflection in proposed SAB-UAS and Wu et al. [56] that shows better packet delivery ratio in comparison with other authentication schemes [54,55]. Also, when the addition of rows grew consistently, the signal congestion continued to exist. As a result, the energy model defined in the wireless environment started draining more than expected, when there was a report of far distance message transmission. To improve the delivery ratio, a threshold limit can be set at the receiver side to control the energy dissipation or to abort the packet transmission when there is a far distance communication.

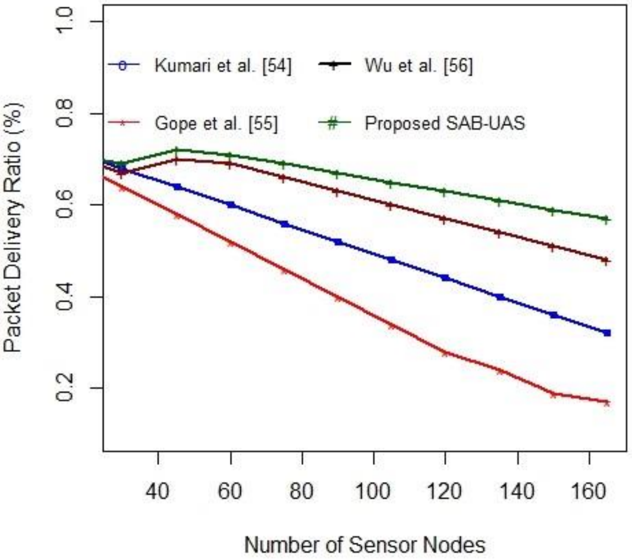

Fig.2 Packet Delivery Ratio

From the examination, it is realized that there may be an increasing number of connection breakdown when the mobility varies from $\sim 4\ ms$ to $\sim 20\ ms$. As a consequence, unusual packet loss and failures are resulted to degrade the quality of link connectivity.

Analysis of end-to-end (ETE) delay: It is defined as the average time taken by the data transmission packets to reach the receiver from the source node. Thus, it can be mathematically expressed as:

$$\langle ETE\rangle = \sum_{i=1}^{N_P} \frac{\left(T_i^{rec} - T_i^{send}\right)}{N_P} \tag{25}$$

Where N_P defines the total number of data transmission packets and $\langle T_i^{rec}, T_i^{send}\rangle$ denotes the sending and receiving time of packet transmission with respect to the given scenario. Fig.3 illustrates the packet end-to-end delay of proposed SAB-UAS with other existing authentication schemes. The examination results show that the proposed SAB-UAS consumes less delay in comparison with other existing schemes [54-56] such as 0.0278 sec, 0.0238 sec, 0.0203 sec and 0.0174 sec respectively. From the analysis, it is observed that the end-to-end delay increases when the number of communication nodes is proportionally increased. As a result, it is strongly stated that a number of transmission messages are subjected to experience more congestion as addressed in the given execution scenario.

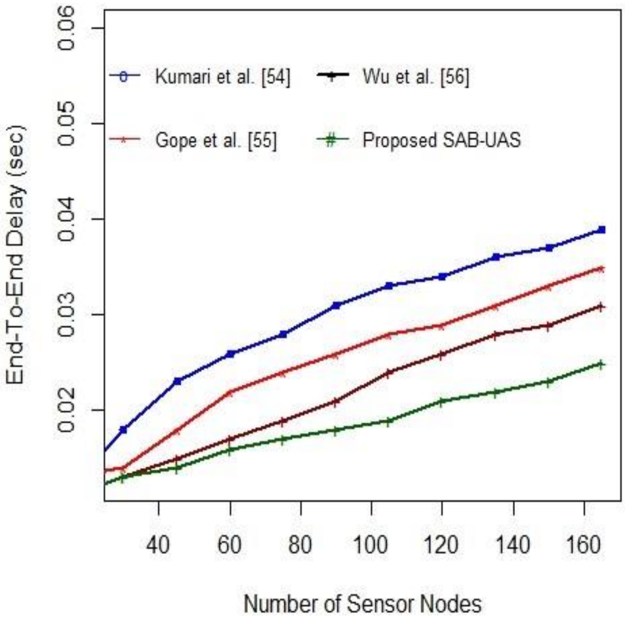

Fig.3. End-To-End Delay (sec)

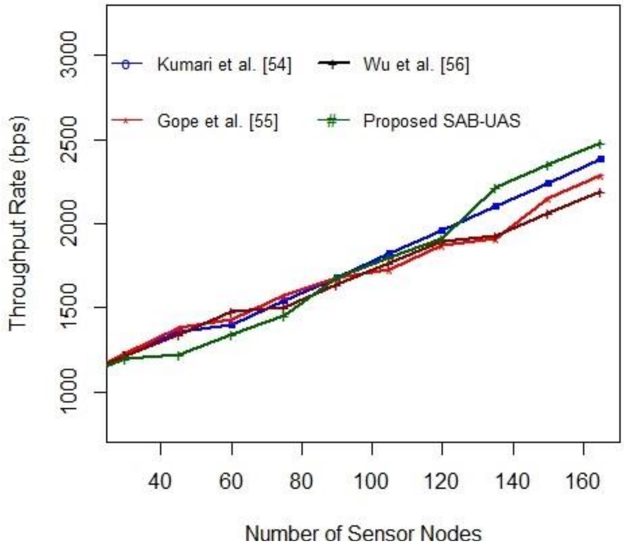

Fig.4. Throughput Rate (bps)

Analysis of throughput transmission rate $\langle TTE\rangle$: The throughput rate can be defined as the number of bits transmitted per unit of execution time. The throughput rate $\langle bps\rangle$ of proposed SAB-UAS is illustrated in Fig. 4. It can be expressed as:

$$\langle TTE\rangle = \frac{(N_R \times |P_{kt}|)}{T_D} \tag{26}$$

Where T_D is the total data transmission time $\langle Secs\rangle$, P_{kt} is the data transmission packet and N_R is the total number of receiving packets successfully. From Fig. 4, it is witnessed that the execution time was considered to evaluate the number of transmission packets i.e. for proposed SAB-UAS and other existing authentication protocols [54-56]. The execution result shows that the proposed SAB-UAS achieves better throughput rate in comparison with other existing authentication protocols [54-56] such as 1.64 kbps, 1.602 kbps, 1.604 kbps, and 1.624 kbps respectively. It is evident that the proposed SAB-UAS has a negligible deviation at 45 to 60 and 120 to 140 because of the increasing number of sensor nodes.

Analysis of Routing Overhead $\langle RTO\rangle$: The routing overhead can be defined as the total number of routing packets divided by the total number of successfully delivered packets during the mobility interval $\approx 2 \text{ to } 50 \text{ m/s}$.

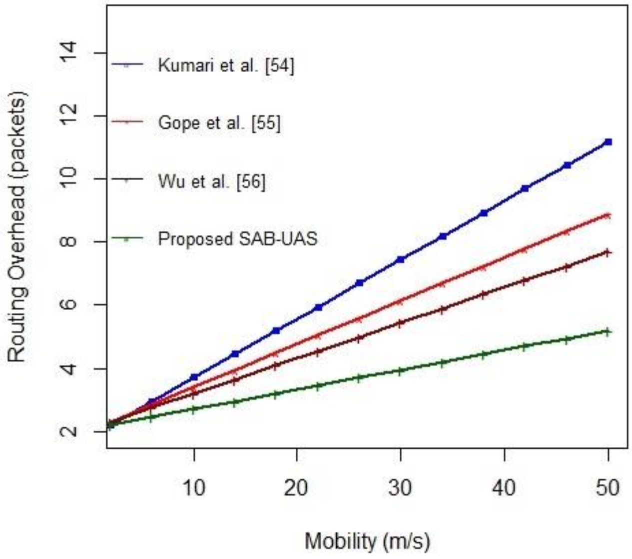

Fig.5. Routing Overhead ($packets$)

The in-depth analysis shows that the average number of routing packets is involved to deliver a data packet successfully. Moreover, this parameter is essential to find the excess bandwidth usage during routing overhead to handle network traffic. The simulation result reveals that the OLSR protocol tries to minimize the communication overhead as it maintains a proactive routing table to handle the periodic $'Hello'$ transmission and $'Topology\ Control'$ messages. From Fig.5, it is observed that the proposed SAB-UAS achieves less routing overhead i.e. packet in comparison with other existing protocol [54-56] such as 11.3, 6.7, 5.9, and 4.5 routing packets. In OLSR, the packet routing is tactfully managed to enhance the network performance and bandwidth usage at the mobility speed $\approx 2 \ to\ 50\ m/s$.

VII. CONCLUSIONS

In this paper, a secure-anonymous biometric-based user authentication scheme (SAB-UAS) has been proposed for a smart electronic-healthcare application using IoM. The proposed SAB-UAS scheme shows the formal security model, resource and performance efficiency analysis to prove the security, storage and performance efficiencies. The former proof demonstrates that the proposed scheme can protect the sensitive information of a user from adversary to achieve the property of perfect forward secrecy. The latter analysis shows that the proposed SAB-UAS scheme can substantially reduce the storage, computation and communication cost to improve the performance efficiency of any real-time based healthcare application systems. In addition, the rigorous informal and formal security analysis using BAN logic and random-oracle model proves that the SAB-UAS scheme provides better security evidence for the protection of various potential attacks for application based on IoMs. It is also shown that the proposed scheme achieves improved resource efficiencies such as storage, computation, and communication to build smart e-healthcare systems. Importantly, the network parameters such as packet delivery ratio, end-to-end delay, and throughput rate have been evaluated using a network simulator NS3. It is shown that the proposed SAB-UAS scheme experiences more congestion when the number of message transmission increases proportionally i.e. adding $\langle 20 \rangle$ sensors in a row. However, the proposed SAB-UAS could achieve better packet delivery ratio, end-to-end delay, throughput rate and routing overhead for the given scenario in comparison with other authentication protocols [61-63] even if the message transmission grew proportionally between $\mathrm{U_{sr}}$, $\mathrm{WG_{Ac}}$ and M_S.

REFERENCES

[1] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E. J. Yoon, and K. Y. Yoo, “Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications,” IEEE Access, vol. 5, pp. 3028– 3043, 2017.

[2] Otoum, S., Kantarci, B., & Mouftah, H. (2019, May). Empowering Reinforcement Learning on Big Sensed Data for Intrusion Detection. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)* (pp. 1-7). IEEE.

[3] Al-Turjman, F., Zahmatkesh, H., & Mostarda, L. (2019). Quantifying Uncertainty in Internet of Medical Things and Big-Data Services Using Intelligence and Deep Learning. *IEEE Access*.

[4] Al-Turjman, F. (2019). Intelligence and security in big 5G-oriented IoNT: An overview. Future Generation Computer Systems.

[5] Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2019). An overview of security and privacy in smart cities' IoT communications. Transactions on Emerging Telecommunications Technologies, e3677.

[6] Habib, Muhammad Asif, Mudassar Ahmad, Sohail Jabbar, Shehzad Khalid, Junaid Chaudhry, Kashif Saleem, Joel JPC Rodrigues, and Muhammad Sayim Khalil. "Security and privacy based access control model for internet of connected vehicles." Future Generation Computer Systems (2019).

[7] Wazid, M., Das, A. K., Kumar, N., Vasilakos, A. V., & Rodrigues, J. J. (2018). Design and Analysis of Secure Lightweight Remote User Authentication and Key Agreement Scheme in Internet of Drones Deployment. IEEE Internet of Things Journal.

[8] He, D., Kumar, N., Chen, J., Lee, C.-C., Chilamkurti, N., & Yeo, S.-S. (2015). Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. Multimedia Systems, 21(1), 49–60.

[9] Kumar, P., Lee, S. G., & Lee, H. J. (2012). E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. Sensors, 12(2), 1625–1647.

[10] Das, A. K., Wazid, M., Yannam, A. R., Rodrigues, J. J., & Park, Y. (2019). Provably Secure ECC-Based Device Access Control and Key Agreement Protocol for IoT Environment. IEEE Access, 7, 55382-55397.

[11] Das, A. K. (2016). A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks. Peer-to-Peer Networking and Applications, 9(1), 223–244.

[12] Odelu, V., Das, A. K., & Goswami, A. (2015). A secure biometrics-based multi-server authentication protocol using smart cards. IEEE Transactions on Information Forensics and Security, 10(9), 1953–1966.

[13] Farash, M.S.; Chaudhry, S.A.; Heydari, M.; Sadough, S.M.S.; Kumari, S.; Khan, M.K. A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security. Int. J. Commun. Syst. 2017, 30, e3019.

[14] X. Huang, X. Chen, J. Li, and L. Xiang, Yang ang Xu, “Further observations on smart-card-based password-authenticated key agreement in distributed systems,” IEEE Trans. Para. Distrib. Syst., vol. 25, no. 7, pp. 1767–1775, 2014.

[15] R. Madhusudhan and R. Mittal, “Dynamic id-based remote user password authentication schemes using smart cards: A review,” J. Netw. Comput. Appl., vol. 35, no. 4, pp. 1235–1248, 2012.

[16] G. M. Yang, D. S. Wong, H. X. Wang, and X. T. Deng, “Two factor mutual authentication based on smart cards and passwords,” J. Comput. Syst. Sci., vol. 74, no. 7, pp. 1160–1172, 2008.

[17] Watro R., Kong D., Cuti S., Gardiner C., Lynn C., Kruus P. TinyPK: Securing sensor networks with public key technology; Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks; Washington, DC, USA. 25 October 2004; pp. 59–64.

[18] Wong K., Zheng Y., Cao J., Wang S. A dynamic user authentication scheme for wireless sensor networks; Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing; Taichung, Taiwan. 5–7 June 2006; pp. 1–8.

[19] Das M. Two-factor user authentication in wireless sensor networks. IEEE Trans. Wirel. Commun. 2009;8:1086–1090.

[20] Yoon E., Kim C. Advanced biometric-based user authentication scheme for wireless sensor networks. Sens. Lett. 2013;11:1836–1843.

[21] Choi Y., Lee Y., Won D. Security improvement on biometric based authentication scheme for wireless sensor networks using fuzzy extraction. Int. J. Distrib. Sens. Netw. 2016;2016:1–16.

[22] Park Y., Lee S., Kim C., Park Y. Secure biometric-based authentication scheme with smart card revocation/reissue for wireless sensor networks. Int. J. Distrib. Sens. Netw. 2016;12:1–11.

[23] L. Lamport, “Password authentication with insecure communication,” Communications of the ACM, vol. 24, no. 11, pp. 770–772, 1981.

[24] C.-C. Chang and H.-D. Le, “A Provably Secure, Efficient and Flexible Authentication Scheme for Ad hoc Wireless Sensor Networks,” IEEE Transactions on Wireless Communications, vol. 15, no. 1, pp. 357–366, 2016.

[25] H.-L. Yeh, T.-H. Chen, P.-C. Liu, T.-H. Kim, and H.-W. Wei, “A secured authentication protocol for wireless sensor networks using elliptic curves cryptography,” Sensors, vol. 11, no. 5, pp. 4767–4779, 2011.

[26] W. Shi and P. Gong, “A new user authentication protocol for wireless sensor networks using elliptic curves cryptography,” International Journal of Distributed Sensor Networks, vol. 2013, pp. 1–7, 2013.

[27] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, and D. Won, "Security Enhanced User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography," Sensors, vol. 14, no. 6, pp. 10 081– 10 106, 2014.

[28] C. T. Li, C. C. Lee, C. Y. Weng, and C. M. Chen, "Towards secure authenticating of cache in the reader for RFID-based IoT systems," Peer-to-Peer Networking and Applications, vol. 11, no. 1, pp. 198–208, 2018.

[29] C.-T. Li, T.-Y. Wu, C.-L. Chen, C.-C. Lee, and C.-M. Chen, "An Efficient User Authentication and User Anonymity Scheme with Provably Security for IoT-Based Medical Care System," Sensors (Basel), vol. 17, no. 7, pp. 1–18, 2017.

[30] C.-T. Li, C.-L. Chen, C.-C. Lee, C.-Y. Weng, and C.-M. Chen, "A novel three-party password-based authenticated key exchange protocol with user anonymity based on chaotic maps," Soft Computing, vol. 22, no. 8, pp. 2495–2506, 2018.

[31] K. Hameed, A. Khan, M. Ahmed, A. G. Reddy, and M. M. Rathore, "Towards a formally verified zero watermarking scheme for data integrity in the Internet of Things based-wireless sensor networks," Future Generation Computer Systems, vol. 82, pp. 274–289, 2018.

[32] Al-Turjman, F., Hasan, M. Z., & Al-Rizzo, H. (2018). Task scheduling in cloud-based survivability applications using swarm optimization in IoT. *Transactions on Emerging Telecommunications Technologies*, e3539.

[33] P. Gope, J. Lee, and T. Q. S. Quek, "Lightweight and Practical Anonymous Authentication Protocol for RFID Systems Using Physically Unclonable Functions," IEEE Transactions on Information Forensics and Security, vol. 13, no. 11, pp. 2831–2843, 2018.

[34] Al-Turjman, F., Ever, Y. K., Ever, E., Nguyen, H. X., & David, D. B. (2017). Seamless key agreement framework for mobile-sink in IoT based cloud-centric secured public safety sensor networks. IEEE Access, 5, 24617-24631.

[35] D. Deebak, F. Al-Turjman, L. Mostarda, "Hash-Based RFID Authentication Mechanism for Context-Aware Management in IoT-Based Multimedia Systems", MDPI Sensors, 2019.

[36] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks," IEEE Internet of Things Journal, vol. 5, no. 1, pp. 269–282, Feb 2018.

[37] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, S. Kumari, and M. Jo, "Chaotic Map-based Anonymous User Authentication Scheme with User Biometrics and Fuzzy Extractor for Crowdsourcing Internet of Things," IEEE Internet of Things Journal, 2017, DOI: 10.1109/JIOT.2017.2714179.

[38] M. Wazid, A. K. Das, M. K. Khan, A. A. D. Al-Ghaiheb, N. Kumar, and A. V. Vasilakos, "Secure Authentication Scheme for Medicine Anti-Counterfeiting System in IoT Environment," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1634–1646, 2017.

[39] Al-Turjman, F., & Alturjman, S. (2018). Context-sensitive access in industrial internet of things (IIoT) healthcare applications. IEEE Transactions on Industrial Informatics, 14(6), 2736-2744.

[40] Koblitz N. Elliptic curve cryptosystems. Math. Comput. 1987;48:203–209.

[41] Miller V. Use of elliptic curves in cryptography. Adv. Cryptol. 1985;218:417–426.

[42] Dolev, D.; Yao, A. On the security of public key protocols. IEEE Trans. Inf. Theory 1983, 29, 198–208.

[43] S. Halevi and H. Krawczyk, "Public-key cryptography and password protocols," ACM Trans. Inform. Syst. Secur., vol. 2, pp. 230–268, 1999.

[44] Otoum, S., Kantarci, B., & Mouftah, H. (2018, May). Adaptively supervised and intrusion-aware data aggregation for wireless sensor clusters in critical infrastructures. In 2018 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

[45] Balasubramanian, V., Zaman, F., Aloqaily, M., Al Ridhawi, I., Jararweh, Y., & Salameh, H. B. (2019, May). A Mobility Management Architecture for Seamless Delivery of 5G-IoT Services. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)* (pp. 1-7). IEEE.

[46] Otoum, S., Kantarci, B., & Mouftah, H. T. (2017, May). Hierarchical trust-based black-hole detection in WSN-based smart grid monitoring. In *2017 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.

[47] Oueida, S., Aloqaily, M., & Ionescu, S. (2018). A smart healthcare reward model for resource allocation in smart city. *Multimedia Tools and Applications*, 1-22.

[48] D. Wang, C. G. Ma, and P. Wu, "Secure password-based remote user authentication scheme with non-tamper resistant smart cards," in Proc. DBSec 2012, ser. LNCS. Springer, 2012, vol. 7371, pp. 114–121.

[49] Y. G. Wang, "Password protected smart card and memory stick authentication against off-line dictionary attacks," in Proc. SEC 2012.

[50] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in Proc. EUROCRYPT 2000, ser. LNCS. Springer-Verlag, 2000, vol. 1807, pp. 139–155.

[51] M. Burrows, M. Abadi, and R. Needham, A logic of authentication, ACM Trans. Comput. Syst., vol. 8, no. 1, pp. 18—36, Feb. 1990.

[52] Wu, F., Xu, L., Kumari, S., Li, X., Das, A. K., Khan, M. K., & Baliyan, R. (2016). A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks. Security and Communication Networks, 9(16), 3527-3542.

[53] Stallings, W. (2006). Cryptography and Network Security, 4/E. Pearson Education India.

[54] Kumari, S., & Om, H. (2016). Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines. Computer Networks, 104, 137-154.

[55] Gope, P., & Hwang, T. (2016). A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks. IEEE Trans. Industrial Electronics, 63(11), 7124-7132.

[56] Wu, F., Li, X., Sangaiah, A. K., Xu, L., Kumari, S., Wu, L., & Shen, J. (2018). A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. Future Generation Computer Systems, 82, 727-737.

[57] "The Network Simulator-ns-3," https://www.nsnam.org/releases/ns-3-28/. Accessed on January 2019.

[58] Habib, Muhammad Asif, Mudassar Ahmad, Sohail Jabbar, Shehzad Khalid, Junaid Chaudhry, Kashif Saleem, Joel JPC Rodrigues, and Muhammad Sayim Khalil. "Security and privacy based access control model for internet of connected vehicles." Future Generation Computer Systems (2019).