IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 14, 2020, accepted January 22, 2021, date of publication January 28, 2021, date of current version February 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3055148

Practical Identity Based Online/Off-Line Signcryption Scheme for Secure Communication in Internet of Things

VANKAMAMIDI SRINIVASA NARESH[1], SIVARANJANI REDDI[2], SARU KUMARI[3], V. V. L. DIVAKAR ALLAVARPU[4], SACHIN KUMAR[5], AND MING-HOUR YANG[6], (Member, IEEE)

[1]Department of Computer Science and Engineering, Sri Vasavi Engineering College, Tadepalligudeam 534101, India
[2]Department of Computer Science and Engineering, Anil Neerukonda Institute of Technology and Science, Visakhapatnam 530003, India
[3]Department of Mathematics, Chaudhary Charan Singh University, Meerut 250004, India
[4]FinTech Academy, GITAM Institute of Management, GITAM (Deemed to be University), Visakhapatnam 530045, India
[5]Department of Computer Science and Engineering, Ajay Kumar Garg Engineering College, Ghaziabad 201009, India
[6]Chung Yuan Christian University, Chung Li 32023, Taiwan

Corresponding author: Ming-Hour Yang (mhyang@cycu.edu.tw)

This work was supported in part by the Ministry of Science and Technology and National Applied Research Laboratories of Taiwan under Grant MOST 109-2218-E-009-010 - and Grant NARL-ISIM-109-006.

ABSTRACT Contemporary developments in providing proper security in the Internet of Things (IoT) have been made signcryption scheme highly suitable for various applications such as smart cities, smart healthcare and smart agriculture. However, security and privacy are the primary concerns in protecting data as it was highly sensitive. This paper is proposing a new Identity based online/off-line signcryption scheme suitable to provide secure message communication among IoT devices, gateway, and the server. This method is divided into the online and offline phases, where heavy mathematical computations are carried out in the offline phase and light computations in the online phase. This scheme provides a security solution for integrating Wireless Sensor Networks (WSNs) into the IoT. Experimentation was done and finally compared against existing techniques and proved that the proposed mechanism reduces the computation time in online by performing a greater number of operations in off-line signcryption phase. Further, it provides indistinguishability against adaptive chosen ciphertext attacks and existential unforgeability against adaptive chosen messages attacks.

INDEX TERMS Bilinear pairing, certificateless signcryption, HOOSC, heterogeneous, identity based cryptography, online/off-line signcryption.

I. INTRODUCTION

IoT is a diversified network intended to establish communication among various types of sensors and servers also facilitates the communication between person-to-person, person-to-device, device-to-person, or device-to-devices, and so on. Advancements in communication technology, it is widely used in many real-time applications like military vigilance, healthcare, industrial operations monitoring, etc. Data communication of these devices in an open environment may raise the scope to access sensitive data by the intruder, so, security is the primary concern.

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

Security and privacy [1] are always the crucial issues of IoT. In order to provide the security and privacy in the IoT environment, extensive research on physical layer security, secure access control mechanism (e.g., access control scheme based on attribute base encryption), secure communication, network traffic and data analysis method, and threat detection technology has been carried out.

The IoT system in general is usually deployed in a distributed environment. In which, the IoT entities exchange information dynamically to provide a decentralized and scalable infrastructure, to support billions of devices generating and exchanging large amount of data. Decentralized communication has become a crucial trend of Smart-IoT, such as the researches on block-chain based mechanism and device-to-device (D2D) communication technology. we need a more

efficient secure schemes and mechanisms that can secure the message communication in the heterogenous network. Among numerous cryptography methods, signcryption, cryptography primitive can be applied to decentralized communication environment, has received considerable attention because of its high efficiency and security.

Many techniques such as cryptographic algorithms, key management techniques [2], region-based privacy-preserving mechanisms [3], based on public key infrastructures (PKI) [6], Certificateless Public Key Cryptography (CL-PKC), and an Identity based (ID) [7], [8], [21], [23], [24], and signcryption methods [4] were present to address the security issues. Among these, the best cryptography scheme named Signcryption, which fulfills the functionalities of digital signature and encryption in a single step. Where as in traditional public key cryptography data encryption and authentication is accomplished by signing the document digitally and then encrypt the signed document for transmission over a public network (i.e, signature-then- encryption). It results low efficiency and high computational cost. A Signcryption scheme diminishes the computational cost as compared to signature-then- encryption scheme. Encryption and digital signature are two elementary security properties of any signcryption scheme. Such properties include integrity, non-repudiation, unforgeability and confidentiality. Online/offline cryptography is a fundamental concept for several cryptographic systems is a key to reduce computational costs of the devices sending their messages in confidential and/or authenticated way. Where, the signing procedure of online/offline signature scheme is split into the offline phase and the online phase. The signer can accomplish all the computationally expensive operations in the offline phase, Then, in the online phase, only lightweight operations are required to sign the message so that even low-power devices can handle the signing process. From the literature survey, the online/off-line signcryption approach is highly appropriate for IoT since it is finishing most of the operations will be done off-line results increase in performance also concentrating on the security service like authentication, confidentiality, non-repudiation and integration. Advantages of signcryption include:

a. More proficient in computational and communication than the sequential computation of signature and encryption techniques.
b. Needs only one key pair for an individual user, whereas traditional technique requires two pairs of keys used for encryption and signing, respectively
c. Permits the operations to be done in parallel.
d. signcryption can simplify the design of cryptographic protocols by including confidentiality and authenticity.

Zheng [5] has proposed the signcryption scheme, where sender could sign and encipher the message concurrently. It is apposite for the devices consume less power such as sensors. Even *et al.* [9] has proposed an online/off-line signcryption (OOSC) scheme, mainly consist of online and off-line phases. In off-line, majority of complex calculations will be finished in the absence of the message and receiver's information; barely light operations will be done online. Hence, the OOSC scheme is more preferable for the establishment of communication among IoT devices. Zhang *et al.* [10], Sun *et al.* [11], Liu *et al.*, and Sharmila Deva Selvi *et al.* [13] proposed an OOSC scheme using user Identity and shows that the scheme is secure against random oracle.

In recent times, CL-PKC was studied extensively, since it could conquer certificate management and key escrow problem in the ID-based public-key cryptography. Many certificateless key agreement methods [15]–[18], [20], digital signature techniques without certificate [25]–[28], and cryptographic schemes without certificates [29], [30], [33], [41], [43]–[45] have been proposed for various applications. Luo *et al.* [31] projected foremost certificateless online/off-line signcryption (COOSC) scheme [32], [42], demonstrated that it is provably secure in random oracle. Regrettably, these schemes are exposed to the private key compromised problem. Andrew *et al.* [6] proposed an OOSC scheme to produce an optimal solution for BSN by combining signature for authentication, encryption and integrity. Xu *et al.* [34], Mu *et al.* [10], Chen *et al.* [35] and Thwin and Vasupongayya [36] utilizes the idea of blockchain together with proxy re-encryption scheme for the transmission of personal health information securely and to get out of the network performance concerns, security, privacy, storage limitations of sensors, scalability, revocation of consent, secure against Adversary's attacks. Li *et al.* [32] and Luo et al [37], proposed certificateless online/off-line signcryption schemes. Lai and colleagues [38], [39] proposed the signcryption based on ID, that undergoes key escrow issue and the server-side scalability problem. Sun and Li [14] presented two dissimilar domains created on heterogeneous signcryption. Li *et al.* [40] developed a heterogeneous signcryption which can resolves the issues of Li and Sun scheme [39].

To get rid of the computational burden on biosensor nodes, Jawaid *et al.* [41] presented online/off-line signcryption techniques for certificateless cryptosystem (CLC) in heterogeneous environments. Dan and Wakaha [42] proposed multi-divisible online/off-line (MDO) cryptography includes the earlier works such as online/off-line cryptographic schemes, incrementally executable signcryptions, divisible online/off-line signatures, and MDO encryptions. However, we know that the aim of the online/off-line technique is to shift the massive operations to the off-line phase. Numerous online/off-line signcryption algorithms were proposed by many researchers such as Heterogeneous online/off-line signcryption (HOOSC) scheme [19] and the Heterogeneous cryptographic Algorithm [41]. However due to high computational load with complex operations: division, exponentiation and inverse made these protocols weak in terms of performance. To address this and to improve the performance, in the proposed scheme we made the following changes:

- We removed the division operation in key generation.
- Instead of exponentiation and inverse operations in online/off-line signcryption the scalar multiplication and addition operations respectively.
- Used bilinear pairing operations with the objective of reducing the number of operations in the online phase in order to speed up the computations and also to improve the security in communication.

A. CONTRIBUTIONS

The main objective of this paper is to establish a secure channel between a sensor node and an Internet host in order to provide end-to-end communication with confidentiality, integrity, authentication and non-repudiation services. In addition to that, an identity-based cryptosystem (IBC) is used in the sensor node and that the PKI is used in the Internet host. Also, we are aiming to make the computational cost of sensor nodes is low. The proposed solution is heterogeneous online/off-line signcryption with the following features

- It allows a sensor node in the IBC to send a message to an Internet host in the PKI.
- It splits the signcryption into two phases: off-line phase and online phase. In the off-line phase, most of the heavy computations are done without the knowledge of a message. In the online stage, only light computations are done when a message is known.
- The computation time of key generation phase of proposed scheme is less compared to the HOOSC technique.
- Computation time of the proposed online signcrypt is less compared to the HOOSC scheme.

1) ROADMAP

The mathematical background for the proposed work is discussed in section 2, some of the existing techniques and their functionality are elaborated in section 3, the methodology for proposed sign-encryption scheme was presented in section 4, Security analysis of ID-Based OOSC is presented in section 5, results of proposed scheme and comparison of existing schemes with the proposed is shown in section 6, and the last section 7 concludes the paper with future direction.

II. MATHEMATICAL BACKGROUND

This section will concentrate on notations and bilinear pairing properties.

A. NOTATIONS

Table 1 displays the abbreviations and notations used in this paper.

B. BILINEAR MAPS

Let us consider G_1 and G_2 be two groups of prime order p, where G_1 is using additive notation and G_2 using multiplicative notation. We consider W, U and V are three generators of

TABLE 1. Notations.

Symbol	Definition
σ	signature
m	message
u	User u
SID_u	u's private key
QID_u	u's public key
C	cyphertext
P	generator of G_1
p	large prime number
H_1, H_2, H_3 and H_4	Hash functions
ID_u	u's identity
$\mathbb{C}$	Challenger
$\mathbb{A}$	Adversary

G_1, and we write $aW = \overbrace{W + W + \cdots + W}^{a\ times}$ and we consider a bilinear map ê: $G_1 \times G_1 \rightarrow G_2$

The useful bilinear mapping [24], [28] has following properties:

1) BILINEARITY

$$\forall W, U \in G_1, \forall a,b \in Z_q^*, \hat{e}(aW,bU) = \hat{e}(W,U)^{ab} \quad (1)$$

$$\hat{e}(W+U,V) = \hat{e}(W,V).\hat{e}(U,V) \text{ and}$$
$$\hat{e}(W,U+V) = \hat{e}(W,V).\hat{e}(W,U), \forall W,U,V \epsilon G_1 \quad (2)$$

2) NON-DEGENERACY

$$\text{For any } O \neq W \in G_1, \text{ there is } U \in G_1, \text{ such that } \hat{e}(W,U) \neq 1$$
$$\forall W,U \in G_1, \hat{e}(W,\infty) = 1 \text{ and } \hat{e}(\infty,W) = 1 \quad (3)$$
$$\hat{e}(W,-U) = \hat{e}(-W,U) = \hat{e}(W,U)^{-1} \quad (4)$$
$$\hat{e}(W,U) = 1, \quad \forall W \in G_1 \text{ then } U = \infty \quad (5)$$

C. Computability

$\forall (W,U) \in \boldsymbol{G_1} \times \boldsymbol{G_2}, \hat{e}(W,U)$ is efficiently computable.

III. EXISTING SIGNCRYPTION TECHNIQUES

This section will discuss two well-known signcryption schemes Heterogeneous online/off-line signcryption (HOOSC) and Heterogeneous cryptographic Algorithm. Both of them are the off-line/online signcryption mechanisms. The importance of these techniques is, some of the calculations will be done during off-line to save the computation time during the communications. These mechanisms mainly comprise of off-line phase and an online phase. In the off-line phase user will decide the public parameters, user registration with Private Key Generator (PKG), secret key computation from the user ID, and then the signature generation. Once the user decides the message to communicate to other end, online signcryption procedure will be executed.

TABLE 2. Performance comparison.

Scheme	Computational cost		Security			Key size(bits)		Cipher text	off-line storage
	Sign_crypt	Unsign_crypt	IND-CCA2	EUF-CMA	IS	IBC	PKI		
Hetro[15]	1Pa,2H,2A,1Mul	5P,1XoR,2H,1e	√	√	√	480	320	960	960
SL[14]	4H,2XoR,1e	2XOR,3H,1Pa	√	X	X	320	320	640	0
Fagen[19]	1e,2H,2Mul,1XOR	2Pa,3H,1A	√	√	√	320	320	640	1824
LTX[32]	3Mul ,1e	3Pa,4Mul	√	√	√	680	680	1520	2224
LZZ [33]	4Mul ,1e	3Mul,1e,2Pa	√	√	√	680	680	1520	2384
Jawaid[46]	4Mul,1e,2H,1XoR	1e,2Pa,1Mu, 2H	√	√	√	480	320	1200	2720
Proposed	2Mul 1pa	1A,3Pa,1XOR	√	√	√	320	320	1200	2224

IND- CCA2: Indistinguishability under Adaptive Chosen Ciphertext Attack(IND-CCA2), EUF- CMA: Existential Unforgeability under Chosen Message Attack(EUF-CMA), IS: Insider security, IBC: Identity based cryptography, PKI: Public key infra structure

This phase is intended to perform the conversion of message into ciphertext.

A. HOOSC SCHEME [19]

A generic HOOSC method consists of the following steps: setup, IBC-KG, PKI-KG, off-signcrypt, on-signcrypt, and unsigncrypt.

(1) SETUP:PKG run Setup() phase and produces system parameters(*param)* as output by keeping master key s secret.

Setup()
{
a) Choose two groups of G_1 and G_2 of prime order p Where , G_1 is additive and G_2 is multiplicative groups, P *is* a generator of G_1,
$\hat{e} : G_1 X G_1 \rightarrow G_2$ and hash functions
$H_1 : \{0, 1\}^* \rightarrow Z_p^*$
$H_2 : \{0, 1\}^* X G_1 X G_2 \rightarrow Z_p^*$ and
$H_3 : G_2 \rightarrow \{0, 1\}^n$, n is the bit level message length.
b) Choose s randomly
c) Compute $P_{pub} = sP$ and $g = \hat{e}$ (P, P)
d) Publish $param = \{G_1, G_2, H_1, H_2, H_3, \hat{e}, g, n, P, P_{pub}\}$ by keeping s secret.
}

(2) IBC-KG: An identity based key routine, where client submits Identity (ID) to PKG, he computes the secret key(SID) and communicates securely to the user by using user's public key (pk) and ID.

IBC-KG()
{
a) Compute $SID = \frac{1}{H_1(ID)+s} P$
b) Return *key pair* = (public key, private key) = *(ID, SID)*
}

We will denote the sender by ID_r and his key pair (public key, private key) is represented by (ID_r, SID_r)

(3) PKI-KG: A key generation step for PKI user(u), where the user chooses his secretkey (sk_u) and publish the corresponding publickey (pk_u). The pk_u need a digital certificate signed by Certificate Authority (CA).

PKI-KG(sender u)
{
a) Choose a random number x_u from Z_p^*
b) Compute secret key $sk_u = \frac{1}{x_u} P$ and public key $pk_{u=} x_u P$
}

(4) OFF-SIGNCRYPT: Once the sender(u) decides the receiver(r) to whom he wants to send a message(m), then he runs this algorithm, outputs an off-line signcryption(δ) by taking *param*, sender private key (SID_u), and receiver public key (pk_r), as input.

off-signcrypt()
{
a) Choose x, β from Z_p^* randomly
b) Compute $r = g^x, S = \beta.SID_u, T = x.pk_r$
c) return $\delta = (x, r, \beta, S, T)$
}

(5) ON-SIGNCRYPT sender runs this algorithm to output ciphertext(σ), which uses *param*, message(m), and δ as input.

on-signcrypt()
{
a) Compute $c = XOR\ (m, H_3(r))$
b) $h = H_2\ (m, r, S)$
c) and $\theta = (x + h)\ \beta^{-1} modp$
d) return $\sigma = (c,\theta,S,T)$
}

(6) UNSIGNCRYPT: once receiver receives the ciphertext, applies this algorithm to retrieve the m it. This algorithm takes σ, a sender's publickey(pk_u), the receiver's secretkey (sk_r), and outputs m or the symbol $\perp$ if σ is invalid.

unsigncrypt()
{
a) $r = \hat{e}\ (T, sk_r)$
b) Retrieve $m = XOR\ (C, H_3(r))$

c) Compute $h = H_2(m, r, s)$
d) Accept m when $r = \hat{e}(\theta S, H_1(ID_u)P + P_{pub})\, g^{-h}$ otherwise return $\perp$.

}

B. HETEROGENEOUS CRYPTOGRAPHIC ALGORITHM [41]

This attribute-based heterogeneous online/offline scheme that securely transmits information from the biosensor nodes to server using online/off-line heterogeneous signcryption. This heterogeneous online/off-line signcryption scheme comprises the following phases: setup phase, PKG key generation phase, user node key generation phase, offline signcryption phase, online signcryption phase, and unsigncrypt phase. The detailed description of the algorithms is as follows:

1) SETUP

PKG run Setup(), produce system parameters(*param)* as output.

Setup()
{
a) Choose two groups of G_1 and G_2 of prime order p Where , G_1 is additive and G_2 is multiplicative groups, P is a generator of G_1,
ê: $G_1 XG_2 \rightarrow G_2$ and hash functions
$H_1 : \{0, 1\}^* \rightarrow Z_p^*$
$H_2 : G_1 \rightarrow Z_p^*$, $H_3 : G_2 \rightarrow \{0, 1\}^n$ and
$H_4 : \{0, 1\}^n XG_1 XG_2 \rightarrow Z_p^*$, n is the bit level message length.
b) Choose s randomly
c) Compute $P_{pub} = sP$ and $g = \hat{e}(P, P)$
d) Publish $param = \{G_1, G_2, H_1, \hat{e}, g, n, P, P_{pub}\}$ by keeping (s, H_2, H_3, H_4) secret.
}

2) KEY GENERATION

This phase generates the private and public keys of user, mainly consists of i. master key pair generation at PKG, ii. user public key generations, iii. partial private key generation and iv. full key generation algorithms.

I. Master_Key(): This is a key pair generation routine at PKG, where PKG computes the public key and private key.

Master_Key()
{
a) Choose a random number s from Z_p^*
b) Compute $sk_G = \frac{1}{s}P$ and public key as $pk_{G=}\, sP$
c) Return *key pair* = (public key, private key) = (pk_G, sk_G)
}

II. PK_Gen(): An identity based key routine, where client uses his Identity (ID_u) and generates public key, details are as follows:

PK-Gen ()
{
a) Choose a random number x_u from Z_p^*
b) public key $pk_{u=} x_u H_1(ID_u)\, P$
}

III. EPK_Gen(): An identity based key routine, where client submits his Identity (ID_u) and the public key pk_u to PKG, he computes the partial secretkey(spk_u) and communicates securely to the user.

EPK_Gen()
{
Compute partial private secret key
$spk_u = \frac{1}{H_2(pk_u)+sk_G}P$
}

IV. FK_Gen(): This phase takes spk_u and x_u as input parameters and generates thee full private key (FP_u) of the user(u) as $FP_u = spk_u.x_u^{-1}$

3) OFF-SIGNCRYPT

Once the sender(u) runs this algorithm, outputs an off-line signcryption(δ) by taking $param, FP_u, pk_G, x_u, ID_u$ *and* spk_u as the input.

off-signcrypt()
{
a) Choose x, β from Z_p^* randomly
b) Compute D = x. pk_G
c) Compute Z = $\beta^{-1}.FP_u$
d) Compute U = $x_u pk_G$
e) Compute T = $x_u.H_2(spk_u).$P
f) Compute L = g^x
g) return $\delta = (x, \beta, D, Z, U, T, L)$
}

4) ON-SIGNCRYPT()

In this phase, the message(m) and the output of previous offline phase (δ) is taken as the input, computes the signature (σ) and sends to the receiver as follows:

On-signcrypt(m, δ)
{
a) Computes $V = H_3(L)$
b) Computes $C = XOR(m, V)$
c) Computes $h = H_4(M, L, Z)$
d) Computes $b = (x + h)\beta \bmod p$
e) compute encoded text $C = (C, b, Z, D)$
f) return $\sigma = (C, U, T)$
}

5. UNSIGNCRYPT: In this phase, the cipher takes an encoded text C, U, T and FP_r as input and run unsigncryption cipher to get the message(m) and to check the correctness of that data.

unsigncrypt()
{
a) compute $L = \hat{e}(D, FP_r)$
b) Retrieve $m = XOR(C, H_3(L))$
c) Compute $h = H_3$(m, L, Z)
d) Compute $F = b.Z$

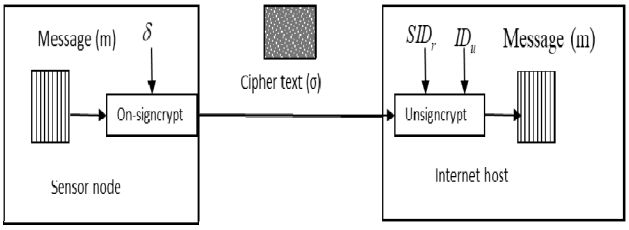

FIGURE 1. Block diagram of secure communication.

e) Accept m when
$L = \hat{e}(F, T, U)\, g^{-h}$
otherwise return $\perp$.

}

IV. PROPOSED METHOD

A. IDENTITY BASED ONLINE/OFF-LINE SIGNCRYPTION SCHEME

The block diagram in Figure 1 shows the steps involved in the communication between two sensors, the sender and receiver, through different media. This scheme consists of the Identity based certificate less communication; initially, the sensor calculates the precomputed results $\delta = (U,W,y,k)$ in off-line. When it wants to send m then it runs the On-signcrypt(δ,m) algorithm to compute the cipher text. As and when the receiver receives the ciphertext, he uses unsigncrypt() method to retrieve message m. The proposed scheme can achieve security services like confidentiality, integrity, authentication, and non-repudiation. Like HOOSC, the proposed algorithm also consists of five algorithms setup, extract, offline-signcryption, online signcryption and unsigncryption.

1) SETUP

PKG runs algorithm, takes security parameter(s) as input and produces *param* as the output.

Setup()
{
a) Choose G_1 and G_2 of prime order p, P is a generator of G_1, a bilinear map $\hat{e} : G_1 X G_1 \rightarrow G_2$ and hash functions $H_1 : \{0,1\}^* \rightarrow G_1, H_2 : \{0,1\}^* \rightarrow Z_p^*$ and $H_3 : G_2 \rightarrow \{0,1\}^n$,n is the number of bits in the message
b) Choose $s \rightarrow Z_p^*$
c) Compute $P_{pub} = sP$ *and* $g = \hat{e}(P,P)$
d) Publish
$Param = \{G_1, G_2, \hat{e}, H_1, H_2, H_3, g, n, p, P, P_{pub}\}$
by keeping s secret
}

2) EXTRACT

In this algorithm, user submits *ID* to PKG, he computes private key *SID* and sends key pair back to the user securely.

Extract()
{
a) Compute $QID = H_1(ID)$
b) Compute $SID = sQID$
c) Return key pair
(public key, private key) = *(QID, SID)*
}

For the user (u) the keypair is (QID_u, SID_u)

3) OFFLINE-SIGNCRYPTION

After deciding receiver (r) by the sender (u), he/she runs this algorithm, outputs an offline signcryption δ by taking system parameters *param*, and receivers public key QID_r as the input.

off-signcrypt()
{
a) Choose $x \leftarrow Z_p^*$ randomly
b) Compute $U = xP$, $W = xP_{pub}$
c) Compute $y = \hat{e}(W, QID_r)$ and then $k = H_3(y)$
d) return $\delta = (U,W,y,k)$
}

4) ONLINE –SIGNCRYPTION

sender runs this algorithm in order to output sinature(σ), which takes *param*, m and an off-line signcryption(δ) as input and then generates the signature (σ) consists of ciphertext(C), U and V.

on-signcrypt()
{
a) Compute $h = H_2(U, m)$
b) $V = hSID_u + W$ and $C = m \oplus k$
c) return $\sigma = (C, U, V)$
}

5) UNSIGNCRYPTION

once receiver receives the signature, he applies this algorithm to retrieve the m from it. This algorithm takes a signature(σ), sender's identity (ID_u), a sender's publickey QID_u and the receiver's secretkey SID_r as input, and accept the message (m'), which is obtained from the XOR on k and C after checking the correctness otherwise returns symbol $\perp$ if σ is invalid.

unsigncrypt()
{
a) Compute $QID_u = H_1(ID_u)$
b) Compute $y = \hat{e}(U, SID_r)$ and then $k = H_3(y)$
c) $m^1 = k \oplus C$ and $h = H_2(U, m^1)$
d) Accept m^1 if
$\hat{e}(V,P) = \hat{e}\left(h.QID_u, P_{pub}\right) \hat{e}\left(U, P_{pub}\right)$
else return $\perp$.
}

B. CORRECTNESS PROOFS

This is the correctness proof of equation $\hat{e}(V,P) = \hat{e}\left(h.QID_u, P_{pub}\right) \hat{e}\left(U, P_{pub}\right)$ in Unsigncryption phase is as follows:

$$\begin{aligned}\hat{e}(V,P) &= \hat{e}(hSID_u + W, P) \\ &= \hat{e}(hSID_u, P)\hat{e}(W,P) \\ &= \hat{e}(h.s.QID_u, P)\hat{e}(xP_{pub}, P)\end{aligned}$$

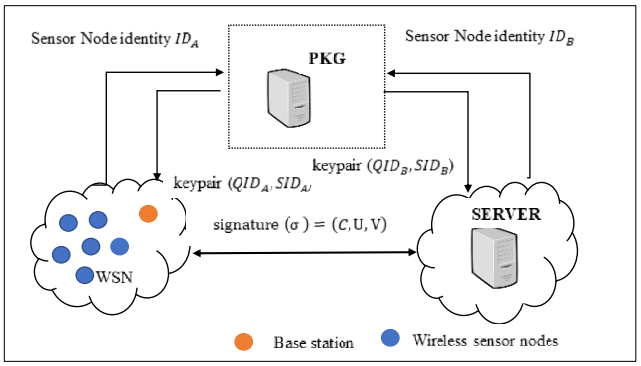

FIGURE 2. Secure communication model of IoT.

$$= \hat{e}(h.QID_u, s.P)\hat{e}(x.s.P, P)$$
$$= \hat{e}(h.QID_u, s.P)\hat{e}(x.P, s.P)$$
$$= \hat{e}(h.QID_u, P_{pub})\hat{e}(U, P_{pub})$$

C. APPLICATION OF SIGNCRYPTION SCHEME IN IoT

Here, we describe about the application of the proposed scheme in the IoT. WSNs composed of large number of tiny nodes, which plays an important part and they are involved in the collection of environmental data for IoT. All these nodes are connected to base station, which is act as the gateway between the sensor nodes and the user since it is forwarding the data from WSNs and the Internet Server. This communication between WSNs and the server should be secured with security services like confidentiality, authentication, integrity, and non-repudiation. Figure 2 shows the secure communication model for IoT using the proposed scheme. This model consists of mainly three entities, PKG, WSNs and the server. Initially PKG runs the setup() routine to finalize the system parameters. Then PKG runs the extract() routine to generate the keypairs to the base station and the server. The base station is loaded with the precomputed result from off-signcrypt() routine. When the WSNs is needed to send the data to the server, the base station runs on-signcrypt() routine and sends the σ to the server. After receiving, the server runs the unsigncrypt() to recover the m and then accepts it after verifying the validity. The computational cost of the base station is very small since there is no exponentiation or pairing in on–signcrypt() routine.

V. SECURITY ANALYSIS OF ID-BASED OOSC

Proposed algorithm is secured against the indistinguishable adaptive chosen ciphertext attacks and existential unforgeability against adaptive chosen message attacks.

Theorem 1: In random oracle model, Adversary ($\mathbb{A}$) has a less advantage ε against IND-CCA2 security, algorithm will run for time, performs q_u unsigncryption queries and qH_i queries for $i = 1,2,3$, then there exists an algorithm which can solves the algorithm with an advantage of

$$\varepsilon' \geq \frac{\varepsilon}{(2qH_2 + qH_3)}(1 - \frac{q_u}{2^k}) \quad (6)$$

Proof: In this proof, we show how challenger ($\mathbb{C}$) can use $\mathbb{A}$ as a subroutine in order to solve given instance $(P, \alpha P)$ of BDHIP.

1. Setup Phase: $\mathbb{C}$ runs setup routine with the security parameters as input, then sends *param* to $\mathbb{A}$ by keeping the master private key in secret. $\mathbb{C}$ chooses $s \in z_p^*$ randomly and computes the $P_{pub} = sP$ *and* $g = \hat{e}(P, P)$. Then sends all *param* to the $\mathbb{A}$.
2. $\mathbb{A}$ performs the following oracle queries to $\mathbb{C}$ in order to extract the secured information. The queries submitted by $\mathbb{A}$ during the setup phase is discussed below:
   - Key Extract query: $\mathbb{A}$ submits his ID_i to PKG and tries to get the corresponding secretkey SID corresponding to ID_i.
   - signcryption query: $\mathbb{A}$ produces m, sender and receiver $IDs(ID_A, ID_R)$ to $\mathbb{C}$. He computes ID_i's privatekey and runs the algorithm off-signcrypt() to obtain an off-line signcryption δ'. Finally $\mathbb{C}$ returns σ to $\mathbb{A}$.

     $\mathbb{C}$ simulates $\mathbb{A}$'s challenger in IND-CCA2 game. $\mathbb{C}$ maintains lists $L_1, L_2,$ *and* L_3 in order to maintain three hash oracles $H_1, H_2, andH_3$. $\mathbb{A}$ will ask the following queries in order to use them in any other queries.
     - **H_1 query:** For the user with ID_A, $\mathbb{A}$ submits query for $H_1(ID_A)$, $\mathbb{C}$ checks the value of H_1 for the input ID_A on list L_1 and returns the value from the list, otherwise returns a random $h_{1,A} \in z_p^*$ as the reply, inserts value $(ID_A, h_{1,A})$ onto L_1.
     - **H_2query:** For query on H_2, $\mathbb{C}$ checks the H_2 value is defined for input m_A and U_A earlier. If it was defined previously corresponding value will be returned, otherwise $\mathbb{C}$ returns a random $h_{2,A} \in z_p^*$ in reply. In addition to that $\mathbb{C}$ calculates the random oracle and inserts the tuple $(m_A, U_A, h_{2,A})$ into L_2.
     - **H_3 query:** As and when $\mathbb{C}$ receives request for $H_3(y_A)$ query, it first checks for the existence of the H_3 value for the input y_A, return its matched value from the L_3, otherwise, $\mathbb{C}$ randomly choose $h_{3,A}$ from $\{0, 1\}^n$, return it as the answer and inserts the tuple $(y_A, h_{3,A})$ into list L_3.

A. UNSIGNCRYPTION QUERY

This query is mainly targeted to extract the message from the queries results collected by the $\mathbb{A}$. At any time, $\mathbb{A}$ can perform make an unsigncrypt query on ciphertext $\sigma = (C, U, V)$, and sender's private key SID_A.$\mathbb{C}$ executes the 1 to find , $h_{1,A} = H_1(ID_A)$ and tries to estimate the sender's private key $SID_A = s.h_{1,A}$.Later, he tries to find $h_{2,A} = H_2(U_A, H_3(\hat{e}(U_A, SID_A)) \oplus C)$.Then For all ciphertexts he check the list L_2 for the entries of the form $(U_A, h_{2,A})$, returns the message m_A if any entry was matched otherwise rejects σ. The probability in rejection of ciphertext do not exceed $\frac{q_u}{2^k}$.

B. GUESS

$\mathbb{C}$ fetches a random entry from L_2 or L_3, since L_3 is containing additionally $qH_2 + qH_3$ records, choosing the right element, is having the probability $1/2qH_2+qH_3$. From the analysis, the probability of not aborting is prob $[\neg E]$ we know prob $[\neg E] \leq \frac{q_u}{2^k}$. So prob $[\neg E] = 1\text{-}.\frac{q_u}{2^k}$. In addition to that $\mathbb{C}$ may choose the right element from L_2 or L_3 with the probability of $1/2qH_2+qH_3$. Therefore, we have an advantage of $\varepsilon' \geq \frac{\varepsilon}{(2qH_2+qH_3)}(1 - \frac{q_u}{2^k})$

Theorem 2: The proposed scheme is existentially unforgeable under a chosen message attack.

Proof: The challenger ($\mathbb{C}$) generates a valid keypair *(pk,sk)* and gives pk to the adversary($\mathbb{A}$).The attacker may now repeatedly ask for signatures on chosen messages $(m_1, m_2, \ldots, m_q)$ of its choosing, and receives the valid signatures $(\sigma_1, \sigma_2, \ldots, \sigma_q)$ in response. At the conclusion of the experiment, the attacker must output a message and signature (m^*, σ^*) such that (1) the message m^* was not one of the messages requested in the previous step, and (2) the message/signature verifies correctly under the public key.

We can also prove that our proposed scheme is existentially unforgeable under a chosen message attack in the standard model, In the random oracle model, if an adversary $\mathbb{A}$ has an advantage $\epsilon \geq 10(q_s + 1)(q_s + q_{H_2})/2^k$ against the EUF-CMA security of the proposed scheme when running in a time t and performing q_s signcryption queries and q_{H_i} queries to oracles $H_i (i = 1, 2, 3)$, then there exists an algorithm $\mathbb{C}$ that can solve the q-SDHP for $q = q_{H_1}$ in expected time $\mathbb{C}$ can solve the q-SDHP in expected time

$$t^1 \leq 120686 q_{H_1} q_{H_2} \frac{t + O(q_s t_p)}{\epsilon(1 - 1/2^k)(1 - q/2^k)} + O(q^2 t_m) \quad (7)$$

where t_p denotes the cost for one pairing computation and t_m denotes the cost for a scalar multiplication computation in G_1.

we show $\mathbb{C}$ can provide a faithful simulation to $\mathbb{A}$ and solve the q-SDHP by interacting with $\mathbb{A}$. $\mathbb{C}$ takes as input $(P, \alpha P, \alpha^2 P, \ldots, \alpha^q P)$ and aims to find a pair $\mathbb{C}$ simulates $\mathbb{A}$'s challenger in the EUF-CMA game. F then adaptively performs key generation and signcryption queries as explained in the EUF-CMA game. We describe this process as follows.

Initial: First, $\mathbb{C}$ chooses $w_1, w_2, \ldots, w_q \in Z_p^*$ randomly. takes $\mathbb{C}$ takes as input $(P, \alpha P, \alpha^2 P, \ldots, \alpha^q P)$ as input to compute a generator $Q \in G_1$ and another element $Q_{pub} = \alpha Q \in G_1$. $\mathbb{C}$ sends $\mathbb{A}$ the system parameters with the generator Q, $Q_{pub} = \alpha Q$ and $g = \hat{e}(Q, Q)$. $\mathbb{C}$ chooses a random challenge identity $ID_s^* \in \{0, 1\}^*$ and sends it to A. In addition, $\mathbb{C}$ runs PKI-KG algorithm to get a receiver's public/secret key pair (pk_r^*, sk_r^*) and sends (pk_r^*, sk_r^*) to $\mathbb{A}$.

Attack: $\mathbb{C}$ simulates $\mathbb{A}$'s challenger in the EUF-CMA game. $\mathbb{C}$ maintains three lists L_1, L_2 and L_3 to simulate the hash oracles H_1, H_2 and H_3 respectively. We also assume that H_1 queries are distinct and that $\mathbb{A}$ will ask for H_1 (*ID*) before ID is used in any other queries.

- **H_1queries**: These queries are indexed by a counter v that is initially set to 1. If ID $= ID_s^*$, $\mathbb{C}$ returns a random $w_s \in Z_p^*$ as the answer. Otherwise, $\mathbb{C}$ returns w_v as the answer and increments v. In both cases, $\mathbb{C}$ puts the tuple *(ID, w)* (where $w = w_s or\ w_v$) into the list L_1.
- **H_2queries**: For a query $H_2(m_i, U_i)$, $\mathbb{C}$ first checks if the value of H_2 was previously defined for the input (m_i, U_i). If it was, the previously defined value is returned. Otherwise, $\mathbb{C}$ returns a random $h_{2,i} \in Z_p^*$ as the answer and inserts the tuple $(m_i, U_i, h_{2,i})$ into the list L_2.
- **H_3queries**: For a $H_3(r_i)$ query, $\mathbb{C}$ first checks if the value of H_3 was previously defined for the input r_i. If it was, the previously defined value is returned. Otherwise, $\mathbb{C}$ randomly chooses $h_{3,i}$ from $\{0, 1\}^n$, returns $h_{3,i}$ as an answer and inserts the tuple $(r_i, h_{3,i})$ into the list L_3.

Key generation queries: When $\mathbb{A}$ makes a key generation query on an identity ID_i, if $ID_i = ID_s^*$, then $\mathbb{C}$ fails and stops. Otherwise, $\mathbb{C}$ knows $H_1(ID_i) = w_i$ and returns $V_i = \alpha w_i$ to $\mathbb{A}$.

signcryption queries: $\mathbb{A}$ chooses a plaintext m and a sender's identity ID_i. If $ID_i \neq ID_s^*$, then $\mathbb{C}$ knows the sender's private key SID_i and can answer the query according to the steps of Off-Signcrypt and On-Signcrypt. If $ID_i = ID_s^*$, $\mathbb{C}$ does the following steps.

- Choose $\mathbb{x} \leftarrow Z_p^*$ randomly
- Compute $\mathbb{U} = \mathbb{x}Q$, $\mathbb{W} = \mathbb{x}Q_{pub}$
- Compute $y = \hat{e}(\mathbb{W}, QID_r)$ and then $k = H_3(y)$ and $h = H_2(\mathbb{U}||m)$
- $\mathbb{V} = hSID_u + \mathbb{W}$ and $C = m \oplus k$
- Return $\sigma = (C, \mathbb{U}, \mathbb{V})$ to $\mathbb{A}$

Next, we coalesce the sender identity ID_s^* and the message m into a ''generalized'' forged message (ID_s^*, m) so as to hide the identity-based aspect of the EUF-CMA attacks, and simulate the setting of an identity-less adaptive-CMA existential forgery for which the forking lemma is proven.

From the forking lemma, if $\mathbb{A}$ is an efficient forger in the above interaction, then we can construct a Las Vegas machine A^1 that outputs two signed messages $((ID_s^*, m), \mathbb{x})$ and $((ID_s^*, m), \mathbb{x}^*)$ with $\mathbb{x} \neq \mathbb{x}^*$ and the same commitment.

Finally, to solve the q-SDHP based on the machine $\mathbb{A}^1$ derived from $\mathbb{A}$, we construct a machine $\mathbb{C}$ as follows.

$\mathbb{C}$ gets two distinct signatures $((ID_s^*, m), \mathbb{x})$ and $((ID_s^*, m), \mathbb{x}^*)$ by running $\mathbb{A}^1$.$\mathbb{C}$ outputs *(ws, 1 α+ ws P)* as the solution of q-SDHP.

From the forking lemma and the lemma on the relationship between given-identity attack and chosen-identity attack, if $\mathbb{A}$ succeeds in a time t with probability $\geq 10(q_s + 1)(q_s + q_{H_2})/2^k$, then $\mathbb{C}$ can solve the q-SDHP in expected time $t^1 \leq 120686 q_{H_1} q_{H_2} \frac{t+O(q_s t_p)}{\epsilon(1-1/2^k)(1-q/2^k)} + O(q^2 t_m)$.

VI. RESULTS AND COMPARATIVE ANALYSIS

The performance of the proposed technique was compared against the computational cost, key magnitude, security perspective, ciphertext size, and storage requirement of existing schemes are shown in Table 2. We considered $|G_1| = 160$ bits, $|G_2| = 1024$ bits, $|P| = 160$ bits, $|m| = 160$ bits and $|ID| = 160$ bits. Its performance is compared against existing approaches in terms of signcrypt phase, unsigncrypt phase, and also in security perspective. Also, we had done

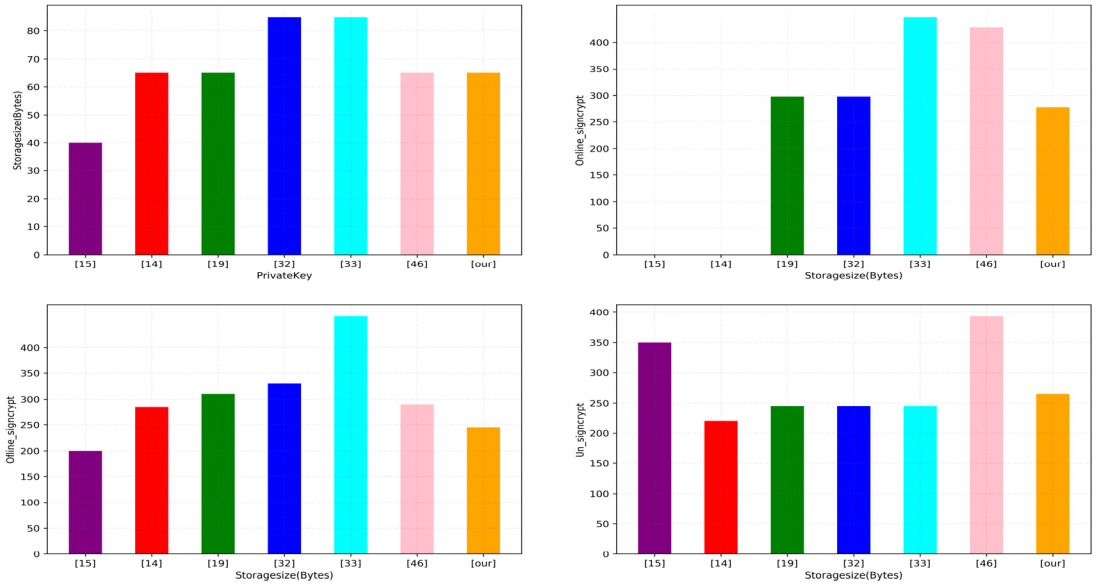

FIGURE 3. Comparative analysis of proposed technique with existed techniques.

the comparative analysis in terms of key size. The notations used are A-addition, Mul-multiplication, XOR-Exclusive OR operation, e-exponentiation, H-hashing, S-subtraction, and Pa-pairing. From the table, we can observe that the proposed algorithm computational cost is less than other existing techniques. In the ''Security'' column, security comparison was performed in terms of CCA2(INDCCA2), CMA(EUF-CMA), and Insider Security(IS). The key size parameter is the sum of sizes of publickey and secretkey were used in the comparison. In the proposed technique, point multiplication has been precomputed during off-line. The online phase does pairing operation, completes signcryption process immediately after m is decided. Therefore, it is fitting to provide a security solution for sensors. The taken key size of PKI is 320 bits in every scheme. For ciphertext length of [14], [19], [15], [31], [32], [41] and ours are 640,640,960,1520,1520,1200 and 1200 bits respectively.

By standard compression technique [46]the G_1 size can be reduced to 65 bytes. As, the existing algorithms are having offline storage, off-signcrypt, on-signcrypt and unsigncrypt phases, proposed algorithm is compared in terms of these phased, so the offline storage is calculated by considering the length of $\left|Z_p^*\right|$ is 20 bytes, G_1 is 65 bytes and G_2 is 128 bytes.

The private key size is calculated by the number of bits used in the derivation of user private key. The comparative analysis of the Hetro [15], SL [14], Fagen [19], LTX [31], LZZ [32], Jawaid [41] and proposed scheme are $2*\left|Z_p^*\right| = 40$bytes, $G_1 = 65$ bytes, $G_1 = 65$ bytes, $\left|Z_p^*\right| + G_1 = 20+65 = 85$ bytes, $\left|Z_p^*\right| + G_1 = 20+65 = 85$ bytes, $G_1 = 65$ bytes, and $G_1 = 65$ bytes respectively.

The offline storage is calculated by summing up the total storage space required to pass the variables derived in offline signcryption phase which are shared to online storage. The comparison of this feature in Hetro [15], SL [14], Fagen [19], LTX [31], LZZ [32], Jawaid [41], and proposed scheme are Zero, Zero, $2\left|Z_p^*\right|+2G_1+G_2 = 2*20+2*65+128 = 298$ bytes, $\left|Z_p^*\right|+2G_1+G_2 = 20+2*65+128 = 298$ bytes, $3\left|Z_p^*\right| + 4G_1 + G_2 = 3*20+4*65+128 = 448$ bytes, $2\left|Z_p^*\right| + 4G_1 + G_2 = 2*20+4*65+128 = 428$ bytes, $\left|Z_p^*\right| + 2G_1 + G_2 = 20+2*65+128 = 278$ bytes respectively.

The on-signcrypt is nothing but the sum of the sizes of the parameters passing to the recievers side after completion of the online signcryption phase. The comparative analysis of Hetro [15], SL [14], Fagen [19], LTX [31], LZZ [32], Jawaid [41], and proposed scheme are $2\left|Z_p^*\right| + |m| = 2*20+160$ bytes $= 200$bytes, $3\left|Z_p^*\right| + G_1 + |m| = 3*20+65+160$bytes $= 285$bytes, $\left|Z_p^*\right| + 2G_1 + |m| = 20+2*65+160$ bytes $= 310$ bytes, $2\left|Z_p^*\right| + 2G_1 + |m| = 2*20+2*65+160$ bytes $= 330$ bytes, $2\left|Z_p^*\right| + 4G_1 + |m| = 2*20+4*65+160$ bytes $= 460$bytes, $2G_1 + |m| = 2*65+160 = 290$ bytes and $\left|Z_p^*\right| + G_1 + |m| = 20+65+160 = 245$ bytes respectively.

The unsigncrypt operation is calculated by the computation time of the entire unsigncryption phase. The comparative analysis of Hetro [15], SL [14], Fagen [19],LTX [31], LZZ [32], Jawaid [41], and proposed scheme are $3\left|Z_p^*\right| + 2G_1 + |m| = 3*20+2*65+160 = 350$ bytes, $3\left|Z_p^*\right| + |m| = 3*20+160 = 220$bytes, $\left|Z_p^*\right| + G_1 + |m| = 20+65+160 = 245$ bytes, $\left|Z_p^*\right| + G_1 + |m| = 20+65+160 = 245$ bytes,

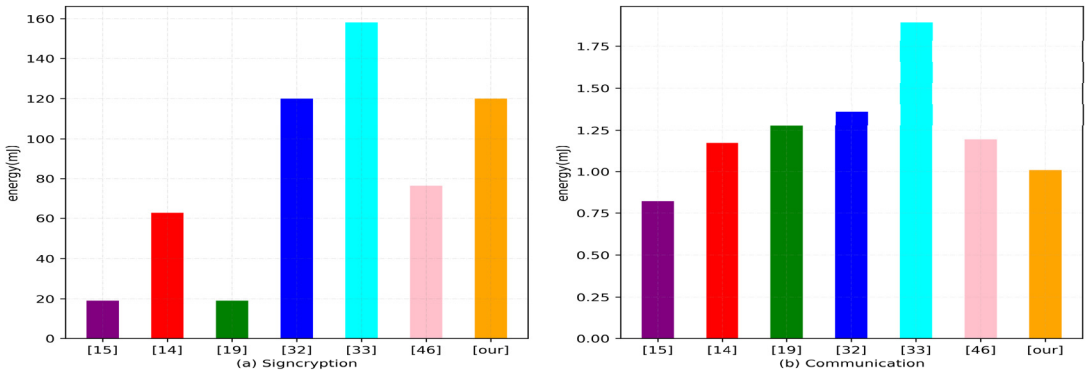

FIGURE 4. Comparison of algorithm energy consumptions.

$\left|Z_p^*\right| + G_1 + |m| = 20{+}65{+}160 = 245$ bytes, $2\left|Z_p^*\right| + G_1 + |m| + G_2 = 2{*}20{+}65{+}20{+}128{+}160 = 393$ bytes, and $2\left|Z_p^*\right| + G_1 + |m| = 2{*}20{+}65{+}160$ bytes $= 265$ bytes respectively.

The overall comparative analysis of the proposed technique with other algorithms is shown in Figure 3.

We adopt the experiment in [17] on MICA2 that is equipped with an ATmega128 8-bit processor clocked at 7.3728 MHz, 4 KB RAM and 128 KB ROM. A point multiplication needs 0.81s using an elliptic curve with 160 bits p.

Figure 4 shows the comparative analysis of energy consumption in terms of offline/online signcryption (Figure 4.a) and communication cost (Figure 4.b) against various existing techniques w.r.t proposed mechanism, according to [17], [18] the energy consumption for a point addition is negligible, a point multiplication uses 19.1mJ and a pairing uses 62.73mJ. Time for online/offline sign_crypt where we are calculating the energy consumption of all the existing techniques with the proposed one, where we are considering only multiplication and pairing energy consumption in both online/offline phases. The energy consumption of Hetro [15], SL [14], Fagen [19], LTX [31], LZZ [32], Jawaid [41], and proposed scheme are 19.1(mj),62.73(mj), 19.1(mj), 120.03(mj), 158.23(mj), 76.4(mj), 120.03(mj) respectively.

According to [20], the MICA2 costs 4.12μ J for bit transmission. Communication costs is nothing but the number of bits outputted from onsigncrypt phase of Hetro [15], SL [14], Fagen [19], LTX [31], LZZ [32], Jawaid [41], and proposed scheme are 0.824(mj),1.1742(mj),1.2772(mj),1.3596(mj), 1.8952(mj),1.1948(mj),1.0094(mj) respectively.

VII. CONCLUSION

An Identity based OOSC scheme was proposed, allows the IoT devices such as sensors, servers can communicate in a secured manner. Our method has adopted both user identity and online/off-line methodology features in order to improve the security level. Algorithm is compared against many existing algorithms, proved that more secured and taken less computation time. Also proved that it is secured against IND-CCA2 and unforgeability, provide the basic security services like end-to-end security services.

As the proposed technique is suitable for many applications like health monitoring system, industrial IoT, smart cities etc. As part of future work, one can apply the proposed approach to build healthcare monitoring systems and IoT based industrial systems.

REFERENCES

[1] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security challenges in the IP-based Internet of Things," *Wireless Pers. Commun.*, vol. 61, no. 3, pp. 527–542, Dec. 2011.

[2] T. Yan and Q. Y. Wen, "A trust-third-party based key management protocol for secure mobile RFID service based on the Internet of Things," in *Advances in Intelligent and Soft Computing* (Lecture Notes in Computer Science), vol. 135. Berlin, Germany: Springer-Verlag, 2012, pp. 201–208.

[3] J. Liu, X. Hu, Z. Wei, D. Jia, and C. Song, "Location privacy protect model based on positioning middleware among the Internet of Things," in *Proc. Int. Conf. Comput. Sci. Electron. Eng.*, Hangzhou, China, Mar. 2012, pp. 288–291.

[4] X. Zhou, Z. Jin, Y. Fu, H. Zhou, and L. Qin, "Short signcryption scheme for the Internet of Things," *Informatica*, vol. 35, no. 4, pp. 521–530, 2011.

[5] Y. Zheng, "Digital signcryption or how to achieve cost (signature and encryption) 6 cost (signature) + cost(encryption)," in *Advances in Cryptology-Crypto*, vol. 1294, J. G. Hartmanis and J. van Leeuwen, Eds. Berlin, Germany: Springer-Verlag, 1996, pp. 291–312.

[6] J. H. Andrew, Y. Dodis, and T. Rabin, "On the security of joint signature and encryption," in *Advances in Cryptology—EUROCRYPT 2002* (Lecture Notes in Computer Science), vol. 2332, L. R. Knudsen, Ed. Berlin, Germany: Springer-Verlag, 2002, pp. 83–107.

[7] J. Malone-Lee, "Identity based signcryption," CryptologyePrint Arch., Tech. Rep. 2002/098, 2002. [Online]. Available: http://eprint.iacr.org/2002/098

[8] B. Libert and J. J. Quisquater, "A new identity based signcryption scheme from pairings," in *Proc. IEEE Inf. Theory Workshop*, Paris, France, Mar./Apr. 2003, pp. 155–158.

[9] S. Even, O. Goldreich, and S. Micali, "On-line/off-line digital signatures," *J. Cryptol.*, vol. 9, no. 1, pp. 35–67, Mar. 1996.

[10] F. Zhang, Y. Mu, and W. Susilo, "Reducing security overhead for mobile networks," in *Proc. 19th Int. Conf. Adv. Inf. Netw. Appl.*, Taipei, Taiwan, vol. 1, Mar. 2005, pp. 398–403.

[11] D. Sun, X. Huang, Y. Mu, and W. Susilo, "Identity-based on-line/off-line signcryption," in *Proc. IFIP Int. Conf. Netw. Parallel Comput.*, Shanghai, China, Oct. 2008, pp. 34–41.

[12] J. K. Liu, J. Baek, and J. Zhou, "Online/offline identity-based signcryption revisited," in *Information Security and Cryptology* (Lecture Notes in Computer Science), vol. 6584. Berlin, Germany: Springer-Verlag, 2011, pp. 36–51.

[13] S. S. D. Selvi, S. S. Vivek, and C. P. Rangan, "Identity based online/off-line signcryption scheme," *Cryptol. ePrint Arch.*, vol. 2010, p. 376, 2010. [Online]. Available: http://eprint.iacr.org/2010/376.pdf

[14] Y. Sun and H. Li, "Efficient signcryption between TPKC and IDPKC and its multi-receiver construction," *Sci. China Inf. Sci.*, vol. 53, no. 3, pp. 557–566, Mar. 2010.
[15] Q. Huang, D. S. Wong, and G. Yang, "Heterogeneous signcryption with key privacy," *Comput. J.*, vol. 54, no. 4, pp. 525–536, Apr. 2011.
[16] S. Cui, P. Duan, C. W. Chan, and X. Cheng, "An efficient identity-based signature scheme and its applications," *Int. J. Netw. Secur.*, vol. 5, no. 1, pp. 89–98, Jul. 2007.
[17] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science), vol. 3156. New York, NY, USA: Springer-Verlag, 2004, pp. 119–132.
[18] P. Szczechowiak, A. Kargl, M. Scott, and M. Collier, "On the application of pairing based cryptography to wireless sensor networks," in *Proc. 2nd ACM Conf. Wireless Netw. Secur. (WiSec)*, Zurich, Switzerland, 2009, pp. 1–12.
[19] F. Li and P. Xiong, "Practical secure communication for integrating wireless sensor networks into the Internet of Things," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3677–3684, Oct. 2013.
[20] D. Galindo, R. Roman, and J. Lopez, "On the energy cost of authenticated key agreement in wireless sensor networks," *Wireless Commun. Mobile Comput.*, vol. 12, no. 1, pp. 133–143, Jan. 2012.
[21] S. S. M. Chow, S. M. Yiu, L. C. K. Hui, and K. P. Chow, "Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity," in *Information Security and Cryptology* (Lecture Notes in Computer Science), vol. 2971. New York, NY, USA: Springer-Verlag, 2004, pp. 352–369.
[22] X. Boyen, "Multipurpose identity-based signcryption: A swiss army knife for identity-based cryptography," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 2729. New York, NY, USA: Springer-Verlag, 2003, pp. 383–399.
[23] L. Chen and J. Malone-Lee, "Improved identity-based signcryption," in *Public Key Cryptography* (Lecture Notes in Computer Science), vol. 3386. New York, NY, USA: Springer-Verlag, 2005, pp. 362–379.
[24] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 3788. New York, NY, USA: Springer-Verlag, 2005, pp. 515–532.
[25] D. He and J. Chen, "An efficient certificateless designated verifier signature scheme," *Int. Arab J. Inf. Technol.*, vol. 10, no. 4, pp. 317–324, 2013.
[26] D. He, Y. Chen, and J. Chen, "An efficient certificateless proxy signature scheme without pairing," *Math. Comput. Model.*, vol. 57, nos. 9–10, pp. 2510–2518, 2013.
[27] D. He, B. Huang, and J. Chen, "New certificateless short signature scheme," *IET Inf. Secur.*, vol. 7, no. 2, pp. 113–117, Jun. 2013.
[28] D. He, J. Chen, and R. Zhang, "An efficient and provably-secure certificateless signature scheme without bilinear pairings," *Int. J. Commun. Syst.*, vol. 25, no. 11, pp. 1432–1442, Nov. 2012.
[29] Y. Sun and F. Zhang, "Secure certificateless encryption with short ciphertext," *Chin. J. Electron.*, vol. 19, no. 2, pp. 313–318, 2010.
[30] Y. Sun and H. Li, "Short-ciphertext and BDH-based CCA2 secure certificateless certificateless online/off-line signcryption for Internet of Things encryption," *Sci. China Inf. Sci.*, vol. 53, no. 1, pp. 2005–2015, 2012.
[31] M. Luo, M. Tu, and J. Xu, "A security communication model based on certificateless online/offline signcryption for Internet of Things," *Secur. Commun. Netw.*, vol. 7, no. 10, pp. 1560–1569, Oct. 2014, doi: 10.1002/Sec.836.
[32] J. Li, J. Zhao, and Y. Zhang, "Certificateless online/offline signcryption scheme," *Secur. Commun. Netw.*, vol. 8, no. 11, pp. 1979–1990, Jul. 2015.
[33] W. Shi, N. Kumar, P. Gong, N. Chilamkurti, and H. Chang, "On the security of a certificateless online/offline signcryption for Internet of Things," *Peer-Peer Netw. Appl.*, vol. 8, no. 5, pp. 881–885, Sep. 2015.
[34] Z. Xu, G. Dai, and D. Yang, "An efficient online/offline signcryption scheme for MANET," in *Proc. 21st Int. Conf. Adv. Inf. Netw. Appl. Workshops (AINAW)*, Niagara Falls, ON, Canada, May 2007, pp. 3–8.
[35] X. Chen, Y. Zhang, and Y. Yan, "Efficient online/offline signcryption without key exposure," *Int. J. Grid. Util Comput.*, vol. 4, no. 1, pp. 85–93, 2013.
[36] T. T. Thwin and S. Vasupongayya, "Blockchain based secret-data sharing model for personal health record system," in *Proc. 5th Int. Conf. Adv. Inform., Concept Theory Appl. (ICAICTA)*, Krabi, Thailand, Aug. 2018, pp. 196–201.
[37] Y. Huang and J. Yang, "A novel identity-based signcryption scheme in the standard model," *Information*, vol. 8, no. 2, p. 58, May 2017.
[38] J. Lai, Y. Mu, and F. Guo, "Efficient identity-based online/offline encryption and signcryption with short ciphertext," *Int. J. Inf. Secur.*, vol. 16, no. 3, pp. 299–311, Jun. 2017.
[39] A. Karati, S. H. Islam, G. P. Biswas, M. Z. A. Bhuiyan, P. Vijayakumar, and M. Karuppiah, "Provably secure identity-based signcryption scheme for crowdsourced industrial Internet of Things environments," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2904–2914, Aug. 2018.
[40] F. Li, Y. Han, and C. Jin, "Practical signcryption for secure communication of wireless sensor networks," *Wireless Pers. Commun.*, vol. 89, no. 4, pp. 1391–1412, Aug. 2016.
[41] J. Iqbal, A. I. Umar, N. Amin, and A. Waheed, "Efficient and secure attribute-based heterogeneous online/offline signcryption for body sensor networks based on blockchain," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 9, pp. 1–23, Sep. 2019.
[42] D. Yamamoto and W. Ogata, "Multidivisible online/offline cryptography and its application to signcryptions," *Secur. Commun. Netw.*, vol. 2019, pp. 1–21, Oct. 2019, doi: 10.1155/2019/1042649.
[43] F. Li, Y. Han, and C. Jin, "Certificateless online/offline signcryption for the Internet of Things," *Wireless Netw.*, vol. 23, no. 1, pp. 145–158, Jan. 2017, doi: 10.1007/s11276-015-1145-3.
[44] V. Balasubramanian and T. Mala, "Improved certificateless signcryption for IoT smart devices," *Appl. Math. Inf. Sci.*, vol. 13, no. 1, pp. 31–38, Jan. 2019.
[45] J. Qiu, K. Fan, K. Zhang, Q. Pan, H. Li, and Y. Yang, "An efficient multi-message and multi-receiver signcryption scheme for heterogeneous smart mobile IoT," *IEEE Access*, vol. 7, pp. 180205–180217, 2019.
[46] K.-A. Shim, "$\mathcal{CPAS}$: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 4, pp. 1874–1883, May 2012.

VANKAMAMIDI SRINIVASA NARESH received the M.Sc. degree in Mathematics from Andhra University, the M.Phil. degree in mathematics from Madurai Kamaraj University, the AMIE degree in CSE from IEI, and the M.Tech. and Ph.D. degrees in computer science and engineering from J.N.T.University-Kakinada. He is currently working as an Associate Dean (Research and Development) and a Professor with the Department of Computer Science and Engineering, Sri Vasavi Engineering College, Tadepalligudem, Andhra Pradesh, India. He is having a teaching experience of 19+ years. He successfully completed a UGC-Research Project. He published articles in reputed SCI journals in the area of cryptography and security. He published two books and a chapter in the area of security. He published two patents in blockchain-based group key agreements. He was a recipient of UGC.-C.S.I.R. Junior Research Fellowship and cleared NET for Lectureship in Mathematical sciences and also cleared UGC NET in Computer Science and Applications, and the State Best Researcher.

SIVARANJANI REDDI received the B.Tech. degree from NIT, Warangal, in 2002, and the M.Tech. and Ph.D. degrees in computer science from Andhra University, in 2005 and 2015, respectively. She is currently a Professor and the Head of the Computer Science Department, ANITS. She published articles in reputed SCI journals in the area of cryptography and security. She published two patents in blockchain based group key agreements. Her research interests include information security, cyber forensics, image processing, and opinion mining. She is a Life Member of ISTE and CSI.

SARU KUMARI received the Ph.D. degree in mathematics from CCS University, Meerut, India, in 2012. She has published more than 200 research papers in reputed international journals and conferences, including 180 publications in SCI-indexed journals. Her current research interests include information security and applied cryptography. She is on the Editorial board of the *AEÜ - International Journal of Electronics and Communications* (Elsevier) (SCI), the *International Journal of Communication Systems* (Wiley) (SCI-E), the *Telecommunication Systems* (Springer) (SCI), the *Human Centric Computing and Information Sciences* (Springer) (SCI-E), the *Transactions on Emerging Telecommunications Technologies* (Wiley) (SCI-E), the *Information Technology and Control*, Kaunas University of Technology, Lithuania (SCI-E), the *KSII Transactions on Internet and Information Systems* (SCI-E), published from Taiwan, the *Information Security: A Global Perspective*, Taylor & Francis (ESCI, Scopus), the *International Journal of Wireless Information Networks* (ESCI, Scopus), Springer, the *Journal of Reliable Intelligent Environments* (Springer) (ESCI, Scopus), the *Security and Privacy* (Wiley), the *Iran Journal of Computer Science* (Springer), and the *Azerbaijan Journal of High Performance Computing*, published by Azerbaijan State Oil and Industry University, Azerbaijan. She is the Technical Program Committee Member for more than a dozen of international conferences. She is a Reviewer of more than 50 reputed journals, including the SCI-indexed journals of IEEE, Elsevier, Springer, and Wiley. She has served as the Guest Editor for the Special Issue Big-Data and IoT in e-Healthcare for Computers and Electrical Engineering (Elsevier) (SCI-E), Elsevier.

V. V. L. DIVAKAR ALLAVARPU received the B.Tech. degree in computer science and engineering from the Avanthi Institute of Engineering and Technology, Visakhapatnam, India, in 2006, and the M.Tech. degree in artificial intelligence from the University of Hyderabad, Hyderabad, India, in 2008. He is currently an Assistant Professor with the FinTech Academy, GITAM Institute of Management, Visakhapatnam. His research interests include blockchain, network security, artificial intelligence, machine learning, cloud computing, and parallel computing. He is also managing Blockchain Centre of Excellence (BoE), FinTech Academy, GITAM (Deemed to be University). He published two patents in blockchain-based group key agreements.

SACHIN KUMAR received the Ph.D. degree in computer science from CCS University, Meerut, in 2007. Since October 2011, he has been working as a Professor with the Department of Computer Science and Engineering, Ajay Kumar Garg Engineering College (AKGEC), Ghaziabad. Prior to joining AKGEC, he has worked with the Raj Kumar Goel Institute of Technology (RKGIT) Ghaziabad, Krishna Institute of Engineering Technology (KIET), Ghaziabad, and CCS University, Meerut. He has more than 18 years of academic experience. He has guided four Ph.D. students and ten M.Tech. students. He has published/presented several papers in journals/conferences of repute. He is the author/coauthor of three books of computer science.

MING-HOUR YANG (Member, IEEE) received the Ph.D. degree in computer science and information engineering from National Central University, Taiwan. His research interests include network security and system security with particular interests on security issues in RFID and NFC security communication protocols. His topics include mutual authentication protocols, secure ownership transfer protocols, polymorphic worms, and tracing mobile attackers.