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.2020.DOI

A Lightweight and Secure Attribute-Based Multi Receiver Generalized Signcryption Scheme for Body Sensor Networks

JAWAID IQBAL[1], ABDUL WAHEED[1,2], MAHDI ZAREEI [3], (Senior Member, IEEE), ARIF IQBAL UMAR[1], NOOR UL AMIN[1], ABDALLAH ALDOSARY[4], EHAB MAHMOUD MOHAMED[5,6], (Member, IEEE)

[1]Department of Information Technology, Hazara University, Mansehra 21120, KP, PK
[2]School of Electrical and Computer Engineering, Seoul National University 08826, Korea
[3]Tecnologico de Monterrey, School of Engineering and Sciences, Zapopan 45201, Mexico
[4]Department of Computer Science, Prince Sattam Bin Abdulaziz University, As Sulayyil, 11991, Saudi Arabia
[5]Electrical Engineering Department, College of Engineering, Prince Sattam Bin Abdulaziz University, Wadi Addwasir 11991, Saudi Arabia
[6]Electrical Engineering Department, Faculty of Engineering, Aswan University, Aswan 81542, Egypt

Corresponding author: Abdul Waheed (abdul@netlab.snu.ac.kr).

ABSTRACT With the rising number of patients along with the same time, the comparative evolution in wireless technology has made Body Sensor Networks (BSNs) flourishing in the market. In BSNs, tiny biosensor nodes are deployed inside/outside of a human body to continuously monitor patient vital signs such as heartbeat rate, blood pressure, respiratory rate, and temperature. BSNs face various challenges due to their constrained natured environment. These are prioritized, delay less and secure transmission of patient data using a public network, simultaneous reception of patient data by end-users, patient identity privacy, high overhead, and energy constraints. However, various researchers have worked in this domain, unable to cope with all these issues in one go. In this paper, we have proposed a novel cryptosystem covering the mentioned issues in a desirable way. For this purpose, we design a novel concept of a lightweight and secure attribute-based multi-receiver generalized signcryption scheme that can adaptively work as an encryption mode, a signature mode, or a signcryption mode with a single algorithm and consume fewer resources by using shorter keys size of Hyper-elliptic Curve Cryptography (HECC). Similarly, we design a modified priority-based scheduling algorithm to delay less emergency patient data. Multiple end-users access the encoded data simultaneously by defining an access policy using AND & OR logic gates. Furthermore, we simulate our scheme using the AVISPA tool and demonstrate that our proposed scheme can meet the security requirements such as data confidentiality (IND-CCA), integrity, unforgeability (EUF-CMA), patient data authenticity, forward secrecy, and non-repudiation distinctly in the Random Oracle Model (ROM). Due to lower processing costs and transmission overhead, this scheme is more efficient and suitable for the resource-constrained environment of BSNs.

INDEX TERMS Body sensor networks, security, HECC, generalized signcryption, multi-receiver, priority based scheduling

I. INTRODUCTION

BSNs consist of many biosensor nodes that are continuously monitoring diverse physiological signals, such as BP (systolic and diastolic), ECG, EMG, SpO2 and activity recognition [1]. These types of biosensors are accessible in different shapes, i.e., implantable devices, biomedical smart clothes, and wrist wearable devices with the aim not to disturb the routine life of humans [2]. According to the nature of various biosensor nodes in BSNs, monitor patient vital signs and provide complete intelligent treatment when any abnormality occurs in the human body, i.e., accurate insulin injection when the patient's sugar level increased [3]. 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.2020.3035324, IEEE Access

applications of BSNs are to prolong human life, enhance society's medical treatment, and indorse the living quality of people [4]. In BSNs, prioritized simultaneous reception of patient data by end-users, delaying less secure dissemination of sensitive patient data from source to destination with minimal cost is the massive challenging issue in the present era [5]–[8].

Furthermore, various researchers worked in this domain but impotent to cope with all these mentioned issues in one go. In this paper, we propose a novel cryptosystem for BSNs to handle the mentioned issues in a desirable way. We design a novel concept of multi-receiver generalized signcryption to resolve the issues of delay less secure transmission of patient data, simultaneous reception of patient data by end-users with minimal cost. Additionally, we apply attribute-based access policies in BSNs to efficiently manage patient information privacy protection. Security policies are statements that combine patient attributes using boolean logic (AND & OR) gates to specify the rules for permitting/ denying the patient sensitive information [9], such as {("Dept of Cardiology" AND "Specialist") AND ("Islamabad" OR "Peshawar") OR "Name: Dr. Alice" }. Multiple end users (doctor, nurse, the insurance company, and researcher) can access the encoded data simultaneously by defining an access policy using (AND & OR) logic gates [10]. At the same time, only those register end users can decrypt the patient-encoded data who access structure matched with pre-defined access policies stored on a server. In this paper, attribute-based multi-receiver Generalized Signcryption (GSC) works in three different modes simultaneously or separately using a single algorithm [11]. According to the user requirements, GSC work on only encryption mode when patient data confidentiality is required, only signature mode when patient data authenticity is needed, only signcryption mode when both are needed, such as data confidentiality and data authenticity to overcome the burden on networks and utilized system resources efficiently.

Moreover, in this paper, using a modified priority-based scheduling algorithm system prioritizes the emergency patient data for earlier diagnosis and better patient disease treatment. This scheme is more appropriate for resource-constrained environments, such as (low memory for storing data, less power capability, low computational power) of BSNs. Additionally, we also demonstrate this scheme's security using the AVISPA tool and the security model.

II. RELATED WORK

In the literature, various signcryption schemes used for body sensor networks are efficient but still not performed excellently when only one of three functions, patient data confidentiality, patient data authenticity, or patient data confidentiality and authenticity, is required. To resolve this gap, [12] proposed the scheme and discussed the concept of GSC that works in three different modes, such as encryption mode, a signature mode, or a signcryption mode. In the scheme [13], the first time proposed a novel idea of multiple receiver GSC in the Random Oracle Model (ROM) for $ECDLP$ supposition. However, still, this scheme suffers from only the signature mode property. In the scheme [14], the authors presented the concept of ID-based proxy authenticated encryption using UC structure. Moreover, this scheme is secure in their defined security model and satisfied the security properties of UF-CMA and IND-CCA2 but due to the high cost, not suitable for the resource-constrained environment. In scheme [31], proposed a generalized multi-receiver signcryption scheme based on $ECDLP$ assumption that works for the signature, multi-receiver encryption, and multi-receiver signcryption, but still not provide data confidentiality. In scheme, [32] advised the concept of CDH assumption for multi-receiver scheme GSC. However, schemes [15], [16], and [32] proposed a multi-receiver GSC scheme that is not IND-CCA2 secure in the pure encryption mode and encryption hybrid mode and provides the enhancement of their system secure under the CDH supposition. However, the scheme is inefficient in terms of security. In scheme [17], a hybrid encryption (HECC and symmetric key) method is used to secure data for transmission in a multi-user environment. Furthermore, it is still suffering from man-in-the-middle attacks and does not provide security properties like public verifiability and forward secrecy. Due to high overhead, this scheme is not suitable for the resource-constrained environment of BSNs.

In a scheme [18], a multi-receiver privacy-preserving protocol is used to transmit data securely from source to destination using the signcryption method in a heterogeneous environment. However, this scheme is insecure in its defined security model and suffered from Indistinguishability Chosen Cipher Text Attack (IND-CCA). In the scheme [19], the authors proposed a heterogeneous hybrid security model based on signcryption that transmitted data in the multi-receiver environment. However, this scheme still has security weaknesses like replay attack, and due to paring operations, the processing cost and transmission cost are high and cannot recommend for tiny biosensor nodes.

In scheme [20], a generalized authenticated encryption method is used for secure dissemination of data from the sender to the receiver node using HECC. Moreover, this scheme is still suffered from existential unforgeability against adaptive chosen message attacks, and the security of the scheme is not adequately proved in the form of theorems.

In the scheme [21], the authors proposed the first time the concept of ID-based generalized signcryption based on the Paterson-Scheldt scheme that is secure in the standard model. The main contribution of this scheme is to overcome the implementation complexity. Additionally, it is not suitable for disseminating sensitive data and cannot provide a non-repudiation property. In the scheme [22], the signcryption based HECC method used for efficient utilization of the bandwidth and minimized the computational cost and communication cost, but this scheme still does not meet the security requirements of IND-CCA in the Random Oracle Model (ROM). In this scheme [23], the authors proposed CLC based generalized signcryption for the secure transmis-

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.2020.3035324, IEEE Access

sion of remote patient data from source to destination. In this scheme, the authors resolved the key escrow problem of ID-based cryptosystem using the third party called PKG; moreover, this scheme has no proper mechanism for distributing partial key among sensor nodes. The medical server and the attacker easily modified the sensitive data of the patient. In scheme [24], the author proposed an efficient and novel method based on CLC based generalized signcryption that satisfied the essential security property of data confidentiality and unforgeability against massage and chosen-ciphertext attacks, respectively, in ROM. In this scheme, the security is obtained without applying pairing operations due to which this scheme suitable for the low processor and low memory devices. In scheme [25], a novel protocol designed based on CLC generalized signcryption to improve the life quality of the mobile health system and enhanced the efficiency of health care using minimum system resources. This scheme cannot provide unforgeability property. In the scheme [26], the authors proposed a novel certificate-less generalized signcryption and proved the scheme's security using a formal security model. The scheme suggested that it proved secure IND-CCA2 under GBDH assumption and CDH assumptions. Moreover, this scheme's authors say that the scheme is practical and efficient, shown in the performance analysis. In scheme [27], proposed a novel generalized ring signcryption that performs both ring signature and ring signcryption function using a single key pair along with one algorithm. It is more attractive for an extensive system where many users can work and change their responsibilities. Its security proved using formal security models in certificate less environment. Moreover, using GBDH and CDH, the confidentiality property is confirmed and using GDH and CDH, the scheme's unforgeability property proved in ROM. Furthermore, this scheme used the concept of bilinear paring due to which it is suffered from high computational cost and communication overhead and not suitable for the resource-constrained environment of BSNs.

In scheme [28], proposed the concept of blind signature along with message recovery to protect the data using ECDLP and utilized the communication bandwidth efficiently. However, this scheme still suffered from high overhead in terms of computation and communication. To handle these issues, smart and secure cryptosystem is required.

In the scheme [29], the authors proposed an ID-based generalized signcryption technique to achieve the security properties of data confidentiality and authentication in the big data environment and claimed that the security of their scheme is formally proved in the standard model. In scheme [30] proposed the updated version of [29], and he claimed that the scheme [29] is not secure in the standard model and does not satisfy (IND-CCA) and (EUF-CMA) properties. Moreover, the third-party PKG is still compromised, and the attacker can easily modify the data in the big data environment. In the scheme [49], to ensure the security of data stored in a cloud, the key insulated method is proposed that overcomes the problem of secret key exposure and enhanced the cloud-based data-keeping environment's overall security. In this method, we used CLC based setting without bilinear pairing along with generalized signcryption. This scheme is more attractive for those types of users who connected to the cloud using smartphones.

In the scheme [50], the authors proposed a novel, efficient and secure method for WBAN to preserve the registered doctor anonymity through a controller before disseminating patient vital signs to a centralized server for storage. It consumed fewer system resources during mutual authentication and computation. Furthermore, the tracking system enhances patient-sensitive information privacy and protects the WBAN from adversaries' attacks. As compared to the existing literature, this method performed better results in terms of certificate verification, patient data transmission, and signature. Moreover, the scheme still suffers from IND-CCA and does not satisfy the backward and forward secrecy and integrity protection. In the scheme [51], the authors proposed a novel routing algorithm called (EOCC-TARA) for WBAN based on SDN technology to minimize the traffic congestion, energy consumption, and node thermal dissipation during patient data transmission. Moreover, the proposed algorithm initially chooses the forwarding biosensor nodes for route establishment based on network temperature and node energy. While the nodes that have high temperatures do not be considered for route establishment. EMSMO is used to select the best path to enhance the quality of WBAN in terms of high throughput, less packet loss, less delay, high data rate, less network temperature, and less congestion overhead. Furthermore, the practical implementation of SDN-based WBAN is still missing, and the scheme is not flexible for dynamic network topology. In the scheme [52], the authors used the concept of blockchain along with CP-ABE to enhance the security and privacy of patient electronic health records. Furthermore, the malicious medical officer cannot upload the patient's fraudulent medical information to the server during patient diagnosis. While the polynomial equation is used for keyword searching, and the logic gates (AND, OR) are used for creating access policies. Only registered doctors can access the patient electronic medical record from the server according to a pre-defined access structure. Moreover, the scheme does not fulfill EUF-CMA security property. The scheme [53] highlighted the limitations of conventional fine-grained search techniques, such as (PEKS, ABKS) and proposed a novel method called CP-DABKS. Furthermore, the system administrator creates a secure link and stored pre-defined access policy for the medical server. Now each authorized user can decrypt the encoded patient-sensitive medical information which satisfied the pre-defined rules. It eradicates the secure link for trapdoor communication. Additionally, the scheme is efficient in energy and cost and protects sensitive patient data from adversaries' attacks. In the scheme, [54] designed an efficient ring signature based on a certificateless environment to protect the patient's identity privacy. Furthermore, a public auditing technique is proposed for cloud-assisted BAN. certificateless signature is suitable

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.2020.3035324, IEEE Access

for the resource-constrained environment of WBAN. The simulation results show that the proposed method's efficiency is improved compared to other existing schemes, resisting the forging attacks. In a scheme [55], a novel fault-tolerant mechanism is applied to enhance the reliability of the patient data and networks. Furthermore, this scheme used efficient co-operative transmission techniques to utilize resources and reduce the channel's impairment effectively. The results show that this scheme reduces energy, bit error rate, and transmission delay. However, the throughput of the networks is still not improved, which affects the overall performance of the WBAN. In the scheme [56], a novel trust-based ERCS is proposed for WBANs to enhance patient data privacy and reliability. Additionally, the co-operative method is applied to ensure reliability, while the cryptographic technique improves patient data confidentiality. Moreover, the fuzzy logic approach is applied to ranking determinations. However, this scheme is still suffered from high delay during patient data communication.

In the above-related works, we reviewed the state of the art schemes for security and privacy within BSNs. Moreover, we have determined from the literature review that a lightweight and secure attribute-based multi-receiver generalized signcryption scheme is needed. The proposed lightweight scheme will be improved the security and privacy of patient data with minimal cost and enhanced the overall efficiency of the BSNs.

A. CONTRIBUTIONS

This paper proposes a lightweight and secure attribute-based multi-receiver generalized signcryption scheme to cope with BSNs issues in one go. Our contributions are as follows:

- We design a novel concept of multi-receiver generalized signcryption in BSNs that can adaptively work as an encryption mode, a signature mode, or a signcryption mode with a single algorithm and consume fewer resources by using a shorter key size of HECC to resolve the issues of secure transmission of patient data using a public network, simultaneous reception of patient data by end-users and high overhead. Additionally, using this method, we efficiently utilized the system resources and overcame the burden on BSNs.
- We design the concept of attribute-based access control policies to improve data privacy and protect patient-sensitive information from adversaries' attacks. Security policies are statements that combine patient attributes using boolean logic (AND & OR) gates to specify the rules for permitting/ denying patient sensitive data. Only the registered and legal users can access the patient data whose access structure matched with the preloaded access structure of the server in BSNs.
- We design the concept of a modified priority-based scheduling algorithm for transmission of delay less emergency patient data, and efficient utilization of communication bandwidth.
- Furthermore, we simulate our scheme using the AVISPA tool and using the security model, we demonstrate that our proposed scheme can meet the security requirements such as data confidentiality (IND-CCA), integrity, unforgeability (EUF-CMA), patient data authenticity, forward secrecy and non-repudiation distinctly in the ROM.
- Due to lower processing costs and transmission overhead, our scheme is more efficient and suitable for the resource-constrained environment of BSNs.

B. PAPER ORGANIZATION

The rest of the manuscript is organized as follows: "Section II presents the related work on BSNs, Section III presents the knowledge of preliminary, Section IV describes the proposed scheme in detail, Section V describe performance analysis, Section VI presents the simulation results using AVISPA tool and Section VII, provides the conclusion.

III. PRELIMINARIES

This section of the manuscript discusses the basic security primitives, hard problems, and definitions before explaining the proposed scheme.

A. BI-LINEAR PAIRINGS (BP)

Let assume that we have two groups closed under addition and multiplication with the prime order p such as $(\mathbb{G}_1, +)$ known as an additive group and $\mathbb{G}_2$ known as a multiplicative group$(\mathbb{G}_1, *)$ having the generator g. A bi-linear pairing $\hat{e}$ map is: $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ satisfying the following basic properties of pairing [63].

- **Bi-linearity:** Let $\mathbb{P}, \mathbb{Q}$ are two points belong to $\mathbb{G}_1$ and a, b belong to $\mathbb{Z}_p^*$, compute the bi-linearity as $\hat{e}(\mathbb{P}^a, \mathbb{Q}^b) = \hat{e}(\mathbb{P}, \mathbb{Q})^{ab}$.
- **Non-degeneracy**: Let $\mathbb{P}, \mathbb{Q}$ are two points belong to $\mathbb{G}_1$ and its pair equal to 1 such that $\hat{e}(\mathbb{P}, \mathbb{Q}) = 1$, where 1 represents the multiplicative identity element of $\mathbb{G}_2$.
- **Computability**: Let $\mathbb{P}, \mathbb{Q}$ are two points belong to $\mathbb{G}_1$ and its pair such that $\hat{e}(\mathbb{P}, \mathbb{Q})$ can be computed more efficiently.
  In the BSNs, the security of patient vital signs and associated data rely on the hardness of the following computationally hard problems groups $(\mathbb{G}_1, +)$, $(\mathbb{G}_1, *)$ having prime order p, using a generator g and bi-linear map such that: $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$,

Some of the basic computationally hard problems are in the following.

Definition 1 (Computational Diffie Hellman Problem (CDHP))**.** *Let $\mathbb{G}_1$ is a group of prime order p having the generator g such that (x, y, z) are three random numbers $\in_R \mathbb{Z}_p^*$, compute (g, g^a, g^b) such that $(g^{ab}$) which is proved that it is computationally hard to solve for attacker.*

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.2020.3035324, IEEE Access

Definition 2 (Bi-linear Diffie Hellman Problem (BDHP)). *Lets to $(\mathbb{G}_1, \mathbb{G}_2)$ are two groups and (a, b, c) are random numbers belong to $\mathbb{Z}_p^*$, such that computing $(g, g^a, g^b,\ g^c)$ where $T = \hat{e}(g,g)^{abc}$, proved that the said problem computational hard for the attacker to solve.*

Definition 3 (Decisional bilinear Diffie-Hellman Problem (DBDHP)). *Lets $\mathbb{G}$ is a group of prime order p having generator $g \in \mathbb{G}$, and few random numbers $(a, b, c) \in_R \mathbb{Z}_p^*$, such that $(g, g^a, g^b,\ g^c)$ where, $T = \hat{e}g^{ab} = g^c$ whether $T = \hat{e}(g,g)^{abc}$, If (g^a, g^b, g^c) not given and element $T \in \mathbb{G}_2$. If $T = \hat{e}(g,g)^{abc}$ so we denoted that it is DBDHP $(g, g^a, g^b, g^c, T) =\gg$ Else it is denoted DBDHP $(g, g^a, g^b,\ g^c, T) = \perp$.*

Definition 4 (Gap Bilinear Diffie Hellman Problem (GBDHP)). *In the GBDH problem, let $(\mathbb{G}_1, \mathbb{G}_2, \hat{e})$ are to calculate $T = \hat{e}(g,g)^{abc}$ given $(g, g^a, g^b,\ g^c)$ using DBDHP $(g, g^a, g^b,\ g^c, T) =>$or $\perp$.*

Definition 5 (Gap Diffie Hellman Problem (GDHP)). *In the GDHP the $\mathbb{G}_1$ calculate $(g)^{ab}$ given $(g, g^a, g^b\ )$ using DBDHP procedure $(g, g^a, g^b,\ g^c, T)$= > or $\perp$.*

Definition 6 (Hyper Elliptic Curve Cryptography (HECC)). *HECC is a public cryptography method; it just like an extension of Elliptic Curve Cryptography (ECC). HECC provides the same security compared to another cryptosystem, for instance, ECC, RSA, and Digital Signature Algorithm (DSA). HECC best for resource constraint environment due to small key size, the key size of HECC is 2^{80} bits. The genus of HECC is $2, 3, 4, 5$, and 6, for the security base, the genus (2) is the most secure than others. The security of HECC depends upon a mathematically hard problem called HEC discrete logarithm problem, which prevents the attacker to break the keys even if $\mathbb{Q}$ and $\mathbb{P}$ are publicly known for it.*

Notation: $x = t\ y = u\ z = v$

The equation for HECC: $[E : u^2 + h(t)u = f(t)]h(t)$ is a polynomial of degree of a besides $h(t) \in f(t)$, and $f(t)$ is a monic-polynomial of degree $2g + 1$ and $h(t) \in f(t)$.

B. GENUS OF HECC

HECC is used to build the key encryption and decryption procedure. The polynomial of curve decided the value of g on a prime field F_p.

- **Genus** $g = 2$
  $u^2 = t^5 + \sigma_3 t^3 + \sigma_2 t^2 + \sigma_1 t + \sigma_0$
- **Genus** $g = 3$
  $u^2 = t^7 + \sigma_5 t^5 + \sigma_4 t^4 + \sigma_3 t^3 + \sigma_2 t^2 + \sigma_1 t + \sigma_0$
- **Genus** $g = 4$
  $u^2 = t^9 + \sigma_7 t^7 + \sigma_6 t^6 + \sigma_5 t^5 + \sigma_4 t^4 + \sigma_3 t^3 + \sigma_2 t^2 + \sigma_1 t + \sigma_0$
- **Genus** $g = 5$
  $u^2 = t^{11} + \sigma_9 t^9 + \sigma_8 t^8 + \sigma_7 t^7 + \sigma_6 t^6 + \sigma_5 t^5 + \sigma_4 t^4 + \sigma_3 t^3 + \sigma_2 t^2 + \sigma_1 t + \sigma_0$
- **Genus** $g = 6$
  $u^2 = t^{11} + \sigma_9 t^9 + \sigma_8 t^8 + \sigma_7 t^7 + \sigma_6 t^6 + \sigma_5 t^5 + \sigma_4 t^4 + \sigma_3 t^3 + \sigma_2 t^2 + \sigma_1 t + \sigma_0$

Definition 7 (Jacobian of HECC). *The jacobian of a curve $\mathbb{C}$ is defined on a finite field F which is represented by $J_E(F)$, and every element of the jacobian is denoted individually by a divisor $\mathbb{D}$ as in Eq.*(1).

$$J_E(F) = \frac{\mathbb{D}^\circ}{g} \tag{1}$$

$$\mathbb{D} = \sum_{P_i \in C} m_i P_i \ \ and \ \ m_i \in Z$$

Here $\mathbb{D}$ is a reduced divisor and the m_i arrow numbers on the curve, P_i arrow points on the curve. The finite number m_i cannot be zero.

A unique reduce divisor denotes every element of the jacobian (shown in Eq.(2)).

Reduce divisor form:

$$\mathbb{D} = \sum_{P_i\ \in C} m_i\ P_i\ - (\sum_{P_i\ \in C} m_i)\infty \tag{2}$$

The above equation contains only the opposite points, which are $\sum_{P_i \in C} m_i\ P_i \leq g$

The opposite point for $P(t,u) \in C$ is $\overline{P}\ (t, -u, -h(t)) \in C$ using the discrete log problem (DLP), the security of cryptosystem is enhanced and it hard to break the security of the scheme/system. In HECC, an effective procedure to compute "$\mathbb{D}$" for the bulky whole "$\mathbb{C}$" using Eq.(3).

$$\mathbb{D} = \underbrace{\mathbb{D} + \mathbb{D} + \cdots + \mathbb{D}}_{\mathbb{C}_{pa}3} \tag{3}$$

This is a group operation of addition and doubling of a divisor; which is called scalar multiplication of divisor. ECC point multiplication modifies by a divisor of the jacobian of HEC by this operation. The Fig.1 shows operation on HECC.

IV. PROPOSED SCHEME

Our scheme comprises four phases: initial setup, generation of keys for encryption/decryption, multi-receiver generalized signcryption, and generalized unsigncryption. The following Table 1 shows the notations and their descriptions used in the proposed scheme.

1) Initial Setup

The essential parameters for secure communication among biosensors, base stations, and medical servers are defined and distributed to all external users registered in a medical server. The distributed parameters contain HECC, base point, and finite field, etc.

2) Generation of Keys for Encryption and Decryption

In this phase, the biosensor $i \in \{1, 2, \ldots, P\}$ belongs to the patient, generate randomly a private key $\mathrm{Pr}_i \in \{1, 2, \ldots, n-1\}$ and calculate the public key $Pu_i = \mathrm{Pr}_i.\ G$, where $i \in \{1, 2, \ldots, P\}$. Every biosensor of the patient can send some initial parameters to the certificate authority *(C-Auth)*

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.2020.3035324, IEEE Access

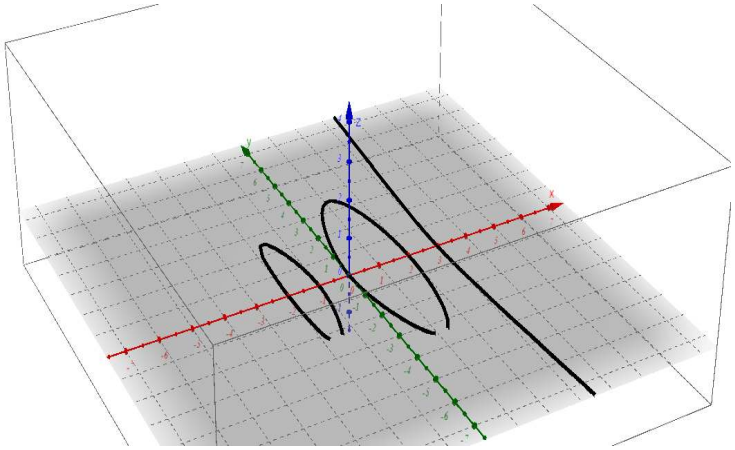

FIGURE 1: Operation of HECC

TABLE 1: Notation guide

Notation	Description
SPAN	Security Protocol Animator for AVISPA
HLPSL	High Level Protocol Specification Language
GSC	Generalized Signcryption
MRGSC	Multi-Receiver Generalized Signcryption
GUSC	Generalized Un-Signcryption
IND-CCA	Indistinguishable Chosen Ciphertext Attack
EUF- CMA	Existential Unforgeable Chosen Message Attack
HCDLP	Hyperelliptic Curve Discrete Logarithm Problem
HECDM	Hyperelliptic Curve Devisors Scalar Multiplication
ECPM	Elliptic Curve Point Multiplication
ECDLP	Elliptic Curve Discrete Logarithm Problem
PKG	Private Key Generator
CLC	Certificateless Cryptography
CDH	Computational Diffie-Hellman problem
UF-CMA	Unforgeability against Chosen-Message Attack
S_i	Body sensor/Biosensor node
C	Hyper Elliptic Curve
$\mathbb{D}$	A divisor of large prime order n in
N	Random number
φ	A function which maps a divisor to integer value
r	Number of receiver
PU_{rn}	Public key of receiver n
Pr_{ri}	Private key of receiver n
Pu_i	Public key of biosensor node
Pr_i	Private key of biosensor node
Mul	Scalar Multiplication
M_{EXP}	Modular Exponentiation
B_P	Bi-linear Paring
E_k/D_k	Encryption / Decryption with key k
H/H_k	Hash / Keyed Hash Function
m/c	Patient medical data /encoded patient data
ψ	Signcrypted text
C-Auth	Certificate Authority
$\perp$	Reject

for obtaining his public key certificate. This certificate as used for verification of the public key on the receiver side.

3) Multi Receiver Generalized Signcryption

Let a biosensor want to transmit a patient sensitive information $m \in M$ to a group of receivers having identification number $(ID_1, ID_2, \ldots, ID_n)$ and public keys $(PU_{r1}, PU_{r2}, \ldots, PU_{rn})$ in a confidential or authentic, or confidential and authenticated fashion.

Biosensor nodes transmitted patient sensitive data in the signcrypted form $\psi = (c, \omega, s, Z)$ to multiple receivers using the following algorithm (1).

The following Fig. 2 shows the proposed multi-receiver generalized signcryption architecture for BSNs.

4) Generalized Unsigncryption

In this section, each external user has a unique identity ID_i for authentication. If a user wants to join the BSNs and access patient information, so in this case, the authenticity of the user is verified by using MS pre-defined rules and policies if it is declared as a valid user, so the permission is granted otherwise blacklisted and isolated from the BSNs. The following algorithm (2) is used for the generalized unsigncryption process.

A. WORKING MODES OF GENERALIZED SIGNCRYPTION

Our proposed efficient attribute-based multi-receiver generalized signcryption scheme used three modes according to the security point of view. In the first mode, signcryption only mode used to get both data confidentiality and authenticity properties in a single logical step; second, we apply the signature only mode if only the data authenticity is required, while in third, we can use the encryption only mode if required only data confidentiality. A generalized signcryption algorithm is more suitable for the resource-constrained and smart environment of BSNs.

1) Only Signcryption Mode

In this section, the signcryption only mode algorithm was designed for BSNs to obtain both security properties of data authentication and confidentiality simultaneously during transmission of patient information from biosensor nodes to MS. For example the $mode_{\text{signature}} \neq 0$ and $mode_{\text{encryption}} \neq 0$; therefore, any biosensor node who knows the doctor public

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.2020.3035324, IEEE Access

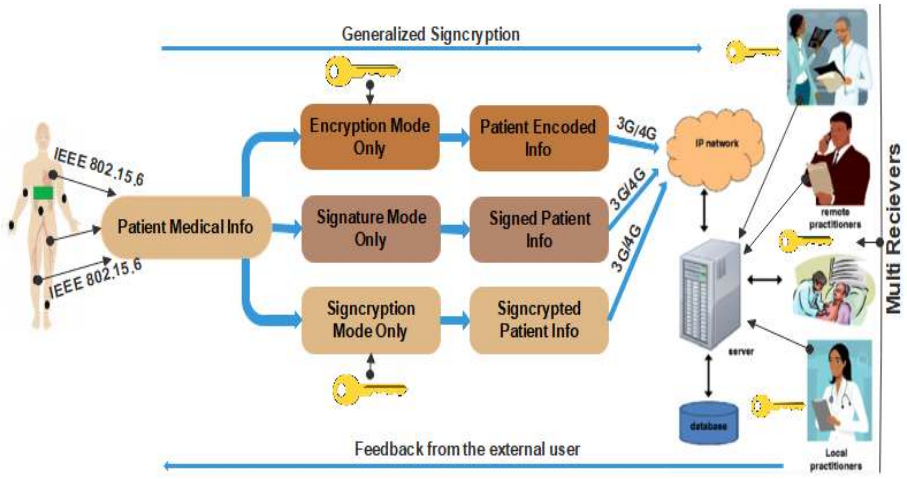

FIGURE 2: Proposed scheme architecture

key and satisfied the attribute-based access structure can signcrypt the patient medical information using algorithm (1) and transmitted toward the MS. In this mode, the input parameters were taken, such as public keys of receiver's $(PU_{r1}, PU_{r2}, \cdots, PU_{rn})$, private key of biosensor(Pr_i), patient medical data(m), and some other system parameters to secure patient sensitive medical information from adversaries attacks during transmission. Random number $N \in_R \{0, 1, \cdots, n-1\}$ was selected to computes $(Z = N \cdot D)$ using multiplication of random number (N) and (D) which is divisor of large prime order (n). Moreover, a random value of $T \in_R \{0, 1, \cdots, n-1\}$ can be selected and apply the one-way hash function to computes $(X_T||Y_T = H_1(T))$. Now the transmitted patient medical data and (X_T) are concatenated and apply a hash to computes $(U = H_2(\text{Patient medical Data}||X_T)$. Additionally, to ensure data confidentiality and authentication, the signcryption algorithm was applied on the biosensor side in which $mode_s \neq 0, mode_e \neq 0$, and transmitting the encoded patient information $(\psi = (C, W, S, Z))$ toward the MS to performed action on data by multiple legitimate receivers and provide feedback to the concerned patient if any abnormalities happened. Each legitimate receiver gets the verified patient medical data using the following secure and efficient deterministic algorithm (2).

Algorithm 1 MRGSC (Signcryption Mode)

Input$((PU_{r1}, PU_{r2}, \ldots, PU_{rn}, mode_s, mode_e, m, Pr_i))$

1) Randomly integer selection $N \in_R \{0, 1, \ldots, n-1\}$
2) Generated $Z = N \cdot \mathbb{D}$
3) if $mode_{encryption} = 0$ and C =patient medical data $(m), W = \Phi$
   else
   a) Choose random value $T \in_R \{0, 1, \ldots, n-1\}$
   b) Computes $X_T||Y_T = H_1(T)$
   c) Computes $U = H_2$ (Patient medical Data $||X_T)$
   d) Computes encoded text $C = Enc(Y_T$, Patient medical Data $||Z)$
   e) For each receiver $i = 1 to\ r$
   a) Computes $X_N||Y_N = H_3(N.PU_{ri})$
   b) Computes $C_i = Enc(Y_N, T||X_{xN})$
   c) $W = (C_1, C_2, C_3, C_4, \ldots, C_r)$
4) if $\text{mode}_{\text{signature}(s)} = 0,\ s = \Phi$
   else
5) Computes $L = H_2(\text{Patient medical Data}||X_T||Z)$
6) Computes $S = (\frac{N}{(Pr_i + L)}) mod\ n$

Now transmitted patient medical data in the signcrypted form $\psi = (C, W, S, Z)$

2) Only Signature Mode

In this section, biosensor nodes sign the patient medical information by using an algorithm (3) to accomplished data authentication. Furthermore, using this algorithm, MS can validate that the received data is original and get from a truthful entity. In this mode, the input parameters were taken, such as the private key of biosensor node (Pr_i), patient medical data (m), and some other system parameters to ensure patient data authenticity in the resource-constrained environment of BSNs. Moreover, $mode_{\text{signature}} \neq 0$ and $mode_{\text{encryption}} = 0$, will be considered signing the patient digital record.

All legitimate external users can verify the above patient data that knows the biosensor node public key using an algorithm (4).

3) Only Encryption Mode

In this section, the proposed algorithm (5) represents only encryption mode. This algorithm encrypts the sensed patient vital signs to accomplished patient data confidentiality. The encrypted patient data are safely transmitted toward the MS using public networks, and adversaries cannot modify 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.2020.3035324, IEEE Access

Algorithm 2 GUSC $(C, C_i, S, Z, PU_i, \mathrm{Pr}_{ri})$

1) Verification of biosensor node public key PU_i using their certificate from Certificate Authority(C-Auth)
2) if $W = \Phi$, patient medical data $(m) = C, X_T = 0$
   else
   {
   a) Computes $X_N||Y_N = H_3(\mathrm{Pr}_{ri} \cdot Z)$
   b) Computes $T||X_N = Dec(Y_N, C_i)$
   c) Computes $X_T||Y_T = H_1(T)$
   d) Computes $m||U$ = Dec (Y_T, C)
   e) Computes $U^{'} = H_2$ (patient medical data $||X_T)$
   f) If $U' = U$, accepted patient medical data otherwise $\perp$
   }
3) if $S \neq \Phi$
   {
   a) Computes $L = H_2($ patient medical data$||X_T||Z)$
   b) Computes $Z' = S \cdot (PU_i + L \cdot \mathbb{D})$
4) If $Z' = Z$ Accepted patient data as valid else $\perp$ }

Algorithm 3 MRGSC (Only Signature Mode)

Inputs $(mode_{\text{signature}}, mode_{\text{encryption}},$ patient data (m), Pr_i, $PU_{r1}, PU_{r2}, \ldots, PU_{rn})$

1) Choose random integer value $N \in_R \{0, 1, \ldots, n-1\}$
2) Computes $Z = N \cdot \mathbb{D}$
3) if $mode_{encryption} = 0, C =$ patient medical data $(m), W = \Phi$
4) $mode_{signature} \neq 0$
5) Computes $L = H_2$ (patient medical data $||Z)$
6) Computes $S = (\frac{N}{(\mathrm{Pr}_i + L)})$ mod n
7) Return $\psi = (C, S, Z)$
   Disseminated signcrypted patient medical data $\psi = (C, S, Z)$

sensitive data for illegal activities. Moreover, only legitimate receivers, such as doctor, nurse, microbiologist, government agency, insurance company, and family members can decrypt/access the patient encoded data whose access structure matched with predefine access policies stored on MS. The biosensor node can encrypt a patient vital signs, such as EEG, ECG, EMG, blood pressure, and temperature for (n) external users/receivers. In this mode, the input parameters were taken such as, public keys of receiver's $(PU_{r1}, PU_{r2}, \cdots, PU_{rn})$, patient medical data (m), and some other system parameters to secure patient sensitive medical information from adversaries attacks during communication from biosensor nodes to MS using public networks. Furthermore, random number $N \in_R \{0, 1, \cdots, n-1\}$ was selected to computes $(Z = N \cdot D)$ using multiplication of random number $(N)$and (D) which is divisor of large prime order (n). Moreover, a random value $T \in_R \{0, 1, \ldots, n-1\}$ can be selected and apply one-way hash function to computes $(X_T||Y_T = H_1(T))$. Now the transmitted patient medical data and (X_T) are concatenated and apply hash to computes

Algorithm 4 GUSC $(C, S, Z, PU_{ri}, \mathrm{Pr}_{ri})$

1) Receiver first verifies the public key PU_i of biosensor node using their certificate from C-Auth. {
2) if $W = \Phi$, patient medical data$(m) = C, X_T = \Phi$
3) $S \neq \Phi$
   a) Computes $L = H_2($patient medical data$||X_T||Z)$
   b) Computes $Z^{'} = S \cdot (PU_i + L \cdot \mathbb{D})$
4) if $Z^{'} = Z$ Accepted patient data as valid else $\perp$ }

$(U = H_2(PatientmedicalData||X_T)$. Also, to ensure patient data confidentiality, we apply the encryption only mode algorithm on biosensor side in which $mode_{\text{signature}} = 0$,$mode_{\text{encryption}} \neq 0$ and transmitted the encoded patient information $(\psi = (C, W, Z))$ toward the MS.

Algorithm 5 MRGSC (Only Encryption Mode)

Inputs $(\text{mode}_{\text{signature}}, \text{mode}_{\text{encryption}}, \text{patient data}(m), Pr_i, PU_{r1}, PU_{r2}, \ldots, PU_{rn})$

1) Choose random integer value N $\in_R \{0, 1, \ldots, n-1\}$
2) Computes $Z = N \cdot \mathbb{D}$
3) if mode$_{\text{encryption}} \neq 0$
4) Choose random integer value $T \in_R \{0, 1, \ldots, n-1\}$
5) Computes $X_T||Y_T = H_1(T)$
6) Computes $U = H_2($patient medical data$||X_T)$
7) Computes encoded text:
   $C = Enc(Y_T,$ patient medical data $||U)$
8) For each receiver $i = 1 to\ r$
   a) Computes $X_N||Y_N = H_3(N \cdot PU_{ri})$
   b) Computes encoded text $C_i = Enc(Y_N, T||X_N)$
   c) $W = \{C_1, C_2, C_3, \ldots, C_r\}$
9) $if\ mode_{signature} = 0,\ s = \Phi$
   Transmitted encrypted patient medical data $\psi = (C, W,$ Z$)$

Each receiver can get the patient's sensitive medical data using the following deterministic algorithm (6).

Algorithm 6 GUSC $(C, C_i, S, Z, PU_i, \mathrm{Pr}_{ri})$

1) Verification of biosensor node public key PU_i using their certificate from C-Auth.
   {
2) If $W \neq \Phi$
3) Computes $X_N||Y_N = H_3(\mathrm{Pr}_{ri} \cdot Z)$
4) Computes $T||X_N = Dec(Y_N, C_i)$
5) Computes $X_T||Y_T = H_1(T)$
6) Computes (patient medical data$||U) = Dec(Y_T, C)$
7) Computes $U^{'} = H_2($patient medical data$||X_T)$
8) If $U^{'} = U$ information valid and accepted else $\perp$
9) $s = \Phi$
   }

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.2020.3035324, IEEE Access

B. ATTRIBUTE BASED ACCESS CONTROL ARCHITECTURE (ABACA) FOR BSNS

ABACA contains four major components that process external users' policies and then decide based on user policies. If the policy matched, it granted the user permission to access the patient data; otherwise, they discard the policy. The Fig. 3 shows proposed ABACA.

i) Policy Enforcement Point (PEP), The PEP is responsible for protecting and review the external user request for accessing patient information, then makes an authorization appeal for transmitting toward the PDP.
ii) Policy Decision Points (PDP), In ABAC architecture, PDP works as a brain that evaluates the external user, i.e., doctor incoming requests for patient sensitive records against policies. Permit or deny the decision performed by PDP and access additional attributes if missing from PIP.
iii) Policy Information Point (PIP), The PIP provides an interface between external sources of patient information (LDAP or databases) and PDP. If decision-making requires extra attributes from PDP, so we access these attributes from PIP.
iv) Policy Administration Point (PAP), The PAP is a device used to generate the PDP policies for decision-making.

In our proposed ABACA, we have applied the Extended Access Control List (EACL) concept inside the PDP to filter and efficiently distinguish the data using various parameters. Furthermore, PDP permits or denies the doctor's request on the bases of attribute-based policies. Incase doctor request/ policy matched with pre-define attribute-based access policies stored inside the MS so that permission will be granted to the authorized doctor; otherwise, deny/blacklisted the concerned doctor's request and stored the record for future use. Additionally, this technique system administrator achieved greater flexibility to design smart privacy-preserving attribute-based access control architecture for BSNs.

C. ATTRIBUTE BASED GSC MODEL FOR BSN

In our proposed attribute-based GSC model, the registered data user, i.e., (doctor), sends a request to KGC (Key Generation Center) for obtaining the secret attribute key. Furthermore, KGC computes the secret attribute keys for patient data accessing using their master key and other preloaded secret parameters. Using that secret attribute key, the data user gained access to the medical server and received the particular patient encoded data for further processing. Additionally, in this paper, security policies are statements that combine patient attributes using boolean logic (AND & OR) gates to specify the rules for permitting/ denying patient sensitive data. Only the legal users can access the patient data whose access structure matched with the preloaded access structure of the server in BSNs. Fig. 4 shows the proposed attribute-based GSC model for BSNs.

D. PROPOSED MODIFIED PRIORITY BASED SCHEDULING

In modified priority-based scheduling algorithm, the Base Station (BS) prioritized the received patient data using algorithm (8) and assign high priority to emergency patient data instead of normal patient data for delay less communication. Due to this method doctor earlier diagnosis the concerned patient disease and provides better treatment for the patient in minimal time consumption to increase the patient quality of life in BSNs. Fig. 5 shows the modified priority-based scheduling process.

V. PROPOSED SCHEME PERFORMANCE ANALYSIS

In the performance analysis section, we proved the efficiency, correctness, and security of the proposed three modes. Moreover, we have discussed the threat model, security model, and informal security model in detail.

A. PROPOSED SCHEME CORRECTNESS ANALYSIS

In the correctness analysis of the proposed scheme, we used three different theorems to prove the consistency of encryption, signature, and signcryption only mode along with judge verification.

Theorem V.1. ***Signature only mode***

We used theorem (1) to prove the signature only mode for obtaining data authentication. In this case, the signature/ verification is legal if and only if the biosensor node and external user, i.e., doctor, verify the following equation:

$$S \cdot (PU_i + L \cdot \mathbb{D}) = Z$$

Let us proof the right side:
$S \cdot (PU_i + L \cdot \mathbb{D})$

$= (\frac{N}{(Pr_i + L)})(Pr_i \cdot \mathbb{D} + L \cdot \mathbb{D})$

$= \frac{N \cdot \mathbb{D}}{(Pr_i + L)}(Pr_i + L)$

$= N \cdot \mathbb{D} = Z$

Now evidently, the equation $S \cdot (PU_i + L \cdot \mathbb{D}) = Z$ *is proved.*

Theorem V.2. ***Encryption only mode***

We used theorem (2) to prove encryption only mode for obtaining data confidentiality. In this case, encryption/decryption is legal if and only if the biosensor node and external user, i.e., doctor, verify the following equation:

$$Pr_{ri} \cdot Z = Pr_{ri} \cdot N \cdot PU_{ri}$$

Let us proof the left side:
$Pr_{ri} \cdot Z$
$= Pr_{ri} \cdot N \cdot \mathbb{D} = N \cdot Pr_{ri} \cdot \mathbb{D}$
$= N \cdot PU_{ri}$
Now evidently, the equation.
$Pr_{ri} \cdot Z = N \cdot PU_{ri}$ *is proved.*

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.2020.3035324, IEEE Access

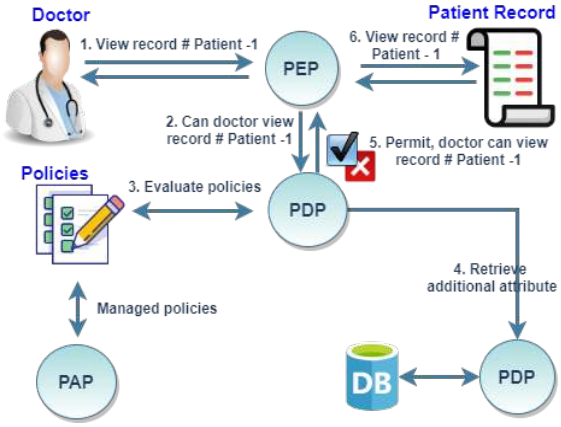

FIGURE 3: Proposed attribute-based access control architecture

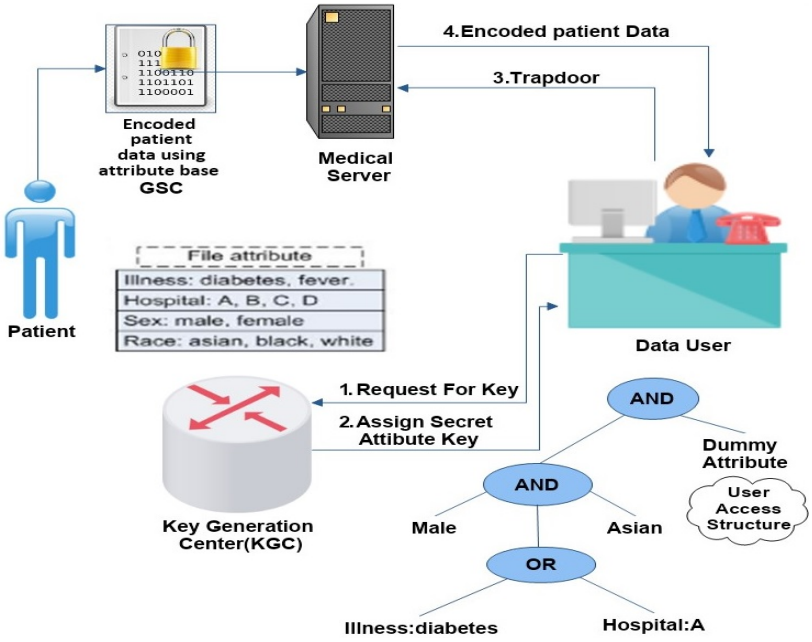

FIGURE 4: Proposed attribute based GSC model for BSNs

Theorem V.3. ***Signcryption only mode***

We used theorem (3) to prove signcryption only for obtaining data authenticity and data confidentiality. In this case, signcryption/unsigncryption is legal if and only if the biosensor node and external user, i.e., doctor, verify the following equation:

$$Pr_{ri} \cdot Z = Pr_{ri} \cdot N \cdot PU_{ri} \;\; \&$$
$$S \cdot (PU_i + L \cdot \mathbb{D}) = Z$$

Now evidently, both the equation holds as proved in theorem (2 and 3).

B. SECURITY ANALYSIS

In this section, we study the fundamental security properties needed for secure communication in BSNs. Moreover, using HCDLP and HCDHP assumptions [21], we prove that our proposed scheme is secure and infeasible for an attacker to get the secret key because it satisfies all the essential security properties and protects the patient sensitive medical information from disclosure. We used HECC for patient data security, which consumes fewer resources and provides adequate security using HCDLP mathematical hard problem and hash function. The following Table 2 shows the comparison of the proposed scheme's security properties and existing schemes.

1) Data Confidentiality (IND-CCA)

To prevent patient medical information from revelation, BSNs needs data confidentiality. In disseminating patient data from the biosensor node to the medical server, there is a probability of eavesdropping the patient's sensitive information by the enemy/adversary. To obtain data confidentiality, we must share secret keys on a secure channel or convert plaintext data into encoded text.

Let an adversary want to get the sensitive patient informa-

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.2020.3035324, IEEE Access

tion from signcrypted text $\psi = (C,\ W, S, Z)$, the adversary must get secret key Y_N. Moreover, obtaining the secret key Y_N is hard and equivalent to solve HCDLP.

Case (1): An adversary can calculate Y_N using Eq. (5), if the adversary calculate Pr_{ri} using Eq. (4). The adversary obtains PU_{ri} simply, but if efforts to compute Pr_{ri} from Eq. (4), and then adversary need to computes HCDLP.

$$PU_i = Pr_i \cdot \mathbb{D} \tag{4}$$

$$X_N||Y_N = H_3(Pr_{ri} \cdot Z) \tag{5}$$

Case (2): An adversary knows $PU_{ri} = \mathrm{Pr}_{ri} \cdot \mathbb{D}$ and $Z = N \cdot \mathbb{D}$ so it can generate Y_N using Eq. (7), if adversary generate K using Eq. (6) but if attempts to generate K using $PU_{ri} = \mathrm{Pr}_{ri} \cdot \mathbb{D}$ and $Z = N \cdot \mathbb{D}$, is computing HCDLP.

$$K = Pr_{ri} \cdot N \cdot \mathbb{D} \tag{6}$$

$$X_N||Y_N = H_3(K) \tag{7}$$

2) Data Integrity

In our proposed scheme, the medical server can check the integrity of patient medical information by using Eq. (8) and Eq. (9) that the patient medical information is either original or modified. If an adversary modify $C\ \ as\ C'$ so, the related patient medical data (m) is modified to m' and $m \neq m'$ and $L' \neq L$. For adversary, it is hard and infeasible computationally to change $C \neq C'$ such that $L' = L$ using hash function. Using Eq. (10), it is proved that the received data is original and not altered.

$$L = H_2(\text{patient medical data}(m)||X_T||Z) \tag{8}$$

$$Z' = S \cdot (PU_i + L \cdot \mathbb{D}) \tag{9}$$

$$Z' = Z \tag{10}$$

3) Data Un-forgeability (EUF-CMA)

Supposed an adversary/receiver forge a legal (m, S', Z') using the previous one that adversary overheard/received. They must compute S' from Eq. (12) for the patient medical data m. Moreover, to generate S', adversary needs to calculate Pr_i using Eq. (4) and N from Eq. (11) which is same to computes two HCDLP hard problems, and a doctor can calculate Pr_i from Eq. (4) that is same to computes single HCDLP. Moreover, we proved that our proposed model is un-forgeable.

$$Z = N \cdot \mathbb{D} \tag{11}$$

$$S' = \left(\frac{N}{(\mathrm{Pr}_i + L)}\right) \bmod n \tag{12}$$

4) Patient Data Authentication

Authentication is a process through which legal and illegal data and nodes are verified. In our proposed scheme, the authentication of the biosensor is checked using a public key certificate, while in the medical server-side, we used one-way hash function: $L = H_2$ (patient medical data $(m)\ ||X_T||\ Z$), data signature S used $Z' = S \cdot (PU_i + L \cdot D)$ and authenticate the patient data validity using $Z' = Z$.

5) Non-Repudiation

If a dispute occurs between a biosensor node and a medical server, a reliable judge/party can solve the problem in our proposed scheme. The receiver transferred (m, X_T, Z) to the judge/party, and the judge used the following algorithm (7) to resolve the clash.

Algorithm 7 Judge Verification

Input (patient medical data $(m), X_T, Z, PU_i)$

1) Verification of biosensor node public key PU_i using their certificate
2) Computes $L = H_2(\text{patient medical data}(m)||X_T||Z)$
3) Computes $Z^{'} = S \cdot (PU_i + L \cdot \mathbb{D})$
4) Patient medical information is disseminated by the biosensor node having public key PU_i
5) $Z' = Z$
6) Else
7) Rejected $\perp$

6) Forward Secrecy

Supposed an adversary computes biosensor private key Pr_i, he still unable to get previous session patient medical data m from the available signcrypted text $\psi = (C, W, S, Z)$. Supposed an adversary computes the secret key Pr_i, still he require L for Eq. (13) which is generated from Eq. (14) encoded text. Moreover, adversary cannot access any previous session patient information and computationally hard to get valid L without knowing original patient medical data m.

$$L = H_2(\text{patient medical data } m||X_T||Z) \tag{13}$$

$$N = (L + Pr_i)^{-1} \cdot S \tag{14}$$

C. THREAT MODEL

In this paper, we have used the concept of a well-known threat model called Dolev-Yao (DY) [57]. According to the Dolev-Yao threat model's rule and regulations, transmission between any two systems is performed using public networks. In this model, the end node of communication is considered untrustworthy. Moreover, due to the open channel on a public network, the patient information is easily modified by the adversaries for illegal activities during the transmission from biosensor nodes to MS. Additionally, some biosensor nodes or MS are quickly imprisoned by adversaries to misuse the patient's sensitive information for specious activities. Furthermore, in case the smartphone of a doctor lost or stolen, then adversaries can extract the secret password of the MS easily to performed various attacks on patient data stored on MS, such as main in the middle attack, reply attack,

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.2020.3035324, IEEE Access

TABLE 2: Security properties comparison of proposed scheme and existing schemes

Scheme	SP_1	SP_2	SP_3	SP_4	SP_5	SP_6	SP_7
Proposed	✓	✓	✓	✓	✓	✓	✓
YXM. [31]	×	✓	✓	✓	✓	×	×
HYX. [32]	×	✓	✓	✓	✓	✓	×
ZC. [33]	✓	✓	✓	✓	✓	✓	×
ZC.[[34]	✓	✓	✓	✓	✓	×	×
CMA. [35]	✓	✓	✓	✓	✓	×	✓
ZYH. [36]	✓	✓	✓	✓	×	×	×
HRC. [37]	✓	✓	✓	✓	✓	✓	×
TMA. [38]	✓	✓	✓	✓	×	✓	✓
MR. [39]	✓	✓	✓	✓	✓	×	✓
CN. [40]	✓	✓	✓	✓	×	×	×
CWQ. [41]	✓	✓	✓	✓	✓	✓	×

SP_1 = Confidentiality SP_2 = Integrity SP_3 = Authentication SP_4 = Un-forgeability
SP_5 = Non-repudiation, SP_6 = Encoded text verifiability, SP_7 = Forward secrecy

offline password guessing attack, and privileged insider attack to access the patient sensitive medical information from MS for illegal usage. To preserve patient data security and privacy, we must need to protect the resource-constrained environment of BSNs from possible threats. In our proposed scheme, we have designed a novel, lightweight, and secure attribute-based multi-receiver generalized signcryption for BSNs to enhance patient data security and privacy with minimal cost and protect the patient information stored on MS from adversaries' attacks. Our proposed generalized signcryption is the advanced version of the signcryption algorithm that can adaptively work as encryption mode, signature mode, or signcryption mode with only one algorithm. If we required only the patient data's confidentiality so, we could apply the concept of only encryption mode. If only needed authenticity of the patient data so, we can apply only signature mode. If required, both confidentiality and authenticity of patient data can use the concept of only signcryption mode.

Additionally, in this paper, we have designed an adequate fine-grain access control mechanism to manage data privacy and external users' activities. Each external user must be authenticated; if it is declared a valid user, the permission is granted; otherwise, the user is blacklisted and isolated from the BSNs. ABAC is also known as policy-based access control, which evaluates attributes such as user attributes, environment attributes, and resource attributes.

Moreover, access rights are granted to different users using pre-defined attribute-based policies; the system administrator designed them. Our proposed Attribute-Based Access Control (ABAC) technique is efficient and suitable for the resource-constrained environment of BSNs.

Furthermore, in our proposed scheme, KGC computes the secret attribute-based keys for patient data accessing using their master key along with other preloaded secret parameters for a particular session. Moreover, data users use the computed secret attribute-based key and pre-define policies to access the medical server and receive the specific patient encoded data from the server for further analysis and diagnostics. Furthermore, we simulate the proposed scheme via the AVISPA tool to demonstrate that it can meet the security requirements such as data confidentiality (IND-CCA), integrity, unforgeability (EUFCMA), patient data authenticity, forward secrecy, and non-repudiation distinctly in the ROM with minimal cost.

D. SECURITY MODEL

In this section, we validate the formal security model of our proposed lightweight and secure attribute-based multi-receiver generalized signcryption that fulfill the data confidentiality (IND-CCA) in encryption only mode or signcryption only mode. Furthermore, data unforgeability (EUFCMA) must satisfy in signature only mode or signcryption only mode. In this paper, we have discussed two types of adversaries, i.e., Type-I and Type-II adversaries.

A typical user can not change the public key certificate issued by the certificate authority to the patient to verify the public key on the receiver side. While Type-I adversaries can replace the patient public key adaptively. Moreover, Type-II adversaries are not able to change the patient public key.

Initial setup: The essential parameters for secure communication among BSNs tier -1, tier-2 and tier- 3 are defined and distributed among external shareholders (doctor, nurse, researcher, etc.) that are legal and pre-registered with the medical server in the time of registration.

Secret Key-Gen: Deployed patient biosensor $i \in \{1, 2, \ldots, P\}$ generate randomly private key $(Pr_i) \in \{1, 2, \cdots, n-1\}$ and calculates public key $Pu_i = (Pr_i \cdot G)$ where $i \in \{1, 2, \cdots, P\}$. Every biosensor of the patient can send some initial parameters to certificate authority (C-Auth) for obtaining his public key certificate. Now using secret key patient data $m \in M$ encrypted and transmitted toward multiple receiver.

Phase-I: adversary ($\mathcal{A}$) produced a polynomial number of bounded queries for the following oracles.

MRGSC: Patient sensitive information $m \in M$ transmitted to a group of receivers having identifi-

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.2020.3035324, IEEE Access

cation number $(ID_1, ID_2, \cdots, ID_n)$ and public keys $(PU_{r1}, PU_{r2}, \cdots, PU_{rn})$ in a confidential or authentic, or confidential and authenticated fashion. Biosensor nodes transmitted patient sensitive data in signcrypted form $\psi = (c, \omega, s, Z)$ to multiple receivers using algorithm (1). Input $(PU_{r1}, PU_{r2}, \cdots, PU_{rn}, mode_s, mode_e, m, Pr_i)$ and randomly select $N \in_R \{0, 1, \cdots, n-1\}$ to computes $(Z = N \cdot D)$. If $mode_{\text{encryption}} = 0$ and C =patient medical data (m), $W = \Phi$ so, choose random value $T \in_R \{0, 1, \ldots, n-1\}$ and calculate $(X_T || Y_T) = H_1(T)$. Now generate $U = H_2(\text{Patient medical Data} || X_T)$ using hash function. Moreover, for secure transmission of encoded data to each receiver $i = 1$ to r.

$C = Encrypte(Y_T, \text{Patient medical Data} || Z$

$X_N || Y_N = H_3(N \cdot PU_{ri})$

$C_i = \text{Encrypt}(Y_N, T || X_{xN})$

$W = (C_1, C_2, C_3, C_4, \cdots, C_r)$

if $mode_{\text{signature(s)}} = 0, s = \Phi$ else

$L = H_2(\text{Patient medical Data} || X_T || Z$

$S = (\frac{N}{(Pr_i + L)}) \text{mod} n$

Now communicate $\psi = (C, W, S, Z)$ to multiple external users. MRGSC algorithm work in three different modes according to the user needs.

1) **Encryption mode:** If ID_s is null and ID_r is not and $\text{mode}_{\text{encryption}} \neq 0$, then the GSC encoded text $\psi = (C, W, Z)$ is an encryption ciphertext.
2) **Signature mode:** If ID_r is null and ID_s is not and $mode_s \neq 0$ and $mode_e = 0$ then the GSC text $\psi = (C, W, Z)$ is an signature text.
3) **Signcryption mode:** If neither $ID_s nor ID_r$ is null, and($mode_{encryption} \neq 0$ & $mode_{signature} \neq 0$,then the GSC text $\psi = (C, W, Z)$ is an signcrypted text.

GUSC: Let patient identity ID_s and external receiver identity ID_r and $W \neq$, external receiver gets the patient data $m \in M$ in encryption or signcryption mode or revenues accurate in signature mode; normally run by receiver ID_r in a signature mode.

$X_N || Y_N = H_3(Pr_{ri} \cdot Z)$

$T || X_N = Decrypte(Y_N, C_i)$

$X_T || Y_T = H_1(T)$

$(\text{patient medical data} || U) = Decrypte(Y_T, C)$

$U' = H_2(\text{patient medical data} || X_T)$

If $U' = U$ patient data valid and accepted else $\perp$ and $s \neq \Phi$

$L = H_2(\text{patient medical data} || X_T || Z)$

$Z' = S \cdot (PU_i + L \cdot D)$

$Z' = Z$

GUSC algorithm also works in three different modes according to the sender's needs.

1) **Decryption mode:** If ID_s is null and ID_r is not, it works in decryption mode.
2) **Signature verification mode:** If ID_r is null and ID_s is not so, it works in verification modes.
3) **Unsigncryption mode:** If neither ID_s nor ID_r is null, it works in this mode.

The following queries can be adaptively asked.

Challenger (Ch): Two vectors of patient medical data are produced by adversary (**A**) such as $M_0^* = \{m_{0i}^*, i = 1, \cdots, n\}$, $M_1^* = \{m_{1i}^*, i = 1, \cdots, n\}$, and biosensor arbitrary private key (Pr_i), $\mathcal{B}$ flips a coin $b \in \{0, 1\}$ to generate a signcrypted text $\psi = (C, W, S, Z)$ under the adversaries attacked biosensor public keys (P_{ui}), $N \in_R \{0, 1, \cdots, n-1\}$ to computes $(Z = N \cdot D)$. Furthermore, jacobian of a curve C are defined on finite field F which is represented by $J_E(F)$, and every element of jacobian are denoted individually by divisor $D \cdot \{J_E(F) = \frac{D^\circ}{P}\}, \{D = \sum_{P_i \in C} m_i P_i\}$ and $\{m_i \in Z\}$. Here D is the reduce divisor and the $m_i \rightarrow$ Numbers on the curve, $P_i \rightarrow$ points on the curve. The finite number m_i are cannot be zero. Every element of the jacobian are denoted by unique reduce divisor. The reduce divisor for $[D = \sum_{P_i \in C} m_i P_i - (\sum_{P_i \in C} m_i) \infty]$. Now $\mathcal{B}$ return ψ to adversary $(\mathcal{A})$ as a challenge.

Phase-II: In this phase adversary $(\mathcal{A})$ produced polynomial number of bounded new queries under the restriction, such as adversary $(\mathcal{A})$ should not computes the GUSC (ψ, Pr_i, Pr_{ri}), $(N \in_R 0, 1, \cdots, n-1)$ to compute $(Z = N \cdot D)$.

Guess: In this phase, when the game terminates, the output of adversary $(\mathcal{A}) = b_0$. $(\mathcal{A})$ will be consider the winner of the game if and only if $b_0 = b$. The benefit of the adversary $(\mathcal{A})$ is described as: $Adv^{IND-MRGSC-CCA2}(\mathcal{A}) := 2Pr[b_0 = b] - 1$.

E. INFORMAL SECURITY ANALYSIS OF PROPOSED ARCHITECTURE

We have demonstrated using formal security analysis in the security model. Our proposed lightweight attribute-based multi-receiver generalized signcryption scheme is secure against Type-I and Type-II adversaries attacks. Additionally, we have satisfied that our scheme provides data confidentiality, unforgeability, integrity, and patient data authenticity in the ROM. Furthermore, using informal security analysis, we have proved that our scheme resists other potential attacks, which are discussed in the below sections one by one.

1) Protection Against Replay Attack

Proof: In this scheme, we have used the concept of time stamp (TS) during the communication between source and destination to ensure that the patient sensitive data received by the external users are new and fresh. Moreover, only the targeted receiver can access the patient data whose access policies are matched with pre-define access structure

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.2020.3035324, IEEE Access

designed by the system administrator. Our scheme provides resistance against replay attacks.

2) Protection Against Man-in-the-Middle Attack

Proof: Patient medical information $m \in M$ transmitted to a group of receivers having identification number $(ID_1, ID_2, \cdots, ID_n)$ and public keys $(PU_{r1}, PU_{r2}, \cdots, PU_{rn})$ in a confidential or authentic, or confidential and authenticated fashion. Biosensor nodes transmitted patient sensitive data in signcrypted form $(\psi = (c, \omega, s, Z))$ to multiple receivers using algorithm (1). Only the legitimate user can encrypt and decrypt the patient data by using predefine attribute-based access policies. In this scheme, adversaries cannot guess the secret key (Y_N) for illegal activities. Moreover, Obtaining the secret key (Y_N) is hard and equilent to solve the HECDLP. Therefore, our lightweight scheme provides resistance against man-in-the-middle attacks.

3) Protection Against Offline Password Guessing Attack

Proof: The patient-related records are stored inside the MS for diagnostics of patient disease and delay less treatment. Therefore, each external user(doctor) who wants to get medical data of a particular patient must be registered with MS to manage medical information's real-time data privacy. Furthermore, in case the smartphone of a doctor is lost or stolen so the adversaries cannot guess the secret password of the MS to access the patient's sensitive medical information from MS for misuse. At the same time, illegal users are blocked and isolated from BSNs. Our scheme provided resistance against offline password guessing attacks.

4) Protection Against Privileged Insider Attack

Proof: Using attribute-based multi receivers generalized signcryption, we have protected the abuse of the privileges. Moreover, permission is granted to access the patient's sensitive data if the attribute-based access policies matched; otherwise, discard the user's request. The system administrator classifies the register users' attributes into different classes, which enhanced the data security and privacy of patient data stored in MS. Furthermore, using pre-define attribute-based policies, we can overcome the prohibited actions inside the BSNs.

F. COST ANALYSIS

This section computes our proposed scheme's processing cost and transmission cost and then compares the proposed scheme with exiting multi-receiver generalized signcryption schemes and signcryption schemes. The main objective of resource-constrained environments is to design a smart and optimal cryptosystem that reduces the processing cost and transmission overhead.

1) Comparative Processing Cost Analysis

This section compared our proposed scheme's processing cost with other exiting schemes in terms of major and expensive operations. It identified in the proposed and existing schemes that the costly and major operations are HECDM and ECPM.

Now, we compared and analyzed the proposed scheme costly operation HECDM with other exiting schemes concerning ECPM. The comparative processing cost analysis of the existing scheme and the proposed scheme is checked in the parallel environment on a personal computer running JDK 1.6 on Microsoft window 10 having an Intel microprocessor of four cores 2.6 GHZ speed along with 8GB RAM. In this environment, One ECPM on ECC takes 4.24 ms while one HECDM on HECC takes 2.2 ms [31, 32]. In our proposed multi-receiver generalized signcryption, it involves totally 3 HECDM, 1 DIV operation, 1 MUL operation, 1 Add operation, 1 Sub operation and 6 Hash functions. The HECDM, DIV, and MUL are major operations, while Add, Sub, and Hash are miners and negligible operations. According to the results shown in tables 3 and 4, the proposed scheme is more suitable for the resource-constrained environment of BSNs. It consumes fewer CPU cycles than other exiting schemes shown in tables 3 and 4 because it contains fewer major operations. Our proposed scheme fulfills all the security properties mentioned in table 2, i.e., confidentiality, authentication, integrity, non-repudiation, unforgeability, forward secrecy, and chipper text verifiability. All three modes of the proposed scheme are efficient in terms of cost and memory. Moreover, Table 5 shown the average processing time comparison of the proposed scheme and existing the stat of the art schemes.

2) Transmission Overhead

In the BSNs environment, biosensor nodes have limited resources of memory, processing capability, and battery. Efficient bandwidth utilization in BSNs is a major issue, so transmission overhead should be as less as possible. The existing schemes mentioned in Table 6 suffer due to high transmission overhead compared to the proposed scheme. The proposed scheme only transmitted patients' critical information instead of continuous to increase the network's performance since data transmission consumes more energy than data processing.

VI. SIMULATION RESULTS USING AVISPA TOOL

In this section, we simulated our proposed lightweight multi-receiver generalized signcryption protocol using AVISPA formal verification tool. Most research communities related to information security and cryptography can prefer this tool to check the security strength of numerous secure transmission protocols and applications used on the public network. Fig. 9 shows the general structure of the AVISPA tool. To understand whether our proposed scheme design for BSNs is secure or not, the AVISPA tool provides facilities to check the validation of the proposed scheme using four different model checker/ bank-end called OFMC, CL-AtSe, SATMC, and TA4SP [44], [45].

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.2020.3035324, IEEE Access

TABLE 3: Processing cost comparison of our proposed scheme with existing generalized signcryption schemes

Scheme	Mode	Signcryption cost (Sender)					Un-signcryption cost (for each Receiver)				
		$HECDM$	Mul	M_{EXP}	B_P	H	$HECDM$	Mul	M_{EXP}	B_P	H
Proposed	Signature	1	–	–	–	1	1	2	–	–	1
	Encryption	1	1	–	–	3	–	1	–	–	3
	Signcryption	1	1	–	–	3	1	3	–	–	4
YXM. [31]	Signature	–	1	–	–	2	–	3	–	–	2
	Encryption	–	$r+1$	–	–	1	–	1	–	–	1
	Signcryption	–	$r+2$	–	–	$r+1$	–	4	–	–	2
HYX. [32]	Signature	–	$2r$	–	–	$3r$	–	–	–	2	1
	Encryption	–	$2r$	–	–	$3r$	–	1	–	–	1
	Signcryption	–	$3r+2$	–	–	$2r$	–	1	–	2	3
ZC. [33]	Signature	–	$2r$	–	–	$3r$	–	1	–	2	3
	Encryption	–	$2r$	–	–	$3r$	–	1	–	–	3
	Signcryption	–	$2r$	–	–	$3r$	–	1	–	–	3
ZC. [34]	Signature	–	$r+5$	2	1	3	–	–	$4r+2$	$2r+3$	2
	Encryption	–	$r+5$	2	1	3	–	–	$4r+2$	$2r+3$	2
	Signcryption	–	$r+5$	2	1	3	–	–	$4r+2$	$2r+3$	2

TABLE 4: Processing cost comparison of proposed scheme and existing signcryption schemes

Scheme	Entity	ECPM	ECPA	HECDM	HECDA	DIV	MUL	Add/Sub	KH/hash
proposed	Sender	-	-	1	-	1	-	1	3
	Receiver	-	-	2	-	-	1	1	3
CMA. [35]	Sender	-	-	3	-	1	-	1	2
	Receiver	-	-	2	1	-	1	-	2
ZYH. [36]	Sender	1	-	-	-	1	1	1	2
	Receiver	2	1	-	-	-	1	-	2
HRC. [37]	Sender	2	-	-	-	-	1	1	1
	Receiver	3	1	-	-	-	-	-	1
TMA. [38]	Sender	2	1	-	-	-	1	3	2
	Receiver	3	2	-	-	-	-	1	2
MR. [39]	Sender	3	-	-	-	1	-	1	3
	Receiver	2	1	-	-	-	1	-	3
CN. [40]	Sender	-	-	2	-	1	1	1	2
	Receiver	-	-	2	1	-	1	-	2
CWQ. [41]	Sender	-	-	2	-	1	-	1	-
	Receiver	-	-	2	1	-	1	-	-

Using these four models, we can check the proposed BSNs scheme's security and see the possible weaknesses in terms of attacks. Using various automatic programming procedures, we can detect different attacks against the proposed scheme for finite and infinite sessions. Moreover, AVISPA provides a case-sensitive language called HLPSL. We first define each object's role, control flow design, configuration directions to demonstrate simple roles, Models for an intruder, and design security policies. When the HLPSL source code/script is entirely executed, it will display a SAFE or UN-SAFE message. In which SAFE states mean that the protocol is secure, while UN-SAFE means that the protocol is insecure. Fig. 10,11,12 and 13 show the results of backend models.

Using the below steps, we can determine the security strength of the proposed sachem:

- First, we write the code in HLPSL in which we define the role of different agents, i.e., sender, receiver, intruder, control flow, and encryption/decryption policies to check the security strength of the scheme.
- Now the SPAN simulation tool converts the source code of the HLPSL into a low-level intermediate format called (IF) by using the HLPSL2IF translator.
- Now IF code executed by the back- end/model checker to determine whether the scheme is secure or not. [46], [47]
- After the complete execution of IF specification, each model checker displays the simulation results.
- Using the output format (OF), we can see the weakness or security strength.

Here we represented the basic terminologies/ types 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.2020.3035324, IEEE Access

TABLE 5: Average processing time comparison of our proposed scheme with existing signcryption schemes

Scheme	Average time (ms) sender side	Average time (ms) receiver side
Proposed	$1 \times 2.2 = 2.2$ ms	$2 \times 2.2 = 4.4$ ms
CMA. [35]	$2.2 \times 3 = 6.6$ ms	$2 \times 2.2 = 4.4$ ms
ZYH. [36]	$4.24 \times 1 = 4.24$ ms	$4.24 \times 2 = 8.48$ ms
HRC. [37]	$4.24 \times 2 = 8.48$ ms	$4.24 \times 3 = 12.72$ ms
TMA. [38]	$4.24 \times 2 = 8.48$ ms	$4.24 \times 3 = 12.72$ ms
MR. [39]	$4.24 \times 3 = 12.72$ ms	$4.24 \times 2 = 8.48$ ms
CN. [40]	$2 \times 2.2 = 4.4$ ms	$2 \times 2.2 = 4.4$ ms
CWQ. [41]	$2 \times 2.2 = 4.4$ ms	$2 \times 2.2 = 4.4$ ms

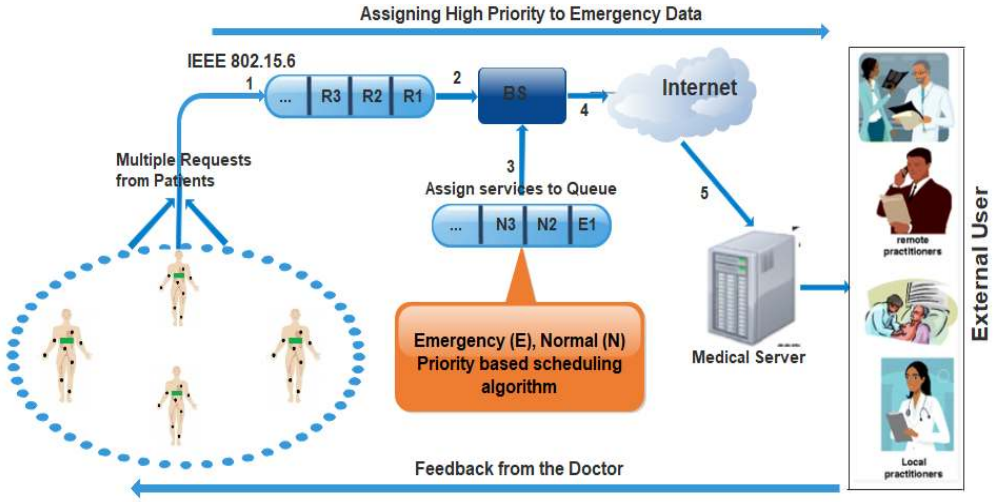

FIGURE 5: Proposed Modified Priority based scheduling Process

TABLE 6: Transmission overhead comparison of proposed scheme and existing schemes

Scheme	Mode	Transmission Overhead
Proposed	Signature	$3\|n\|$
	Encryption	$3\|n\|$
	Signcryption	$4\|n\|$
YXM. [31]	Signature	$3\|n\|$
	Encryption	$4\|n\|$
	Signcryption	$4\|n\|$
HYX. [32]	Signature	$r\|n+1\|$
	Encryption	$r\|n+1\|$
	Signcryption	$r\|n+1\|$
ZC. [33]	Signature	$r\|n+1\|$
	Encryption	$r\|n+1\|$
	Signcryption	$r\|n+1\|$
ZC. [34]	Signature	$r\|n+2\|$
	Encryption	$r\|n+2\|$
	Signcryption	$r\|n+2\|$

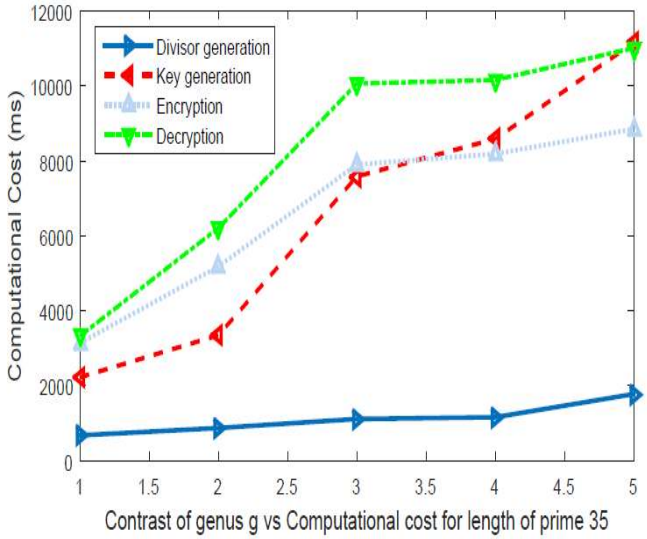

FIGURE 6: Evaluation of HECC genus w.r.t. processing cost

case-sensitive HLPSL language:

- **Agent**: Used to show the principle or protocol entity.
- **Public key**: Used to define agent public key in the protocol.
- **Symmetric key**: Define private key for the agent used in the protocol. Let us P_K is public key of the agent, so *inv* P_K), called secret key of the agent.
- **Function**: Using this, we define the domain and co-

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.2020.3035324, IEEE Access

TABLE 7: Key comparison in term of bits

Symmetric (key size in bits)	RSA (key size in bits)	ECC (key size in bits)	HECC (key size in bits)
80	1024	160	80
112	2048	224	54
128	3072	256	40

Algorithm 8 Proposed Modified Priority Based Scheduling Algorithm

1) Patient P (t) = $\{P_1, P_2, \ldots, P_n\}$ number of patient s send data at time t combine (S) mean (Patients)
2) BS= $\{BS_1, BS_2, \ldots, BS_n\}$ belong to hospital ward
3) Number of the patient within a particular BS area
4) REQ P_i (t) requests send by patient P_i in time t
5) Each patient sense vital sign, send to BS
6) On BS, perform priority-based scheduling
7) On BS, **Request Categorization** on the following parameters;
   a) Request priority (Emergency, Normal)
   b) Patient type (Heart patient, Psychiatrist patient, HIV Patient, Cancer Patient)
   c) Request value (α_1 , α_2)
8) On BS, **Data Categorization** on the following parameters; Data priority (Emergency, Normal)
   a) Data type (ECG, EMG, BP, SPO2, Pulse Rate, Respiratory Rate etc.)
   b) Priority value (β_1 , β_2)
9) Bs perform priority-based scheduling using the following steps
10) If (Priority Value = = β_1)
11) Gives the highest priority
12) Send Emergency (E) patient data to MS for further necessary actions
13) Else if (Priority Value = = β_2)
14) Gives Normal (N) priority
15) Send normal patient data to MS
16) end if
17) end if
18) end if

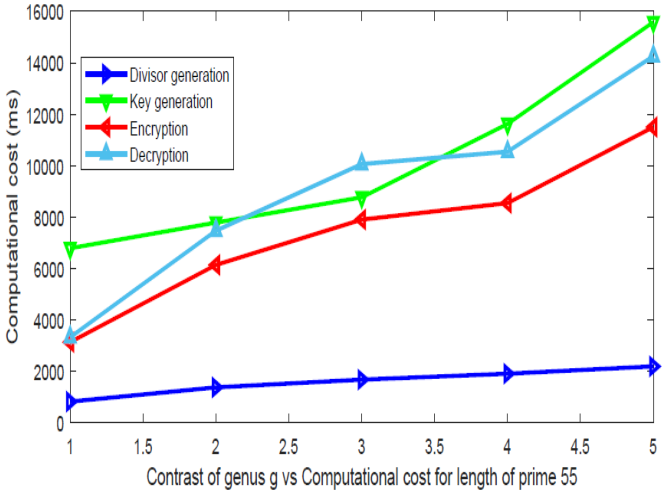

FIGURE 7: Evaluation of HECC genus w.r.t. processing cost using line graph

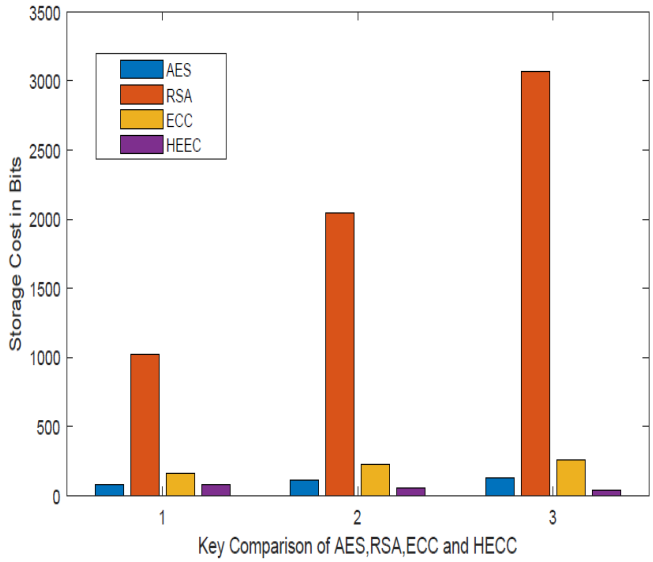

FIGURE 8: Storage evaluation of various ciphers

domain function of the data. This function is also used for modeling, i.e., one-way collision resistance HASH function used in the cryptography for the massage's integrity and non- invertible.

- **Channel**: Using this, we establish the link through which an agent can communicate. Channel used for dissemination of information from one agent to another agent in the networks. AVISPA tool only used (*dy*) for channel establishment [48].
- **Played_by:** using this, we can indicate the role-played in the protocol by a specific agent.
- **Local**: used for declaration agent local variables. The (*State*) variable declared as natural number representing using *(nat)* which used to indicate the agent local variables in the protocol. In (*init*) section, put the starting value zero.
- **Text:**using this text we indicate (*Nonce*). Each Nonce's value is fresh, new, and used to protect the replay attack,

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.2020.3035324, IEEE Access

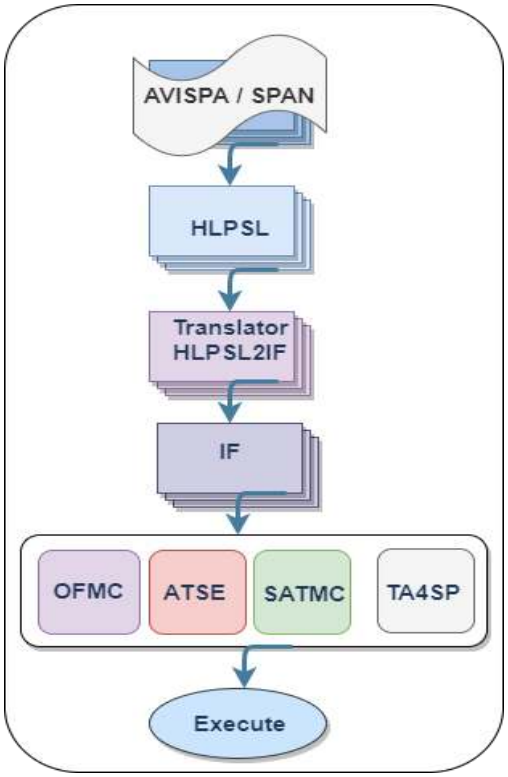

FIGURE 9: General structure of AVISPA tool

a nonce value not known by an intruder.

- **nat:**used to indicate natural numbers.
- **Const:** used in multiple roles for global constant declaration. Here, multiple declarations are also permitted but defended on the condition; if the data not changed, we declare multiple declarations otherwise not.
- **Protocol_id:** using this, securely communicate the secret parameters among agents, and we declare a constant as a protocol identifier, which specifies a secret among agents.
- **Snd/Rcv:**this is the type of link (*dy*) through which the sender and receiver agent can transmit information with each other.
- **P=|>Q:** indicate of event P with an agent action Q for abrupt response change.
- **Witness (A, B, id, E):** using this, we specify (E) as an authentication property over agent (A) by agent (B) using (id) protocol identifier.
- **Request (B, A, id, E):** using this, we specify the substantial authentication security property of agent (A) by agent (B) to (E) authentication property.
- **Secret (T, id, t, A, B):** using this, we specify that T is a secret for an agent (A) and agent (B).
- **Secret (T, id t, A, B):** using this, we specify that T is a secret for an agent (A) and agent (B).

In this paper the proposed scheme security evaluated through AVISPA tool as shown in Fig. 10,11,12,13,14 and 15.

Table 7 shows the key comparison in terms of bits, while in Fig. 8, we elaborated these values in terms of groups. Moreover, Fig. 6 and 7 show the genus's comparison concerning computational cost and different prime numbers.

VII. CONCLUSION

Here in this paper, we have designed a wholistic attribute-based multi-receiver generalized signcryption to fulfill the research gaps of prioritized, delay less, and secure transmission of patient data using a public network, simultaneous reception of patient's data by end-users, patient identity privacy, high overhead, and energy constraints in an efficient way. Attribute-based multi-receiver generalized signcryption is a suitable approach for constrained nature environments, i.e., BSNs, embedded systems, smart cards, smart grids, and wireless sensor networks. In this paper, we have applied a priority-based scheduling algorithm for delay less emergency patient data; multiple end-users access encoded data simultaneously by defining attribute-based access policy using (AND & OR) logic gates. Furthermore, to overcome the cost overhead of BSNs and avoid the key exposer problem, we applied the concept of HECC without utilizing bilinear pairing operations. The proposed scheme provided several security goals under the Hyper-elliptic Curve Discrete Logarithm Problem (HECDLP) in the random oracle model. The proposed scheme simulated in the AVISPA tool ensured that the scheme protected against adversaries' attacks. The obtainable results and proposed theorems show that our scheme fulfills all the essential security properties in three modes: encryption, signature, and signcryption, using a single efficient algorithm. The presented comparative studies can give benchmarks for academic research in the future and valuable for applied applications.

REFERENCES

[1] Jafer, Essa, Sattar Hussain, and Xavier Fernando. "A wireless body area network for remote observation of physiological signals." *IEEE Consumer Electronics Magazine* 9.2, pp. 103-106, 2020.

[2] Latha, R., and P. Vetrivelan. "Wireless Body Area Network (WBAN)-Based Telemedicine for Emergency Care." *Sensors-MDPI* 20.7, pp. 2153, 2020.

[3] Rashid, Tarique, et al. "Co-REERP: Cooperative Reliable and Energy Efficient Routing Protocol for Intra Body Sensor Network (Intra-WBSN)." *Wireless Personal Communications*, pp.1-22, 2020.

[4] Singh, Ritika, et al. "Wireless Body Area Network: An Application of IoT and Its Issuses—A Survey." *Computational Intelligence in Pattern Recognition.* Springer, Singapore, pp.285-293, 2020.

[5] Gouda, Kanhu Charan, et al. "Implementation of Traffic Priority Aware Medium Access Control Protocol for Wireless Body Area Networks." *Design Frameworks for Wireless Networks.* Springer, Singapore, pp. 379-397, 2020.

[6] Yang, Guangsong, et al. "Energy efficient protocol for routing and scheduling in wireless body area networks." *Wireless Networks*, 26.2, pp.1265-1273, 2020.

[7] Benmansour, Tariq, et al. "Performance analyses of the IEEE 802.15. 6 wireless body area network with heterogeneous traffic."*Journal of Network and Computer Applications*, pp.102651, 2020.

[8] Ahmed, Omar, et al. "Energy Optimized Congestion Control-Based Temperature Aware Routing Algorithm for Software Defined Wireless Body Area Networks." *IEEE Access* 8, pp. 41085-41099, 2020.

[9] Mubarakali, Azath, et al. "Design an attribute based health record protection algorithm for healthcare services in cloud environment." *Multimedia Tools and Applications* 79.5, pp.3943-3956, 2020.

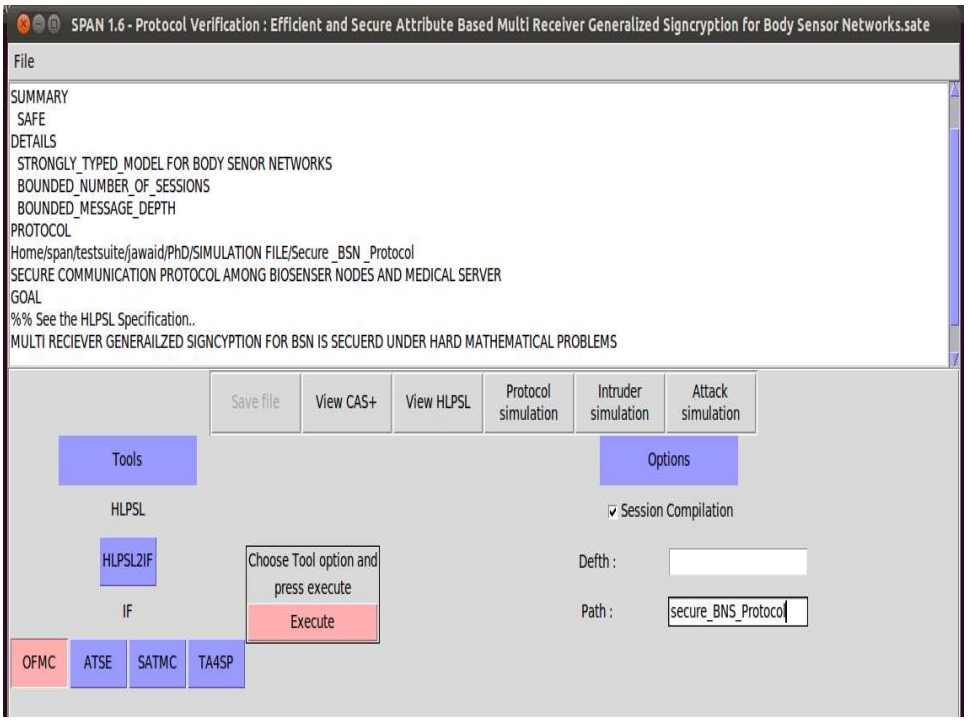

FIGURE 10: OFMC summary for HLPSL

[10] Liu, Meiping, et al. "An Efficient Attribute-Based Access Control (ABAC) Policy Retrieval Method Based on Attribute and Value Levels in Multimedia Networks." *Sensors-mDPI* 20.6, pp.1741, 2020.

[11] Zhang, Bo. "Comments on "Provably Secure Generalized Signcryption Scheme With Public Verifiability for Secure Data Transmission Between Resource-Constrained IoT Devices" *IEEE Internet of Things Journal* 7.5, pp. 4666-4670, 2020.

[12] Han, Yiliang, et al. "ECGSC: elliptic curve based generalized signcryption."*International Conference on Ubiquitous Intelligence and Computing*. Springer, Berlin, Heidelberg, pp. 956-965, 2006.

[13] Han, Yiliang. "Generalization of signcryption for resources-constrained environments."*Wireless Communications and Mobile Computing*7.7, pp. 919-931, 2007.

[14] Yu, Huifang, et al. "Identity-based proxy signcryption protocol with universal composability."*Security and Communication Networks* 2018.

[15] Zhou, Cai-Xue. "An improved multi-receiver generalized signcryption scheme."*International Journal of Network Security* 17.3, pp.340-350, 2015.

[16] Zhou, Cai-xue. "Cryptanalysis and Improvement of a Multi-Receiver Generalized Signcryption Scheme."*IACR Cryptology ePrint Archive, pp.* 638, 2012.

[17] Rahman, Abid Ur, et al. "A lightweight multi-message and multi-receiver heterogeneous hybrid signcryption scheme based on hyper elliptic curve."*Int. J. Adv. Comput. Sci. Appl.*9.5, pp.160-167, 2018.

[18] Li, Yahong, et al. "Privacy-preserving multi-receiver signcryption scheme for heterogeneous systems."*Security and Communication Networks*,9.17, pp. 4574-4584, 2016.

[19] Niu, Shufen, et al. "Heterogeneous hybrid signcryption for multi-message and multi-receiver."*PloS one*,12.9 (2017).

[20] Mehmood, Asad, Insaf Ullah, and Arif Iqbal Umar Noor-Ul-Amin. "Public Verifiable Generalized Authenticated Encryption based on Hyper Elliptic Curve."*J. Appl. Environ. Biol. Sci*, 7.12, pp. 69-73, 2017.

[21] Shen, Xiaoqin, Yang Ming, and Jie Feng. "Identity Based Generalized Signcryption Scheme in the Standard Model."*Entropy* 19.3, pp. 121, 2017.

[22] Sadat, Anwar, et al. "Multi Receiver Signcryption Based On Hyper Elliptic Curve Cryptosystem."*J. Appl. Environ. Biol. Sci* 7.12, pp. 194-200, 2017.

[23] NIU, Shu-fen, et al. "Certificateless generalized signcryption scheme in the standard model."*Journal on Communications* 38.4, pp.35-45, 2017.

[24] Zhang, Bo, Zhongtian Jia, and Chuan Zhao. "An efficient Certificateless generalized Signcryption scheme." *Security and Communication Networks*,2018.

[25] Zhang, Aiqing, et al. "Light-weight and robust security-aware D2D-assist data transmission protocol for mobile-health systems."*IEEE Transactions on Information Forensics and Security*,12.3, pp. 662-675, 2016.

[26] Zhou, Caixue, Wan Zhou, and Xiwei Dong. "Provable certificateless generalized signcryption scheme."*Designs, codes and cryptography*,71.2, pp. 331-346,2014.

[27] Zhou, Caixue, et al. "Certificate-Based Generalized Ring Signcryption Scheme." *International Journal of Foundations of Computer Science* 29.06, pp. 1063-1088, 2018.

[28] James, Salome, N. B. Gayathri, and P. Vasudeva Reddy. "Pairing free identity-based blind signature scheme with message recovery." *Cryptography*,2.4, pp. 29, 2018.

[29] Wei, Guiyi, et al. "Obtain confidentiality or/and authenticity in Big Data by ID-based generalized signcryption." *Information Sciences* 318, pp. 111-122, 2015.

[30] Waheed, Abdul, et al. "Cryptanalysis of an Authentication Scheme Using an Identity Based Generalized Signcryption." *Mathematics-MDPI* 7.9 : pp.782, 2019.

[31] Yang, Xiaoyuan, et al. "New ECDSA-verifiable multi-receiver generalization signcryption." *10th IEEE International Conference on High Performance Computing and Communications*. IEEE, pp. 1042-1047, 2008.

[32] Han, Yiliang, and Xiaolin Gui. "Adaptive secure multicast in wireless networks." *International Journal of Communication Systems* 22.9, pp. 1213-1239, 2009.

[33] Zhou, Cai-xue. "Cryptanalysis and Improvement of a Multi-Receiver Generalized Signcryption Scheme." *IACR Cryptology ePrint Archive,* pp.638, 2012.

[34] Zhou, Caixue. "A Multi-Receiver ID-Based Generalized Signcryption Scheme." *IACR Cryptology ePrint Archive*, pp.601, 2011.

[35] Ch, Shehzad Ashraf, et al. "An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography." *Multimedia Tools and Applications* 74.5 pp.1711-1723, 2015.

[36] Zheng, Yuliang, and Hideki Imai. "How to construct efficient signcryption schemes on elliptic curves." *Information processing letters* 68.5 pp. 227-233, 1998.

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.2020.3035324, IEEE Access

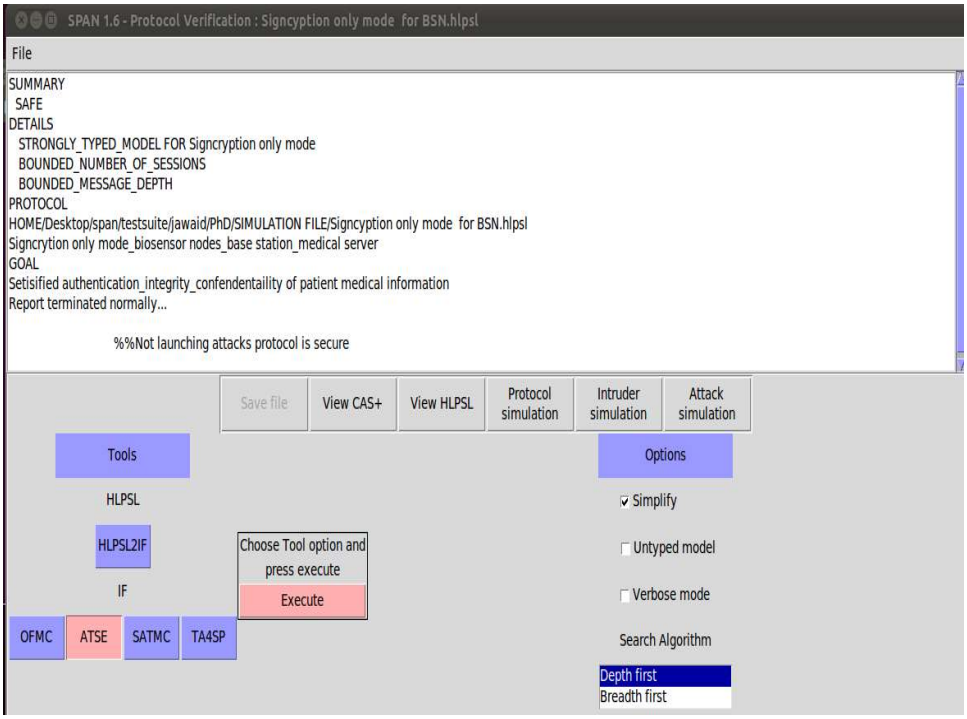

FIGURE 11: CL-ATSe summary for HLPSLC

[37] Hwang, Ren-Junn, Chih-Hua Lai, and Feng-Fu Su. "An efficient signcryption scheme with forward secrecy based on elliptic curve." *Applied Mathematics and computation* 167.2, pp. 870-881, 2005.

[38] Toorani, Mohsen, and Ali A. Beheshti. "An elliptic curve-based signcryption scheme with forward secrecy." *arXiv preprint arXiv:1005.1856*, 2010.

[39] Mohapatra, Ramesh Kumar. *Signcryption schemes with forward secrecy based on elliptic curve cryptography*. Diss. 2010.

[40] Ch, Shehzad Ashraf, and Noorul Amin. "Signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem." *8th International Conference on High-capacity Optical Networks and Emerging Technologies*. IEEE, pp. 244- 247, 2011.

[41] Ch, Shehzad Ashraf, Waqas Nasar, and Qaisar Javaid. "Efficient signcryption schemes based on hyperelliptic curve cryptosystem." *7th International Conference on Emerging Technologies*. IEEE, pp. 1-4, 2011.

[42] Al-Zubi, Moath, and Ahmad Adel Abu-Shareha. "Efficient signcryption scheme based on El-Gamal and Schnorr." *Multimedia Tools and Applications* 78.9, pp.11091-11104, 2019.

[43] Ganesan, Ramachandran, Mohan Gobi, and Kanniappan Vivekanandan. "A Novel Digital Envelope Approach for A Secure E-Commerce Channel." *IJ Network Security* 11.3, pp.121-127, 2010.

[44] Armando, Alessandro, et al. "Avispa: automated validation of internet security protocols and applications." *ERCIM News* 64, 2006.

[45] Von Oheimb, David. "The high-level protocol specification language HLPSL developed in the EU project AVISPA." *Proceedings of APPSEM workshop*, pp. 1-17, 2005.

[46] Islam, SK Hafizul. "Design and analysis of a three-party password-based authenticated key exchange protocol using extended chaotic maps." *Information Sciences* 312, pp.104-130, 2015.

[47] Islam, Sk Hafizul, and G. P. Biswas. "Design of two-party authenticated key agreement protocol based on ECC and self-certified public keys." *Wireless Personal Communications* 82.4, pp. 2727-2750, 2015.

[48] Dolev, Danny, and Andrew Yao. "On the security of public key protocols." *IEEE Transactions on information theory* 29.2, pp. 198-208,1983.

[49] Zhou, Caixue, et al. "Certificateless key-insulated generalized signcryption scheme without bilinear pairings." *Security and Communication Networks*, 2017.

[50] Jegadeesan, Subramani, et al. "EPAW: Efficient Privacy Preserving Anonymous Mutual Authentication Scheme for Wireless Body Area Networks (WBANs)." *IEEE Access* 8, pp.48576-48586, 2020.

[51] Ahmed, Omar, et al. "Energy Optimized Congestion Control-Based Temperature Aware Routing Algorithm for Software Defined Wireless Body Area Networks." *IEEE Access* 8, pp.41085-41099, 2020.

[52] Niu, Shufen, et al. "Electronic Health Record Sharing Scheme With Searchable Attribute-Based Encryption on Blockchain." *IEEE Access* 8, pp. 7195-7204,2019.

[53] Guo, Lifeng, et al. "A decryptable attribute-based keyword search scheme on eHealth cloud in Internet of things platforms." *IEEE Access* 8, pp. 26107-26118, 2020.

[54] Zhao, Kaixin, et al. "Public Auditing Scheme With Identity Privacy Preserving Based on Certificateless Ring Signature for Wireless Body Area Networks." *IEEE Access* 8, pp. 41975-41984, 2020.

[55] Mehmood, Gulzar, et al. "An Energy-Efficient and Cooperative Fault-Tolerant Communication Approach for Wireless Body Area Network." IEEE Access 8 (2020): 69134-69147.

[56] G. Mehmood, M. Z. Khan, A. Waheed, M. Zareei and E. M. Mohamed, "A Trust-Based Energy-Efficient and Reliable Communication Scheme (Trust-Based ERCS) for Remote Patient Monitoring in Wireless Body Area Networks," in IEEE Access, doi: 10.1109/ACCESS.2020.3007405.

[57] Dolev, Danny, and Andrew Yao. "On the security of public key protocols." IEEE Transactions on information theory, 29.2, pp.198-208, 1983.

JAWAID IQBAL received the master's degree in computer science from Hazara University Mansehra in 2014 and currently pursuing a Ph.D. degree in computer science from the Department of Information Technology, Hazara University, Pakistan, where he is the lecturer at the Department of Information Technology for three years. His research interests are in the areas of information security, Attribute-based Signcryption for body sensor network and information-centric networking (ICN).

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.2020.3035324, IEEE Access

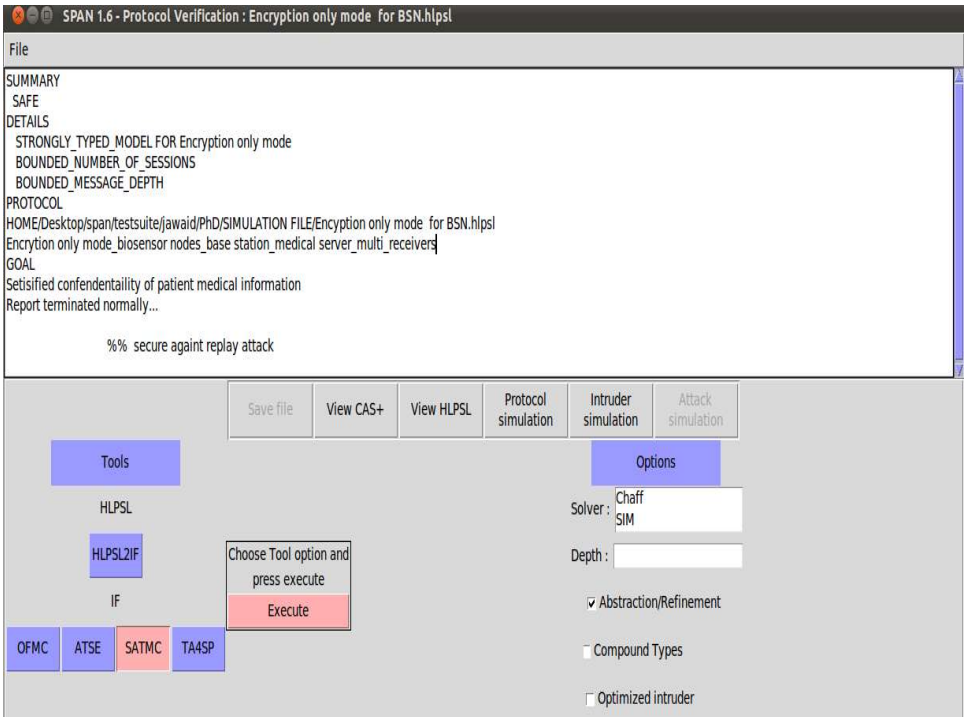

FIGURE 12: SATMC summary for HLPSLC

ABDUL WAHEED received his master's degree in computer sciences from the Department of Information Technology, Hazara University Mansehra, in 2014, and currently pursuing the PhD in computer sciences from the same Department. He is a member of the Crypto-Net research group at Hazara University. He has completed his Ph.D. research from NetLab-INMC under the school of Electrical and Computer Engineering (ECE), Seoul National University (SNU), South Korea in 2019 under the HEC research program. He is also serving as a lecturer in the Department of Computer Sciences, IQRA National University, Peshawar. He has numerous publications in international conferences and journals. His research interests are in the areas of information security, secure and smart cryptography, heterogeneous communications within IoT, mobile Adhoc networks (MANETs), wireless sensor networks (WSNs) security, and fuzzy logic-based decision-making theory.

MAHDI ZAREEI (S'11–M'17) received the M.Sc. degree in computer network from the University of Science, Malaysia, in 2011, and the Ph.D. degree from the Communication Systems and Networks Research Group, Malaysia-Japan International Institute of Technology, University of Technology, Malaysia, in 2016. In 2017, he joined the School of Engineering and Sciences, Tecnologico de Monterrey, as a Postdoctoral Fellow, where from 2019 he started working as a Research Professor. His research mainly focuses on wireless sensor and ad hoc networks, energy harvesting sensors, information security, and machine learning. He is a member of the Mexican National Researchers System (level I). He is also serving as an Associate Editor for the IEEE ACCESS and Ad Hoc & Sensor Wireless Networks Journals.

ARIF IQBAL UMAR earned BSc (Mathematics) degree from the Islamia College Peshawar Pakistan with distinction and MSc (Computer Science) from the University of Peshawar Pakistan in the Year 1991 and 1998 respectively. He accomplished his Ph.D. degree in the field of Information Retrieval from the Bei-Hang University Beijing (Beijing University of Aeronautics and Astronautics BUAA), P.R. China in 2010. He has at his credit rich experience of more than 27 years of Academic, Research, and Educational Management. He joined Hazara University in 2012. He is leading the department of Information Technology Hazara University as Head. He has successfully supervised 08 Ph.D. Scholars and many more are being trained under his supervision. He has at his credit more than 70 research publications in reputed journals and conferences. He has been a reviewer of several international journals and conferences. He is a member of several academic bodies of different Universities and has been on organizing bodies of several international conferences. Currently, his research interest includes Data Mining, Machine Learning, Secure and Heterogeneous Communication in IoT, and Securing Computer Networks.

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.2020.3035324, IEEE Access

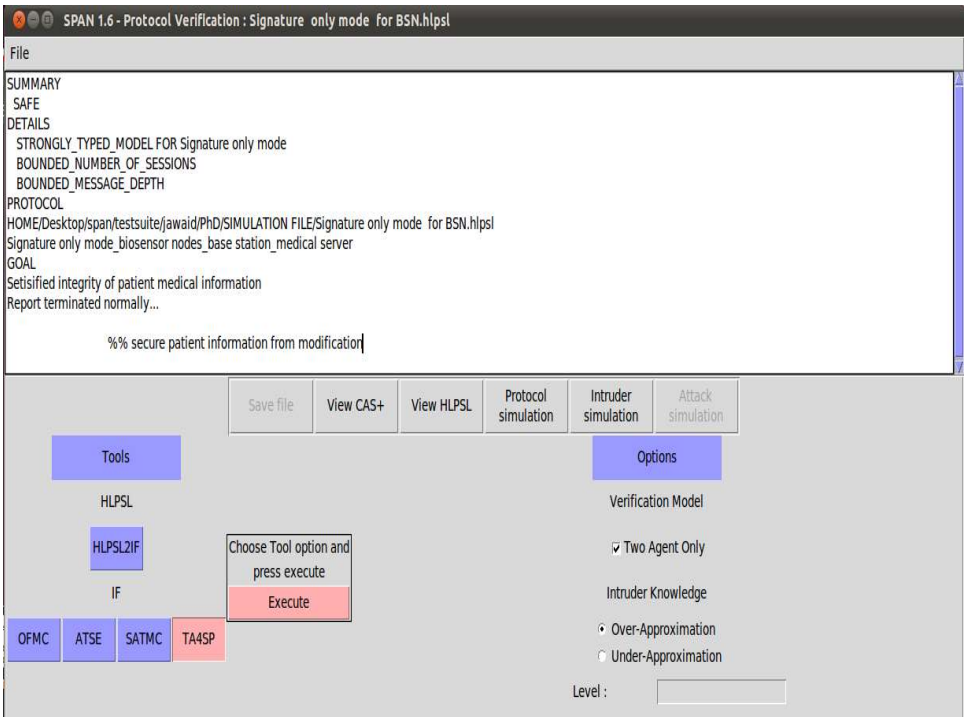

FIGURE 13: TA4SP summary for HLPSLC

NOOR UL AMIN received the master's degree in computer science from the University of Peshawar, Pakistan, in 1996, and the Ph.D. degree in computer science from the Department of Information Technology, Hazara University, Pakistan, where he has been the Head of the Department of Information Technology and the Director of IT for 11 years. He is currently the Chair of the Department of Telecommunication, Hazara University. He has completed recently a Research and Development project sponsored by the Ministry of Science and Technology, Pakistan, and established 07 hi-tech research and development labs. His research interests are in the areas of information security, mobile Adhoc networks (MANETs), wireless sensor networks (WSNs), and information-centric networking (ICN).

ABDALLAH ALDOSARY is an Assistant Professor in the Department of Computer Sciences at Prince Sattam bin Abdulaziz University. He received his Ph.D. in Computer Engineering from Florida Institute of Technology in the USA, where his research was focused on developing different radio energy models for different propagation environments. Dr.Aldosary received his Bachelor of Science in Electrical Engineering and Master of Science in Computer Engineering from the University of South Wales in the United Kingdom. His research interest areas include performance evaluation of wireless sensor networks' protocols, sensor networks, remote monitoring and control, wireless communication, and radiofrequency propagation.

EHAB MAHMOUD MOHAMED received the B.E. degree in electrical engineering from South Valley University, Egypt, in 2001, and the M.E. degree in electrical engineering from South Valley University, Egypt in 2006, and the Ph.D. degree in information science and electrical engineering from Kyushu University, Japan in 2012. From 2013 to 2016, he has joined Osaka University, Japan as a Specially Appointed Researcher. Since 2017, he has been an associate professor at Aswan University, Egypt. Also, he has been an associate professor at Prince Sattam bin Abdulaziz University, Saudi Arabia since 2019. He is the general chair of IEEE ITEMS'16 and IEEE ISWC' 18. He is a technical committee member in many international conferences and a reviewer in many international conferences, journals and transactions. His current research interests are 5G, B5G and 6G networks, cognitive radio networks, millimeter-wave transmissions, Li-Fi technology, MIMO systems, and underwater communication. He is an IEEE member.

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.2020.3035324, IEEE Access

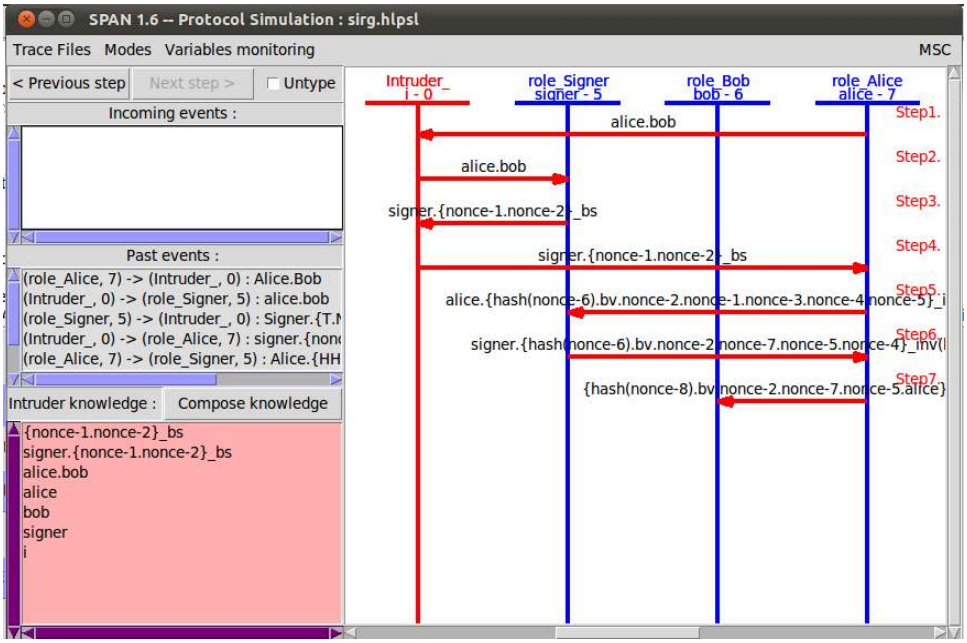

FIGURE 14: Simulation part-I of proposed scheme

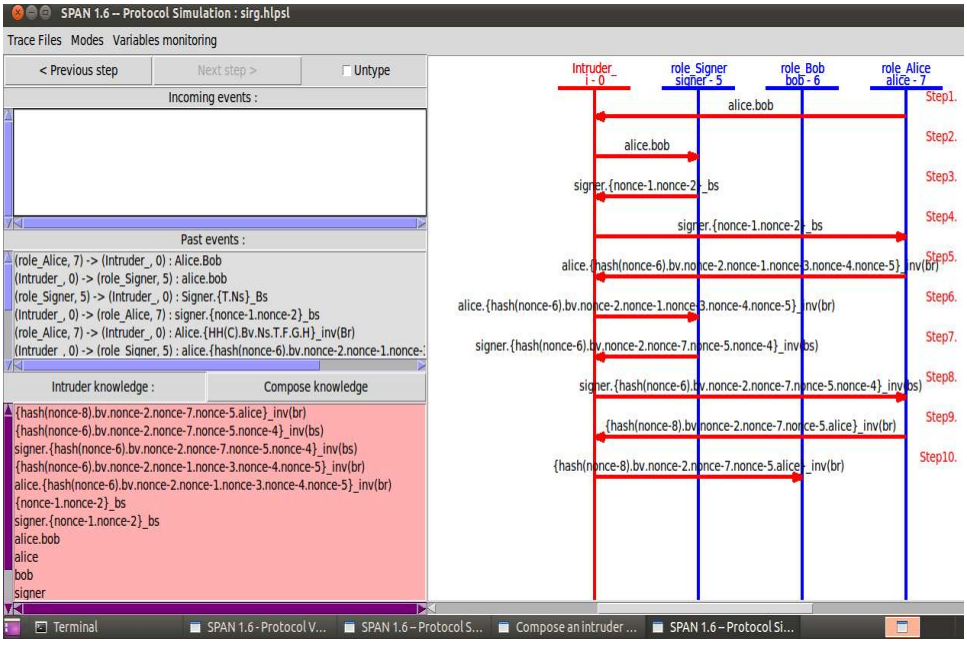

FIGURE 15: Simulation part-II of proposed scheme