Received: 30 April 2019 | Revised: 17 July 2019 | Accepted: 18 August 2019

DOI: 10.1002/dac.4189

SPECIAL ISSUE ARTICLE

WILEY

An efficient lightweight authentication scheme for human-centered industrial Internet of Things

Jaya Singh[1] | **Ashish Gimekar**[2] | **Subramanian Venkatesan**[1]

[1]Department of Information Technology, Indian Institute of Information Technology, Prayagraj, Uttar Pradesh, India

[2]Walmart Labs, Bangalore, India

Correspondence
Jaya Singh, Department of Information Technology, Indian Institute of Information Technology, Prayagraj, Uttar Pradesh 211012, India.
Email: jayasinghoct20@gmail.com

Summary

Internet of Things (IoT) specifies a transparent and coherent integration of assorted and composite nodes. Unification of these nodes with large resources and servers has brought advancement in technology for industrial and government services. The industrial IoT (IIoT), with smart nodes, enhance the development and manufacturing of industrial process, which is on demand now. However, the security concern is substantial, and it is required to control to perform prosperous assimilation of IIoT. Authentication of these smart nodes and establishing mutual trust among them is essential to keep vulnerabilities and potential risks out. Hence, this paper presents an efficient lightweight secure authentication protocol from the perspective of human-centered IIoT. This proposed scheme assumes a registration center which simply generates public and secret information for a node when it initially joins the network. Once registration is done, the registration center is not needed anymore, and advanced processes like mutual authentication, secure key exchange, and communications are independently done by nodes involved. Furthermore, we show that this scheme can reduce exponential computations and computational overhead and resolves various possible attacks.

KEYWORDS

authentication, human-centered, industrial Internet of Things, Internet of Things, security

1 | INTRODUCTION

In recent years, technology has briskly changed our lives. The evolution of new technology such as Internet of Things (IoT) has changed the convention of relationship between human and machines (things) for the past years. This IoT is plotting an advance ecosystem for the human who is encircled by these *living* things. Recently, IoT has achieved a lot of consideration in the field of academia as well as in industries[1-3] for providing a new way of communication between human and things to make virtual information system in our environment.[4]

The term IoT related to industrial processes and critical infrastructure are known as industrial Internet of Things (IIoT) or Industry 4.0.[5] IIoT technology involves the industrial application like smart grid, logistics, transportation, aviation, smart city projects, energy/utilities, smart communication, and robotics. IIoT consists of a collection of smart machines, sensors, and actuators to increase the development and manufacturing power of industrial processes.[6] As many nodes

Abbreviations: IoT, Internet of Things; IIoT, Industrial Internet of Things.

join to a common network, it becomes difficult to identify and deal with security risks. To enhance security in the IIoT environment, these smart nodes must be authenticated before performing any service/task.

Internet of Drones (IoD)[7] is one of the IIoT technologies that includes constrained devices as entities. The constrained devices (drone or unmanned aerial vehicles) may collect the data and give it to users for further analysis and decision. Even, devices may share the data among themselves for decision making. In such a case, a device has to authenticate other devices and users (human-centric) before sharing the data and taking decision based on those data. Also, the confidential sharing of data is required. For example, IoD for the military is sensitive, and data should be confidential. A node or user of military IoD should be authenticated before sharing the data, and the data should be shared securely among nodes using the cryptographic algorithms, which needs shared key. Hence, we need a lightweight authentication scheme and secure key exchange mechanism for secure data sharing.

The IoT and IIoT applications generally ensure that nodes are registered with a Trusted Third Party (TTP)[8] before taking part in communication, and TTP is almost used in all the security operations such as for authentication and key sharing. Since TTP involves in the process of authentication, it leads to various security issues like the single point of failure due to the requirement of continuous availability of it and strict time requirements or session. Hence, many researchers are focusing on authentication scheme with no or less involvement of TTP. The proposed scheme uses single factor authentication because multi-factor authentication[9,10] needs some personal characteristics like card, fingerprint, iris scan, and voice recognition, which is suitable only for human to machine communication not for machine to machine communication, and also, they are very expensive and some complex in installation.

1.1 | Motivation and contribution

Innovation in the field of IoT has gained more attraction by researchers as well as industries in recent years because of its services, new ideas, and favorable circumstances towards making human life more easier and better in the future. Although IoT and IIoT have the same characteristics—availability, intelligence, and connected devices—both terms are different in general usage. IoT is generally used for end-user services such as connecting home appliances to the owner's mobile application to deal with them while IIoT is mostly used for industrial applications like manufacturing, monitoring, management, and development. The IIoT generally deals with efficiency and safety improvement by making physical systems online thus producing consequential advantages and also vulnerable to several attacks. Security is an important concern in the field of IIoT in common and needs more alertness while designing a network in the IIoT ecosystem. Security issues in IIoT provide us an opportunity to specify some efficient lightweight security schemes to protect the IIoT ecosystem from various attackers. Our contributions to this paper are as follows:

- An efficient secure authentication and encryption scheme proposed with lower computation and communication cost for human-centered IIoT based on Guillou-Quisquater's Protocol which reduces the exponential computation and multiplication overheads in the authentication process.
- Secure key sharing through the authentication process based on Diffie-Hellman key agreement algorithm.
- We have also considered previous authentication schemes with their suitability in IIoT ecosystem and presented a comparison with our scheme to show the efficiency with respect to computational cost.
- Device identity validation using Elliptic Curve digital signature public key recovery algorithm.

The remaining paper is organized as follows: Section 2 discusses the related works, Section 3 discusses the threat model to this proposed scheme, Section 4 discusses the detailed proposed authentication scheme, Section 5 provides the proof of correctness to the proposed authentication scheme, Section 6 analyzes the proposed scheme with existing schemes, implementation details with experimental results, and Section 7 discusses the security analysis of the proposed scheme. Finally, Section 8 concludes the paper with the directions of future work.

2 | RELATED WORK

The authentication based on password scheme proposed by Lamport[11] was a one-way hash function which suffered from high hash overhead and needed password resetting. Various password-based authentication schemes, such as previous studies,[12-16] have improved Lamport's scheme, but they have some drawback of storing a verification table which can partially or totally break the system if credential is stolen or modified by an adversary. To overcome this problem, Hwang et al[17] proposed an authentication scheme which requires a smart card by the user, but this scheme also suffers from the

difficulty of password modification. Hwang and Li[18] presented a verifier-free remote user authentication scheme based on ElGamal's public key.[19] Although, this scheme does not allow users to willingly select and alter their passwords, and also, it is vulnerable to forgery and impersonations attacks.[20-23] Kumar[24] had presented a new authentication scheme to overcome the drawbacks of Hwang and Li's scheme, but Shen[25] enhanced this scheme with pointing out the weaknesses of Kumar's scheme that it cannot tolerate insider attacks and smart card stolen attack. Liao et al[26] presented a scheme on password authentication to implement over the insecure network, but later, it was proven that vulnerable to offline password guessing attack, replay attack and denial of service (DoS) attacks. For tolerating these attacks, Kumar et al[27] improved the scheme of Liao et al. Next, Yang et al[28] presented a smart card–based mutual authentication scheme, but it was shown vulnerable to smart card loss attack by Ding Wang et al,[29] and they also proposed a new scheme for efficient authentication with higher security. Subsequently, Chen et al[30] presented a robust remote user password authentication protocol based on a smart card, but it was failed to perform flawless forward secrecy and also vulnerable to offline password guessing attack, impersonation attack, and insider attacks.

The expensive zero-knowledge proof[31-37] generally call upon by unidentified credential schemes and RSA-based schemes, but these schemes are not acceptable for feeble IoT nodes like sensors, actuators, and weak devices. The schemes for IoT or IIoT ecosystems should be lightweight and cost-effective; hence, we have focused on some attractive identity-based schemes with zero knowledge proof.

The first identity-based cryptosystem was presented by Shamir[38] which supports digital signature, but it does not support message encryption. Tsujii[39] proposed an identity-based scheme, which is based on the ElGamal's public key cryptosystem[40] and the discrete logarithm problem. This scheme has a high overhead of exponential computation and suffers from conspiracy problem. The use of identification information in key distribution systems was presented by Tanaka,[41] but it was find insecure for security purposes. The scheme of Shamir was then extended by Okamoto and Tanaka,[42] and they added encryption to this scheme, but it had also the problem of exponential computation overhead and it suffers from the risk of forging and disclosure. Fiat and Shamir[43] presented a protocol by taking the idea of zero-knowledge proof which relies on the difficulty of factoring. The drawback of this protocol is the number of iteration between prover and verifier. Guillou and Quisquater,[44] defined in RSA setting, improved Fiat-Shamir's protocol by reducing the cheating probability, but this scheme also suffers from the large exponential computation. Schnorr[45] presented a zero-knowledge–based identification protocol same as Guillou-Quisquater's protocol except that it is defined in a discrete logarithm setting instead of RSA setting. This protocol has the advantage of requiring just a single online modular multiplication by prover, but it requires more calculation on the verifier side than Fiat-Shamir's and Guillou-Quisquater's protocol. Okamoto[46] presented an identification scheme with the existence of proof of security by modifying Schnorr's protocol. Shieh[47] proposed an identification-based authentication scheme to resolve the security problem and computation overhead of the scheme of Okamoto and Tanaka. Koo et al[48] introduced the authenticated public key distribution scheme without TTP using authentication channel and hashing techniques. A randomly generated password will be shared through an authenticated channel (telephone, paper, etc) and the authenticity verified through the MAC. This solution achieves sharing without any third party. However, the authentication channel is required to share the password which is impossible in all the applications and scenario. Zhou and Lin[49] introduced the authentication protocol without a TTP. However, Key Generation Centre (KGC) is used to generate a partial key for the peers joining the network. Using partial key generated by the KGC, peers will generate the private key. This method is not efficient to authenticate the clients among themselves. Castiglione et al[50] had developed a one-time authentication protocol with noninteractive key scheduling an update. Initially, two parties will be agreed upon the master key and proceed further for key scheduling and others without any interaction among the parties, which is free from the TTP. However, it needs more computation (hash and pseudorandom) for every authentication. Tobias Jeske[51] described a protocol to preserve customer privacy without the involvement of any TTP which is based on zero-knowledge technique. This protocol is divided into two subprotocols, the one is Invoicing Protocol which takes an idea of asymmetric key cryptography to sign and encrypt invoicing data and the other is Load Reporting which is based on group signature schemes. This protocol requires partial group management and also prone to unlimited failure of data producers. Also, this protocol is not specifically for authentication purpose. Ranchal et al[52] have proposed an identity management scheme for cloud computing independent of TTP. This idea is based on the use of predicates over encrypted storage of identity data and multi-party computing for negotiating the use of a cloud service. It uses active bundle scheme for the untrusted host. Since this scheme is free from TTP, it reduces the risk of correlation and side channel attacks, but it suffers from DoS as active bundle may also be not executed at all in the remote host.

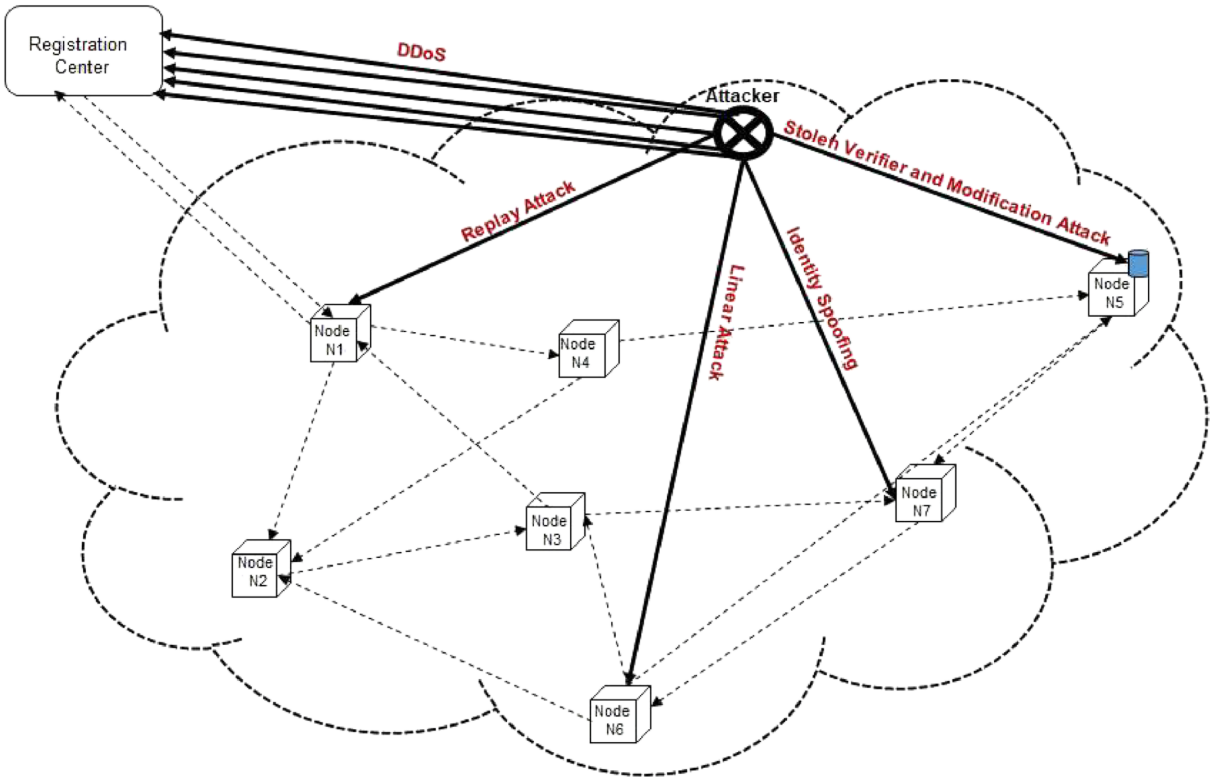

FIGURE 1 Representation of threat model

In recent years, various authentication schemes specifically for IoT and IIoT have proposed by many researchers. The scheme[53] has explained about health care IIoT enabled monitoring framework and validate its security by using watermarking. Schemes[54-56] have proposed user authentication in IIoT-based environment by using three-factor authentication, which are not suitable of IIoT devices as we have discussed earlier about its cons. There are schemes based on anonymous authentication[57,58] and lightweight authentication,[59-65] but most of them are completely based on TTP and having more overheads. Hence, we propose efficient lightweight authentication scheme with one time involvement of TTP with securing against different attacks.

3 | THREAT MODEL

In IIoT, security violation can happen as a result of system compromise or vulnerability. A node which tries to utilize the vulnerability and sabotage the system can be internal or external. The internal and external attacking nodes are the threat agents and following are the threats related to identity and authentication management system.

- Replay attack—Method of network attack in which a valid authentication data is dishonestly repeated by an unauthorized user.
- Identity spoofing—An unauthorized user taking on the identity of authorized node or user and then using that identity to achieve a malicious objective.
- DoS—A malicious user open-endedly disturb the network or a node inaccessible to its anticipated operators.
- Stolen-verifier and modification attack—An adversary steals verified data from the server during the existing or past authentication sessions or directly modifies the server's secret data.

Figure 1 shows the threat model related to identity and authentication management system. The attacker shown is part of the IIoT application; however, an attacker, outside the application, can also perform similar attack with additional effort. The Registration Centre is a part of the IIoT application; however, in Figure 1, it is shown as outsider because it is required only for the registration not for any further communication among nodes. The attacks are shown against individual nodes, but it may be against any single or multiple nodes.

4 | PROPOSED AUTHENTICATION SCHEME

We consider the human-centric perspective in IIoT environment and proposes the lightweight authentication scheme based upon it. The proposed scheme includes two entities: TTP called as Registration Centre (RC) and IIoT devices such as drones, gateways, and users. It is an identity-based authentication scheme, which follows Guillou-Quisquater's protocol[44] and provides a strong authentication with key exchange in IIoT ecosystem. It is also free from the TTP during secure message communication. This scheme runs in following three phases.

1. Preliminary phase—Registration center (TTP) generates and computes its secret parameters. *Entities Involved*: Registration Center
2. Registration phase—Construction of an extended identity for a new node joining the network. *Entities Involved*: Registration Center and client device
3. Authentication phase—Ensure mutual authentication between devices. *Entities Involved*: Client Devices.
4. Key exchange phase—Exchange of session key secure messaging. *Entities Involved*: Client Devices.

4.1 | Preliminary phase

This phase of protocol is not accountable for mutual authentication and also not for common keys generation. Initial RSA settings have done in this phase to create secret key.

4.1.1 | Step 1

The registration center takes two large prime numbers p and q to calculate n and ϕ similar to RSA as in Equations (1) and (2) algorithm.

$$n = p.q, \tag{1}$$

$$\phi(n) = (p-1)(q-1). \tag{2}$$

4.1.2 | Step 2

Select a primitive root g of p and q.

4.1.3 | Step 3

It chooses an static integer 3 ($e = 3$ as given in Shieh et al[47] initial phase, step 2) and calculates the inverse v.

$$v = e^{-1} mod\ \phi(n). \tag{3}$$

p, q, and v are the secrets only for the registration center.

4.2 | Registration phase

In this phase, the Registration Center (RC) commonly generates an *EID* for a fresh registered node with RSA settings and computes the secret value S_i for that registered node. The process of generating the *EID* is given in the following steps:

4.2.1 | Step 1

The registration center takes the unique identity ID of a joining node and generates *EID* with the help of one way function $f(0,1)^* \rightarrow \{0,1\}^m$, where m is the size of n in bits. For any node i, registration centre computes *EID* using Equation (4).

$$EID_i = f(ID_i). \tag{4}$$

The one way function $f(x)$ is made public for further use in verification process.

4.2.2 | Step 2

Registration center computes the secret value for node i as in Equation (5):

$$S_i = (EID_i)^v (mod\ n). \tag{5}$$

4.2.3 | Step 3

Registration center sends EID_i, n, g, and S_i to the node i over a secure channel. Node i must store the public information $f(x), n, g$ and secret information S_i for subsequent use. The registration center will not be needed any more for node i.

The registration center will securely delete v and S_i and ID_i for security purpose. In case, registration center stores secret values v and S of all nodes then there will be secret identity leakage if it is compromised.

4.3 | Authentication phase

This phase needs two nodes i and j for mutual authentication. Node j authenticate node i by a verification procedure. When node i is verified, node j believes that i is authentic. With the same procedure, node i verifies node j. The verification procedure is as follows:

4.3.1 | Step 1

When node i wish to communicate with node j, at first it generates a large random integer $r_i (1 \leq r_i \leq n-1)$, which is nonce during the time period. Using r_i, node will compute X_i and Y_i using Equations (6) and (7)

$$X_i = g^{r_i} (mod\ n), \tag{6}$$

$$Y_i = S_i.Time_i.g^{r_i} (mod\ n), \tag{7}$$

where $Time_i$ is the current linux timestamp of the node taken at the time of calculation of X_i and Y_i. Node keeps r_i secret. It is important to note that r is the random nonce for a time period that is in asynchronous network, messages will be accepted with Δ time delay. The random r is nonce for the Δ time; afterwards, it can be re-used; however, the chance will be less because it is from large uniform distribution space.

4.3.2 | Step 2

Node i sends X_i and Y_i with ID_i and $Time_i$ to node j for verification process.

4.3.3 | Step 3

Node j gets the message with all the contents from node i and compare $Time_i$ with the present local time of system to check the period of validation. If both times are under the valid period of time (the length of period of validation can be adjusted according to environment of the networks), then the message is accepted by the node j, otherwise rejected. After the validation of time, node j calculates $EID_i = f(ID_i)$ with the help of ID_i, one way function $f(.)$ and verify the equality as in Equation (8).

$$X_i.Time_i.EID_i \equiv EID_i^3.Y_i\ (mod\ n). \tag{8}$$

4.3.4 | Step 4

If the above equation satisfies, node j believes that node i is authentic and the message is sent by it. Node j stores X_i for later use (to generate common session keys). Then it generates r_j, calculate X_j and Y_j using Equations (9) and (10),

$$X_j = g^{r_j} (mod\ n), \tag{9}$$

$$Y_j = S_j.Time_j.g^{r_j} (mod\ n), \tag{10}$$

and sends these values X_j and Y_j along with ID_j and $Time_j$ to node i for mutual authentication.

4.3.5 | Step 5

On the other hand, node i receives the message along with all contents from node j, calculates $EID_j = f(ID_j)$, and verifies whether Equation (11) satisfies or not.

$$X_j.Time_j.EID_j \equiv EID_j^3.Y_j\ (mod\ n). \tag{11}$$

4.4 | Key exchange phase

After verification of authentication, both nodes generate a common session key for further communication.

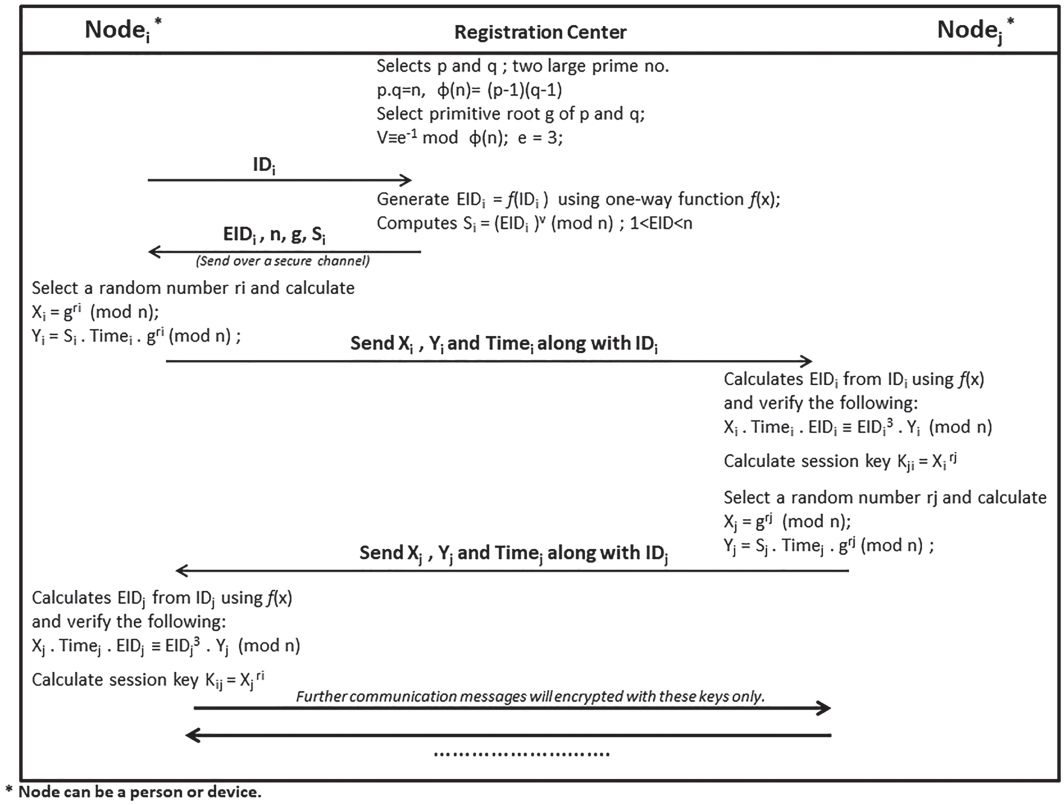

FIGURE 2 Process flow of the proposed authentication scheme

4.4.1 | Step 1

The node *i* authenticates node *j* and calculates session key K_{ij} as in Equation (12).

$$K_{ij} = X_j^{r_i} = g^{r_i.r_j}. \tag{12}$$

4.4.2 | Step 2

In the similar manner, the session key K_{ji} is calculated by node *j* as in Equation (13).

$$K_{ji} = X_i^{r_j} = g^{r_j.r_i}. \tag{13}$$

Now, both of the nodes have common session key $K_{ij} == K_{ji}$ to encrypt further communicating messages. The complete process flow of the proposed scheme is shown in Figure 2.

In the proposed scheme, nodes can mutually authenticate each other and derive the session key for secure communication in the public network.

5 | PROOF OF CORRECTNESS

As explained in the proposed authentication scheme, Equation 8 needs to be verified by both of the nodes to get authenticated. If both nodes are legitimate and information given by them is correct, then every time this equation will get satisfy. The correctness of Equation (8) is as follows:

$$X_i.Time_i.EID_i \equiv EID_i^3.Y_i \ (mod\ n).$$

By applying values of X_i and Y_i from Equation (6) and (7), we get

$$g^{r_i}.Time_i.EID_i \ (mod\ n) \equiv EID_i^3.S_i.Time_i.g^{r_i}(mod\ n)(mod\ n).$$

By solving the above equation, we get

$$EID_i \equiv EID_i^3.S_i(mod\ n).$$

Applying the value of S_i from Equation (5) in the above equation,

$$EID_i \equiv EID_i^3 \left(EID_i^v(mod\ n)\right)(mod\ n)$$

$$EID_i \equiv (EID_i^{3.v}). \tag{14}$$

According to RSA algorithm, we know that $3.v \equiv 1\ mod\ \phi(n)$. So now, it will be,

$$EID_i \equiv EID_i^1. \tag{15}$$

Above equation proves L.H.S. = R.H.S by following Fermat's little theorem. Hence, it proves the correctness of this proposed scheme.

6 | COMPARISON WITH EXISTING SCHEME

This proposed scheme extends the idea of Shieh et al[47] with reducing overheads. The comparative analysis of this proposed scheme has been done with Okamoto and Tanaka[42] and Shieh et al[47] to demonstrate the efficiency of this scheme as compared with previous studies[42,47] and.[66] The comparison of these schemes are as follows:

1. The scheme of Shieh[47] has modified registration phase with value $e = 3$ instead of any possible value as proposed in the scheme of Okamoto.[42] In this proposed scheme, we followed the scheme of Shieh by assuming $e = 3$.
2. The identity-based scheme of Okamoto and Tanaka[42] requires five exponential calculations (for calculating X_i, Y_i, Equation verification of both side and computing common key) for authenticating mutually and exchanging common key for a session. Although, the scheme of Shieh[47] reduced the computation overhead of the scheme of Okamoto and Tanaka from five to two (for calculating g^{r_i} and common key (K_{ij}) but uses lot of multiplications to calculate $X_i = g^{r_i}.g^{r_i}.g^{r_i}$, $Y_i = S_i.Time_i.g^{r_i}.g^{r_i}$ and for equation verification $(Y_i,Y_i,Y_i)(X_i,X_i)$ which increases computation overhead. The scheme of Hwang[66] also has the almost same calculation as the scheme of Shieh.[47] In our proposed scheme, we have reduced the exponential calculations. There are only two exponential calculations needed (one for g^{r_i} and other for K) and we have also removed the multiplication overheads presented in the scheme of Shieh.
3. The schemes of Okamoto,[42] Shieh,[47] and Hwang[66] have the common problem of storing a verification table at registration center while registration containing some secret values, which can sabotage the system if secrets are modified or stolen by attacker. In our proposed scheme, no devices' secret values are stored anywhere. The registration center secretly removes all the sensitive values just after sending it to that registered node. So there is no any problem of stolen or modification of any secret values at registration center's side.

6.1 | Comparison with digital certificate

Nowadays, the use of digital certificate is well accepted and used by almost by all the service provider for authentication and further key sharing purpose. The respective clients or service providers will be authenticated using the digital certificate. The problems with the certificate is cost, and it is not possible to afford digital certificate for the all IIoT devices connected in to the applications. For example, assume we are having the small network connected with 50 nodes and more nodes will join the network regularly. In this case, if we go for 50 or more digital certificate for device authentication, then it will be expensive. Also, there are evidence that certificate authorities are forced to issue certificate to a client who is not eligible for the certificate.[67] To overcome the issues, network can use the proposed scheme to authenticate as well as for key sharing without spending any cost for it.

6.2 | Implementation and evaluation

For better understanding the differences among[42,47,66] and our proposed scheme, we implemented the proposed and equivalent existing schemes in normal desktop computer (full system) with Intel core i7 Processor CPU with quad core running at 3.40 GHz with Windows 10 as well as the Raspberry pi 3B model device with 1.2 GHz quad core processor, 1GB RAM, ARM cortex A53 on a Raspbian Linux 9.4 to show applicability of the proposed authentication scheme in IIoT environment.

Scheme	128 bits	256 bits	512 bits	1024 bits	2048 bits
Okamoto[42]	8.05	10.79	21.07	61.28	251.47
Shieh[47]	5.04	8.56	12.29	27.18	74.42
Hwang[66]	4.69	6.75	10.89	26.43	78.73
Our proposed scheme	3.58	5.84	9.63	21.08	62.6

TABLE 1 Computational time comparison of authentication schemes on full system

Scheme	128 bits	256 bits	512 bits	1024 bits	2048 bits
Okamoto[42]	43.72	78.62	249.55	1388.85	9858.92
Shieh[47]	31.59	46.86	91.47	309.22	1785.36
Hwang[66]	29.63	41.45	88.35	314.89	1841.37
Our Proposed Scheme	24.91	37.14	73.28	270.64	1627.69

TABLE 2 Computational time comparison of authentication schemes on IoT device

Tables 1 and 2 present the computational performance of the proposed and existing schemes respectively implemented on desktop system and IoT device with respect to size of p and q at registration center. The result values are shown in milliseconds, and it is a linux timestamp. The implementation part includes all four phases of the schemes. Tables clearly show that the proposed scheme takes less computational time than all the existing schemes because of their less multiplication and calculation part as compared with existing schemes.

6.3 | Asymptotic analysis

For the calculation of X and Y, it needs $O(c^r) + O(c) => O(c^r)$ and $O(c^r) + O(c^3) => O(c^r)$ complexity respectively. To verify the authenticity that is Equation (11), proposed scheme needs $O(c^3) + O(c^4) => O(c^4)$ complexity, where n refers number of bits of the highest value used in the process. The computation complexity of X and Y and equality verification complexity of the proposed scheme and the scheme of Sheih[47] are the same; however, the proposed scheme requires less computation than the existing schemes as shown in Tables 1 and 2.

7 | SECURITY ANALYSIS

In this section, we analyze the security of the proposed scheme with respect to the threat model and features of the scheme.

7.1 | Replay attack

In our proposed scheme, the replay-attack is not possible because of Linux timestamp and random nonce from the large space. This timestamp is less than upper bound, and it helps to check the validity period of message to confirm its legitimacy by both of the communicating nodes and the random number is distinct for every session. In case, any attacker replays the eavesdropped message from open channel, the success rate of making receiver to accept the message is quite less.

For example, an attacker eavesdrop a communication session between node i and node j and it replay an old message of i to node j. On receiving the message, node j will examine the legality of $Time_i$. Let us consider two cases:

- If systems' clock are synchronized, then node j will confirm that message is invalid by checking $Time_i$ and reject the message.
- If systems' clock are not synchronized, then node j may reconsider the message if the time is within the acceptable range otherwise. In such case, the random nonce will be used to identify the replay and the message will be discarded.

Even the request is accepted, the response cannot be decapsulated by the attacker since r_i is known only to the owner. Hence, it prevent the message replay attack and further consequence.

7.2 | Stolen-verifier and modification attack

There are common drawback of storing a verification table by the registration center based authentication schemes.[12-16,42,47] If an attacker modifies or steals the table, then it will sabotage the complete system that is unauthorized users may get the service and authorized users may not get the service. In our proposed scheme, the registration center discards v, S and ID. Hence, this proposed scheme is resistant to stolen-verifier and modification attack.

7.3 | Identity spoofing

An attacker can spoof the identity *ID* of honest node and register with the registration center. In such case, attacker and honest node will have the same secret identity that is *S* computed using the identity *ID*. This attack will be handled differently in the two way of implementation.

- Record at registration center: RC will store all registered identity. In case any identity repeats, RC will drop such registration request. Hence, identity spoofing is not possible for re-registration.
- No record at registration center: RC will not store the registered identity details of any user to overcome the leakage of secrets after compromise. In case any attacker submits already registered identity, then RC will create the same secret identity *S* and share with the attacker. To overcome this issue, elliptic curve cryptography can be used to derive the node identity using the public key. Even though, attacker spoof the identity and register with registration center, it cannot sign the message using the original owner private key. The authenticating nodes or the RC will get the sender public key from the signature.

Using elliptic curve public key (p_b), the node identity will be derived as in Equation (16).

$$ID = f(p_b). \tag{16}$$

The value X_i of node i will be signed as in Equation 17 using elliptic curve private key (p_r) and sent to the other device along with X_i, Y_i, *Time* and *ID*.

$$r, s = Sig_{p_r}(X). \tag{17}$$

The receiving node validates the signature, and it can derive the public key (p_b) from the signature parameters r and s using the public key recovery concept of elliptic curve digital signature algorithm. Using the (p_b), the *ID* of node i will be computed and verified with the received *ID*. A node with private key can prove the ownership of identity not the attacker even though it has the *ID* known. Hence, identity spoofing will be mitigated by the proposed scheme however it takes additional computational cost but it is once for the session.

7.4 | Denial of service

An attacker can sabotage the system once they perform DoS attack against the registration center not with the individual nodes. The DoS attack on registration center will affect only the new nodes registration not the registered nodes communication. Hence, the DoS is prevented by the proposed scheme for message communication among devices.

7.5 | Linear attack

The scheme of Shieh[47] has used the timestamp to check the legality of message. Since it is linear in Equation (7), an attacker can masquerade as node i by computing

$$Y_i' = Y_i.(Time_i'/Time_i)(mod\ n). \tag{18}$$

Thus, the attacker masquerade as node i and sends (X_i, Y_i', $Time_i'$ and ID_i) to node j. Upon receiving this, node j verifies the equation (8) as

$$X_i.Time_i'.EID_i \equiv EID_i^3.Y_i' \quad (mod\ n). \tag{19}$$

Since the above equation verifies, thus the node j thwart by the attacker. To solve this problem, we follow the solution of the scheme of Hwang[66] by calcualting a random number $r_i' = r_i.Time_i \quad mod\ (n)$ and compute it in Equations (6) and (7) in place of r_i.

7.6 | Forward secrecy

It is a property that ensures that previous secrets of the communication in the system are secure even after master secret key is revealed. In our proposed scheme, different keys are used for every session, and it is constructed using r_i and r_j of nodes. Also consider, an attacker got the secret identity S_i of node i still it cannot compute the previously generated session key (K) without knowing r_i and r_j. Hence the proposed scheme offers forward secrecy.

8 | CONCLUSION AND FUTURE WORK

The IIoT environments such as manufacturing, aviation, and eHealth are the critical infrastructure, and its information are very sensitive when compared with the home automation application. Hence, it is important to secure the IIoT network and its communication. Thus, this paper proposed an authentication scheme, which guarantees the authenticity of the device, message, and secrecy of communication considering human-centric IIoT and generic IoT, which needs security. The proposed scheme is lightweight and more efficient than the existing schemes as shown in our experimental results. Also, we have analyzed the security property of the proposed scheme against different threats such as replay attack, conspiracy problem, Identity spoofing, stolen-verifier, and modification attack and DoS also ensure forward secrecy. The future work of this paper is to evaluate this proposed authentication scheme in different human-centered IIoT environment and prove the applicability.

ORCID

Jaya Singh https://orcid.org/0000-0002-7207-4151

REFERENCES

1. Roman R, Najera P, Lopez J. Securing the internet of things. *Comput*. 2011;9:51-58.
2. Främling K, Nyman J. The compromise between security and usability in the internet of things. In: Proceedings of Adavanced Production Management Systems (APMS); 2008; Finland:15-17.
3. Weber RH. Internet of things—new security and privacy challenges. *Comput Law Sec Rev*. 2010;26(1):23-30.
4. Bandyopadhyay D, Sen J. Internet of things: applications and challenges in technology and standardization. *Wireless Pers Commun*. 2011;58(1):49-69.
5. Fernández-Caramés TM, Fraga-Lamas P. A review on human-centered IoT-connected smart labels for the Industry 4.0. *IEEE Access*. 2018;6:25939-25957.
6. https://internetofthingsagenda.techtarget.com/definition/industrial-internet-of-things-iiot.
7. Mohammad W, Ashok KD, Neeraj K, Athanasios VV, Joel JPC. Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment. *IEEE Internet Things J*. 2019;6(2):3572-3584.
8. Tian Y, Zhang N, Lin Y-H, Wang X, Ur B, Guo X, Tague P. Smartauth: user-centered authorization for the internet of things. In: 26th {USENIX} security symposium ({USENIX} security 17); 2017:361-378.
9. He D, Kumar N, Lee J-H, Sherratt RS. Enhanced three-factor security protocol for consumer USB mass storage devices. *IEEE T Consum Electr*. 2014;60(1):30-37.
10. Huang X, Xiang Y, Chonka A, Zhou J, Deng RH. A generic framework for three-factor authentication: preserving security and privacy in distributed systems. *IEEE T Parall Distr Syst*. 2011;22(8):1390-1397.
11. Lamport L. Password authentication with insecure communication. *Commun of the ACM*. 1981;24(11):770-772.
12. Shimizu A. A dynamic password authentication method using a one-way function. *Syst Comput Japan*. 1991;22(7):32-40.
13. Neil H. The s/key (tm) one-time password system. In: Symposium on network and distributed system security; 1994:151-157.
14. Sandirigama M, Shimizu A, Noda M-T. Simple and secure password authentication protocol (sas). *IEICE T Commun*. 2000;83(6):1363-1365.
15. Chen T-H, Lee W-B. A new method for using hash functions to solve remote user authentication. *Comput Electr Eng*. 2008;34(1):53-62.
16. Harn L, Huang D, Laih C. Password authentication using public-key cryptography. *Comput Math Appl*. 1989;18(12):1001-1017.
17. Hwang T, Chen Y, Laih CJ. Non-interactive password authentications without password tables. In: IEEE tencon'90: 1990 IEEE Region 10 conference on computer and communication systems. conference proceedings IEEE; 1990:429-431.
18. Hwang M-S, Li L-H. A new remote user authentication scheme using smart cards. *IEEE T Consum Electr*. 2000;46(1):28-30.
19. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE T Inform Theory*. 1985;31(4):469-472.
20. Chan C-K, Cheng L-M. Cryptanalysis of a remote user authentication scheme using smart cards. *IEEE T Consum Electr*. 2000;46(4):992-993.
21. Shen J-J, Lin C-W, Hwang M-S. A modified remote user authentication scheme using smart cards. *IEEE T Consum Electr*. 2003;49(2):414-416.
22. Chang C-C, Hwang K-F. Some forgery attacks on a remote user authentication scheme using smart cards. *Inform*. 2003;14(3):289-294.
23. Yeh H-T, Sun H-M, Hsieh B-T. Security of a remote user authentication scheme using smart cards. *IEICE T Commun*. 2004;87(1):192-194.
24. Kumar M. New remote user authentication scheme using smart cards. *IEEE T Consum Electr*. 2004;50(2):597-600.
25. Shen Z-h. A new modified remote user authentication scheme using smart cards. *Appl Math J Chinese U*. 2008;23(3):371-376.
26. Liao I-E, Lee C-C, Hwang M-S. A password authentication scheme over insecure networks. *J Comput Syst Sci*. 2006;72(4):727-740.
27. Kumar M, Gupta MK, Kumari S. An improved efficient remote password authentication scheme with smart card over insecure networks. *IJ Network Secur*. 2011;13(3):167-177.

28. Yang G, Wong DS, Wang H, Deng X. Two-factor mutual authentication based on smart cards and passwords. *J Comput Syst Sci*. 2008;74(7):1160-1172.
29. Ding W, et al. Cryptanalysis and security enhancement of a remote user authentication scheme using smart cards. *The J China U Posts Telecommun*. 2012;19(5):104-114.
30. Chen B-L, Kuo W-C, Wuu L-C. Robust smart-card-based remote user password authentication scheme. *Int J Commun Syst*. 2014;27(2):377-389.
31. Au MH, Susilo W, Mu Y. Constant-size dynamic k-TAA. *International conference on security and cryptography for networks*. Berlin, Heidelberg: Springer; 2006:111-125.
32. Boneh D, Boyen X. Short signatures without random oracles. *International conference on the theory and applications of cryptographic techniques*. Berlin, Heidelberg: Springer; 2004:56-73.
33. Camenisch J, Kohlweiss M, Soriente C. An accumulator based on bilinear maps and efficient revocation for anonymous credentials. *International workshop on public key cryptography*. Berlin, Heidelberg: Springer; 2009:481-500.
34. Boneh D, Boyen X, Shacham H. Short group signatures. *Annual international cryptology conference*. Berlin, Heidelberg: Springer; 2004:41-55.
35. Camenisch J, Van Herreweghen E. Design and implementation of the idemix anonymous credential system. In: Proceedings of the 9th ACM Conference on Computer and Communications Security ACM; 2002:21-30.
36. Camenisch J, Lysyanskaya A. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. *International conference on the theory and applications of cryptographic techniques*. Berlin, Heidelberg: Springer; 2001:93-118.
37. Camenisch J, Lysyanskaya A. A signature scheme with efficient protocols. *International conference on security in communication networks*. Berlin, Heidelberg: Springer; 2002:268-289.
38. Shamir A. Identity-based cryptosystems and signature schemes. *Workshop on the theory and application of cryptographic techniques*. Berlin, Heidelberg: Springer; 1984:47-53.
39. Tsujii S, Itoh T, Kurosawa K. ID-based cryptosystem using discrete logarithm problem. *Electron Lett*. 1987;23(24):1318-1320.
40. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans Inform Theory*. 1985;31(4):469-472.
41. Tanaka H. A realization scheme for the identity-based cryptosystem. *Conference on the theory and application of cryptographic techniques*. Berlin, Heidelberg: Springer; 1987:340-349.
42. Okamoto E, Tanaka K. Identity-based information security management system for personal computer networks. *IEEE J Sel Areas Comm*. 1989;7(2):290-294.
43. Fiat A, Shamir A. How to prove yourself: practical solutions to identification and signature problems. *Conference on the theory and application of cryptographic techniques*. Berlin, Heidelberg: Springer; 1986:186-194.
44. Guillou LC, Quisquater J-J. A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory. *Workshop on the theory and application of of cryptographic techniques*. Berlin, Heidelberg: Springer; 1988:123-128.
45. Schnorr C-P. Efficient signature generation by smart cards. *J Cryptol*. 1991;4(3):161-174.
46. Okamoto T. Provably secure and practical identification schemes and corresponding signature schemes. *Annual international cryptology conference*. Berlin, Heidelberg: Springer; 1992:31-53.
47. Shieh S-P, Yang W-H, Sun H-M. An authentication protocol without trusted third party. *IEEE Commun Lett*. 1997;1(3):87-89.
48. Koo JH, Kim BH, Lee DH. Authenticated public key distribution scheme without trusted third party. *International conference on embedded and ubiquitous computing*. Berlin, Heidelberg: Springer; 2005:926-935.
49. Zhou Y, Lin H. An authentication protocol without trusted third party on p2p network. In: 2010 2nd international conference on future computer and communication, Vol. 2 IEEE; 2010:V2-686.
50. Castiglione A, De Santis A, Castiglione A, Palmieri F. An efficient and transparent one-time authentication protocol with non-interactive key scheduling and update. In: 2014 IEEE 28th International Conference on Advanced Information Networking and Applications IEEE; 2014:351-358.
51. Jeske T. Privacy-preserving smart metering without a trusted-third-party. In: Proceedings of the international conference on security and cryptography IEEE; 2011:114-123.
52. Ranchal R, Bhargava B, Othmane LB, Lilien L, Kim A, Kang M, Linderman M. Protection of identity information in cloud computing without trusted third party. In: 2010 29th IEEE Symposium on Reliable Distributed Systems IEEE; 2010:368-372.
53. Hossain MS, Muhammad G. Cloud-assisted industrial internet of things (IIoT)—enabled framework for health monitoring. *Comp Netw*. 2016;101:192-202.
54. Das AK, Wazid M, Kumar N, Vasilakos AV, Rodrigues JJ. Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment. *IEEE Internet Things J*. 2018;5(6):4900-4913.
55. Li X, Peng J, Niu J, Wu F, Liao J, Choo K-KR. A robust and energy efficient authentication protocol for industrial internet of things. *IEEE Internet of Things J*. 2017;5(3):1606-1615.
56. Li X, Niu J, Bhuiyan MZA, Wu F, Karuppiah M, Kumari S. A robust ECC-based provable secure authentication protocol with privacy preserving for industrial internet of things. *IEEE Trans Ind Informat*. 2017;14(8):3599-3609.
57. Alcaide A, Palomar E, Montero-Castillo J, Ribagorda A. Anonymous authentication for privacy-preserving IoT target-driven applications. *Comput Secur*. 2013;37:111-123.
58. Yang Y, Cai H, Wei Z, Lu H, Choo K-KR. Towards lightweight anonymous entity authentication for IoT applications. *Australasian conference on information security and privacy*. Berlin, Heidelberg: Springer; 2016:265-280.

59. Aman MN, Chua KC, Sikdar B. Mutual authentication in IoT systems using physical unclonable functions. *IEEE Internet Things J*. 2017;4(5):1327-1340.
60. Shivraj V, Rajan M, Singh M, Balamuralidhar P. One time password authentication scheme based on elliptic curves for internet of things (IoT). In: 2015 5th national symposium on information technology: Towards new smart world (NSITNSW) IEEE; 2015:1-6.
61. Moosavi SR, Gia TN, Rahmani A-M, Nigussie E, Virtanen S, Isoaho J, Tenhunen H. Sea: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Comput Sci*. 2015;52:452-459.
62. Yao X, Han X, Du X, Zhou X. A lightweight multicast authentication mechanism for small scale IoT applications. *IEEE Sens J*. 2013;13(10):3693-3701.
63. Porambage P, Schmitt C, Kumar P, Gurtov A, Ylianttila M. Two-phase authentication protocol for wireless sensor networks in distributed IoT applications. In: 2014 IEEE wireless communications and networking conference (WCNC) IEEE; 2014:2728-2733.
64. Li N, Liu D, Nepal S. Lightweight mutual authentication for IoT and its applications. *IEEE Trans Sustain Comput*. 2017;2(4):359-370.
65. Kalra S, Sood SK. Secure authentication scheme for IoT and cloud servers. *Pervasive Mob Comput*. 2015;24:210-223.
66. Hwang M-S, Chang C-C, Hwang K-F. An improved authentication protocol without trusted third party; 2001.
67. Allen C, Brock A, Buterin V, Callas J, Dorje D, Lundkvist C, et al. Decentralized public key infrastructure. Group Report. Rebooting the Web of Trust (RWoT). https://danubetech.com/download/dpki.pdf; 2015.

How to cite this article: Singh J, Gimekar A, Venkatesan S. An efficient lightweight authentication scheme for human-centered industrial Internet of Things. *Int J Commun Syst*. 2019;e4189. https://doi.org/10.1002/dac.4189