IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received November 9, 2020, accepted November 12, 2020, date of publication November 17, 2020,
date of current version December 7, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3038813

Using ID-Based Authentication and Key Agreement Mechanism for Securing Communication in Advanced Metering Infrastructure

SHAIK MULLAPATHI FAROOQ[1], (Senior Member, IEEE), S. M. SUHAIL HUSSAIN[2], (Member, IEEE), TAHA SELIM USTUN[2], (Member, IEEE), AND ATIF IQBAL[3], (Senior Member, IEEE)

[1]Department of Computer Science and Engineering, Madanapalle Institute of Technology and Sciences, Madanapalle 517325, India
[2]Fukushima Renewable Energy Institute, AIST (FREA), National Institute of Advanced Industrial Science and Technology (AIST), Koriyama 963-0298, Japan
[3]Department of Electrical Engineering, Qatar University, Doha 2713, Qatar

Corresponding author: Atif Iqbal (atif.iqbal@qu.edu.qa)

This work was supported in part by the Fukushima Prefectures' Reconstruction Grant, in 2020, and in part by the Open Access Funding provided by the Qatar National Library.

ABSTRACT Smart metering technology plays a key role in Advanced Metering Infrastructure (AMI) in Smart Grid (SG). Smart Meters (SM) measure Power Consumption Data (PCD) of household devices and send it to DSO (Distributed System Operator) for further processing. DSO utilizes PCD for different applications such as monthly billing, demand response and other applications related to power system operation and energy markets. Secure communication between SM and DSO is of paramount importance. Certificate-based authentication is a de facto mechanism in ensuring legitimacy of communicating parties. But it incurs more computational delay as it involves intensive processes such as certificate management, revocation, and verification. ID-based authentication eliminates the risks associated with certificate management. A key agreement protocol based on ID-based authentication mechanism is proposed and analyzed for computational performance. This paper analyzes and evaluates both authentication mechanisms: certificate and ID-based mechanism based on computational times for suitability in AMI network. The experimental results show that ID-based authentication and key agreement mechanism are suitable for securing communication in AMI network.

INDEX TERMS Cybersecurity in advanced metering infrastructure (AMI), smart meter (SM), distribution system operator (DSO), key agreement protocol, energy markets security.

NOMENCLATURE

Symbol	Explanation
X.509	Certificate format
SM	Smart Meter
DSO	Distributed System Operator
SM_{ID}	Smart meter Identification such as IP address or name.
DSO_{ID}	DSO Identification such as IP address or name
P_{SM}	Public key of smart meter
d_{SM}	Private key of smart meter
P_{DSO}	Public key of DSO
d_{DSO}	Private key of DSO
m	Master key at KGC
DSO_{SK}	Private key of DSO in ID based mechanism
CA	Certificate Authority
CSR	Certificate Signing Request
SMPrK	Smart meter's private key in certificate-based mechanism
SMPK	Smart meter's public key in certificate-based mechanism
CAPrK	CA's private key
CAPK	CA's public key
$E(.)$	Encryption function
$D(.)$	Decryption function

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

$\hat{e}$	Bilinear pairing
G1, G2	Additive group of a finite field
Gr	Multiplicative group of a finite filed
P1, P2	Points on the elliptic curve
a, b, c, u, v	Integers
H1, H2	Hash value generated by SHA256
q	Prime number

I. INTRODUCTION

Smart grid is considered as next generation power system. It performs real time monitoring, control and protection operations. In contrast to conventional power systems, smart grid allows bi-directional power flow in the grid. At the end user, customers participate in the grid through Advanced Metering Infrastructure (AMI) [1]. AMI enables automated collection of metering data. Smart meter (SM) plays a key role in AMI which communicates with Distributed System Operator (DSO) and performs a set of operations such as demand response, dynamic pricing and energy management [2], [3]. It also communicates with household equipment and collects Power Consumption Data (PCD) sends it to DSO. Secure communication among smart meter and DSO is very important. Compromising the communication may lead to several security attacks on the network such as side channel attacks, false data injection attack, Man-in-the-Middle (MITM) attack, Denial of Service attack, replay attack etc. [4]–[6]. Authors in [7], focused on securing the communication between AMI and household equipment in the Home Area Network (HAN) and discussed various attacks in HAN such as Impersonation, Man-In-The-Middle (MITM) attack, replay and desynchronization. The severity of attacks increases when PCD is sent to DSO through wide area network which hampers secure communication.

Authentication, data integrity, confidentiality, privacy, and availability are the security requirements for smart meter communication [8]. Authentication ensures that the communicating entities involved are legitimate. Data integrity ensures that data should not be tampered during data communication. Power consumption data reveals customers daily routines, availability at home. Confidentiality ensures that the data transmitted should not be legible. Privacy ensures that the identity of electricity users required to be safeguarded. Availability ensures the communication should be uninterrupted. Among the said security requirements, authentication is the primary one as its compromise leads to other security vulnerabilities. Many researchers focused on providing security at this front. Authors in [9], discussed the need for authenticating power reading signals to prevent impersonation attack and proposed the compressive sensing based statistical authentication technique using residual error of a received signal. Malicious devices may perform this kind of attacks due to wireless broadcast nature which may cause economic loss.

Many authentication techniques were studied in smart grid with respect to timing performances of cryptographic algorithms used in the mechanism to prevent the security attacks. A lightweight message authentication scheme is reported in [10]. The scheme establishes mutual authentication using TLS mechanism which results in sharing of a secret key. Based on the shared secret key, messages are authenticated using hash-based message authenticated code techniques. Authentication mechanism reported in [10] incurs more computational delay in the process of node authentication. The proposed certificate-based mechanism in TLS protocol is not suitable for resource constrained environment [11]. Authors in [12] described a key management protocol based on mutual authentication between smart meter and utility servers. However, the scheme resulted in increased overhead in the network. Authors in [13] proposed Merkle-tree based authentication in AMI to mitigate false injection attack and replay attack. But these techniques may not be suitable for smart meters with limited computing power and limited bandwidth.

Authors in [7] reported novel Identity (ID)-based key establishment authentication mechanism in AMI. ID-based authentication mechanism reduces the computational overhead by removing certificate-based mechanism. Furthermore, the overhead of managing certificates such as transmission and verification times is not present. Hence, assessment of ID-based authentication mechanism and key agreement protocol between SM and DSO becomes necessary. Different authors proposed key agreement protocol based on ID-based authentication. Author in [14] proposed ID-based key agreement protocol based on bilinear pairings. Authors in [15] encountered forward secrecy of the protocol and proposed SCK protocol. Efficient authentication and key management mechanisms in AMI is proposed in [16]. However, they did not evaluate the timing performances of their proposed schemes and do not present the comparative computational evaluation of authentication schemes. Authors in [17] presented computational time of their proposed scheme by implementing in a wireless sensor node MICAZ. More focus is given on key management instead of key agreement operation which is a crucial component in securing the communication.

In AMI, the SM are resource constrained in nature, hence computational burden of security mechanisms is very important. Further, the above works did not check the suitability of ID based authentication and key agreement protocol in resource constrained environment. To fill this knowledge gap, the present paper analyzes and evaluates the ID-based authentication and key agreement protocol by developing a test platform and compares it with traditional certificate-based authentication mechanism. A test-platform that is comprised of Raspberry PI terminal and a computer system is used to test the suitability of the authentication mechanism. Traditional certificate-based authentication mechanism in TLS protocol is implemented using OpenSSL library [18] and ID-based authentication and key agreement protocol is implemented using TinyEC python library [19]. ID-based authentication and key agreement protocol is realized using

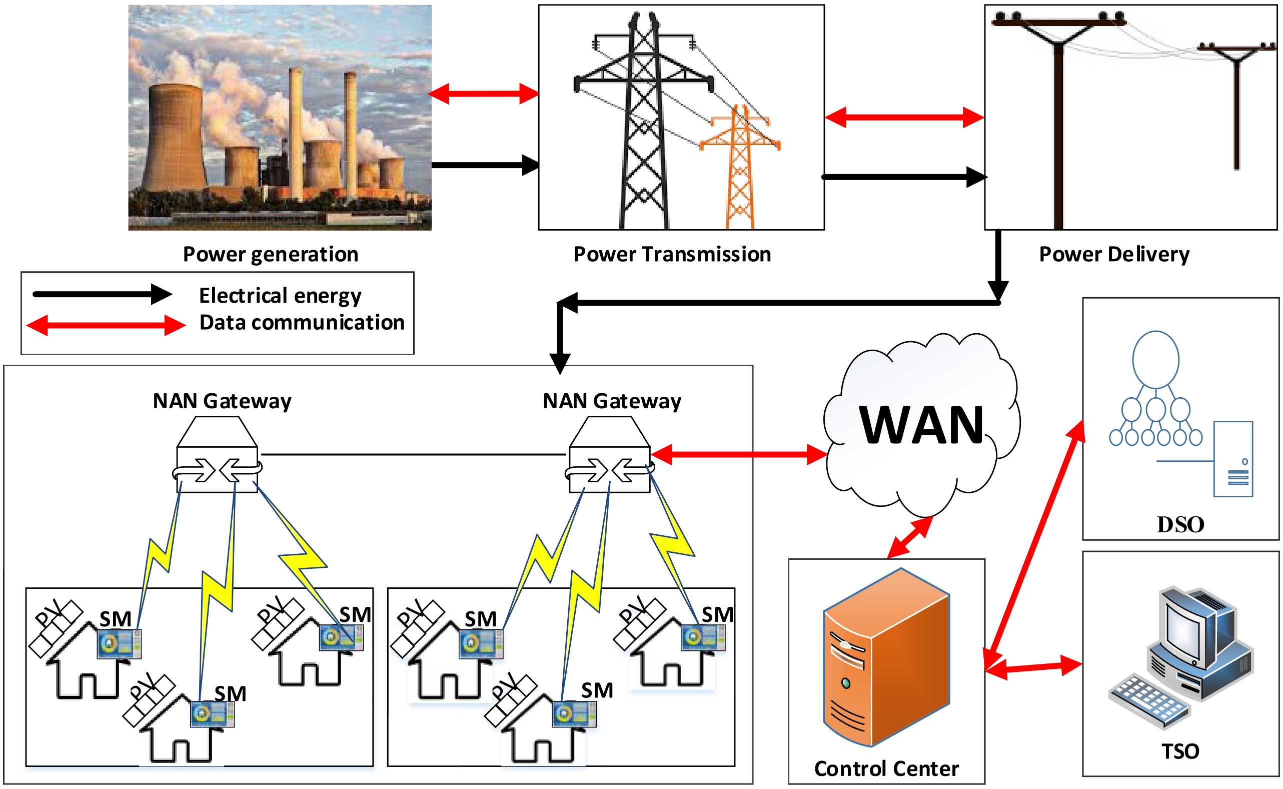

FIGURE 1. Smart grid and AMI infrastructure.

Elliptic Curve Cryptography (ECC). Computational times of vital operations in the considered authentication mechanism were captured. It is observed that ID-based authentication and key agreement protocol outperforms traditional certification-based authentication mechanism and well suitable for AMI environment.

The major contributions of the paper are as follows,

1) An ID based authentication mechanism and key agreement protocol is proposed and implemented.
2) Computational delays for the proposed mechanism are calculated by implementations on resource constraint platform.
3) Comparison of proposed authentication and key agreement mechanism with existing ID based and certificate-based mechanisms is presented.

The rest of the paper is organized as follows: Section II outlines on smart grid communication along with AMI and describes the major parties involved. Section III illustrates about the certificate-based authentication mechanism. Section IV explains about ID-based authentication mechanism and key agreement protocol. Section V gives the implementation details and discussion on the results. Finally, conclusions are presented in section VI.

II. SMART GRID AND ADVANCED METERING INFRASTRUCTURE (AMI)

Smart grid allows two-way communication between the grid entities for efficient operation of the grid. It manages different kinds of processes from generation to delivering to end-users. Electrical energy is generated from different sources and this bulk amount of energy is transmitted to distribution substations through transmission lines. Finally, energy is delivered to individuals through distribution substations. Transmission of energy is monitored by Transmission System Operator (TSO) and distribution of energy through substations are monitored by Distributed System Operator (DSO). Figure 1 shows the conceptual model of smart grid processes.

Smart grid also integrates Electric Vehicles (EVs) through Vehicle to Grid (V2G) communication [20]. It can also perform different tasks such as energy management, demand response and energy trading through AMI. AMI allows communication between smart meters and DSO for various operations related to energy transactions and management. Smart meter is connected to DSO through a hierarchical network structure which consists of Neighbourhood Area Network (NAN), Wide Area Network (WAN) and Control Center. Smart Meter collects PCD and send to DSO through the hierarchy. Multiple entities analyze data for real time grid monitoring and energy management. But this communication should be between the two legitimate entities, any security attack such as Man In The Middle (MITM), may lead to severe issues and economic loss.

Among the security requirements, authentication is an essential cornerstone in securing the communication [21]. Just compromising this requirement in AMI network is a gateway to a plethora of security attacks. Fig. 2 illustrates

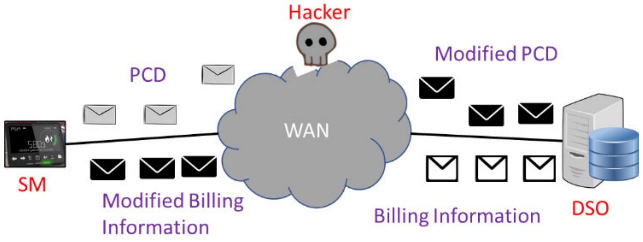

FIGURE 2. MITM attack between SM and DSO.

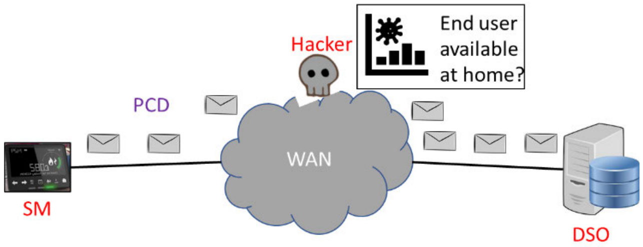

FIGURE 3. Attack on confidentiality to compromise privacy.

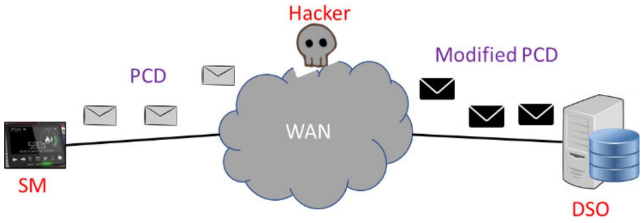

FIGURE 4. Data Integrity attack on SM-DSO communication.

MITM attack between SM and DSO while SM is sending PCD to DSO. After gaining credentials of both SM and DSO, a hacker in the network can modify messages sent between these two entities. Fig. 3 illustrates attack on confidentiality. Once a hacker is able to view the information, he can derive conclusions about the personal amount and time of household device use as well as the house owner's availability at home. This is definitely a privacy issue for to owner of the house. Fig. 4 illustrates a data integrity attack in AMI. Here, hacker is able to modify the PCD and send hacked data to DSO which may lead to false analysis results.

III. CERTIFICATE-BASED AUTHENTICATION SCHEME FOR SECURING COMMUNICATION IN AMI

Certificate based mechanism using Public Key Infrastructure (PKI) ensures authentication and eliminates many security attacks. A Certificate based on X.509 format [22] binds a communicating party's public key with its identity. Fig. 5 describes different fields of X.509 formats for SM and DSO. It is issued by a trusted third party called Certificate Authority (CA). CA also verifies the authenticity of certificates [23] and maintains revocation list which consists of invalid certificates.

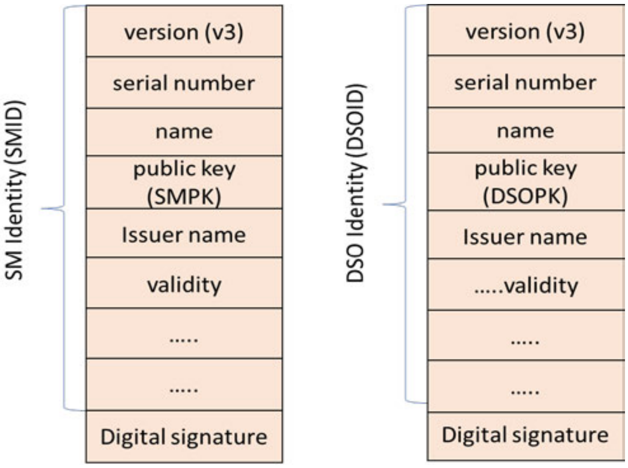

FIGURE 5. X.509 certificate formats of SM and DSO.

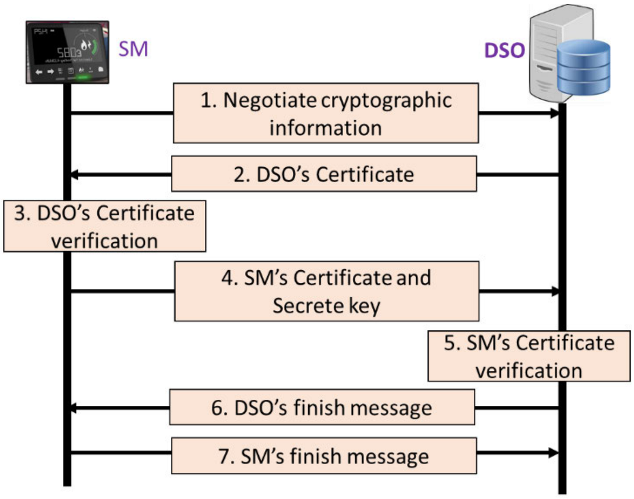
SM
DSO
1. Negotiate cryptographic information
2. DSO's Certificate
3. DSO's Certificate verification
4. SM's Certificate and Secrete key
5. SM's Certificate verification
6. DSO's finish message
7. SM's finish message

FIGURE 6. TLS Handshaking mechanism between SM and DSO.

Fig. 6 illustrates the mutual authentication process accomplished during Transport Layer Security (TLS) handshake mechanism to ensure end to end security. SM initiates communication by sending cryptographic information to DSO. Cryptographic information includes set of cipher-suites [24] to be supported by both parties in the subsequent communication. DSO selects a cipher-suite and send response which also includes its certificate. Certificate is in X.509 format as shown in Fig.6. DSO also sends certificate request which requires SM to send its own certificate in the next step. SM receives the response and verifies the DSO's certificate through Certificate Authority (CA). If the certificate is valid, then SM sends an encrypted secret key along with its certificate to DSO. DSO receives the secret key and verifies the validity of certificate through CA. Once the received SM's certificate is validated by CA, DSO sends the final message which includes encrypted secret key. Finally, SM acknowledges the DSO's final message.

The mechanisms of certificate signing, and verification are illustrated in Fig. 7 and Fig. 8, respectively. In Fig.4, SM send a Certificate Signing Request (CSR) to CA. CSR

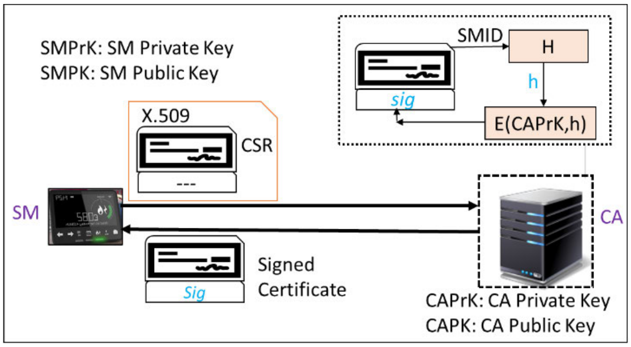

FIGURE 7. Certificate Signing mechanism of SM.

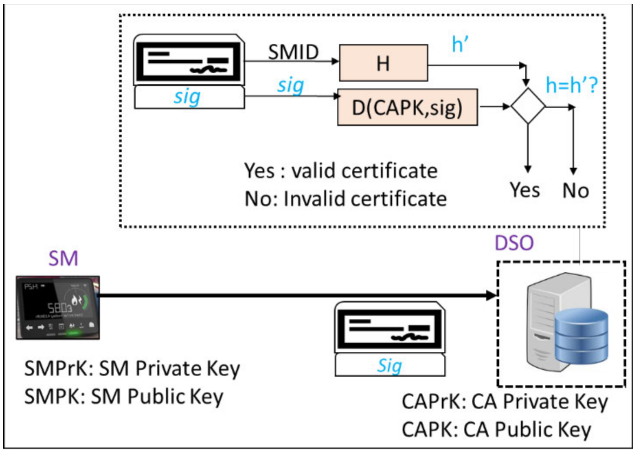

FIGURE 8. Certificate verification mechanism of SM by DSO.

consists of X.509 certificate which consists of different fields of identifying SM such as name, public key, Issuer name, validity of the certificate, digital signature field etc. The different X.509 certificate fields except digital signature field is treated as Identification fields as shown in Fig. 6. CA receives CSR and generates a digital signature (*sig*) by encrypting a hash value (*h*) with CA's private key *(CAPrK)* which is a result of hash function (H) that takes X.509 certificate fields (SMID) as input. X.509 certificate with added digital signature (*sig*) is called as signed certificate. The signed certificate is issued by CA to SM. The process of getting signed certificate for DSO is performed in a similar manner.

The verification of SM's certificate by DSO is done as shown in Figure 8. In step 4 of Fig.4, SM sends its singed certificate to DSO for verification. DSO generates a new hash value (h') by taking SMID as input using hash function (H). Further, it verifies the signed certificate by decrypting the digital signature (*sig*) using CA's Public Key (CAPK). The result value (*h*) of decryption is compared with *h'*. If both *h* and *h*' are same, then the signed certificate is valid, otherwise it is invalid. While this mechanism provides necessary security, it has many drawbacks such as increased computational and communication overhead, management of certificates and maintenance of a revocation list [23].

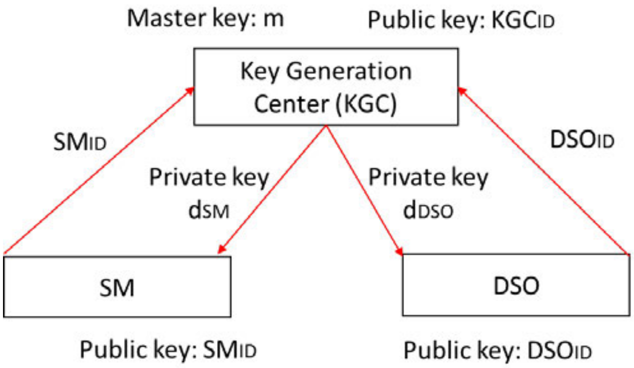

FIGURE 9. ID-based key generation through KGC.

IV. ID-BASED AUTHENTICATION SCHEME FOR SECURING COMMUNICATION IN AMI

To get rid of the pitfalls of certificate-based mechanism, ID-based authentication techniques are proposed in the literature [25]. In this approach, unlike its certificate-based counterpart, authentication between SM and DSO does not depend on trusted third party which generates valid certificates, performs verification of certificates, and maintains revocation information. Fig. 9 Illustrates the basic ID based key generation scheme discussed in [25].

In the ID-based authentication scheme, the management overhead of certificates is eliminated by a Key Generation Center (KGC). Public and private key pairs are not randomly generated by communicating devices. The Secret Key (SK) of a device is generated by KGC using its name or IP address as public key along with a master key (m) known only to KGC. Then, SK is securely transmitted to the communicating device. SMs have limited computing power; hence the generation of SK is delegated to KGC. KGC can be implemented either in DSO or as a third-party entity. Figure 9 shows secret key generation for SM and DSO by KGC. SM send its Identification (SM: {ID}) as its public key to KGC. Generally, IP address or SM name is taken as public key of SM. KGC computes corresponding secret key (d_{SM}) for SM. The same process is accomplished between DSO and KGC.

Private keys are computed by KGC not by SMs or devices with low computational capacities. If a communicating device like SM can compute its private key from corresponding public key, then it also be capable of generating private keys of other devices with their public keys. This reduces the security provided the ID based scheme. Therefore, only KGC can generate the secret key and it maintains privileged information that can be used to generate the secret keys of the devices. Once the secret keys are generated by KGC, different cryptographic operations such as encryption, decryption, signing and verification operations can be accomplished to achieve further security requirements such as confidentiality and Integrity.

For example, to achieve message integrity, SM sends PCD by signing with its secret key (SMSK) and encrypts the result by using the public key (DSOID) of DSO. SM sends the encrypted message to DSO by incorporating its own Identity Information (SMID). After receiving the message, DSO decrypts the message using secret key (DSOSK). The decrypted message is verified by the public key (SMID) of SM.

The security of the ID-based mechanism depends on the underlying cryptographic algorithms used in key generation, signing, verification, encryption, and decryption operations. Furthermore, it also depends on privileged information (m) being kept by KGC. The security of the proposed ID-based authentication depends on the intractability of finding master key (m) when a hacker is able to get the key pairs ($\mathrm{SM_{ID}}$, $\mathrm{d_{SM}}$) or ($\mathrm{DSO_{ID}}$, $\mathrm{d_{DSO}}$). Unfortunately, RSA based authentication is not suitable for ID-based mechanism [26]. Elliptic Curve Cryptography proved to be efficient with respect to providing more security than RSA [26].

ID based authentication is based on elliptic curve cryptography with bilinear pairing operations. Bilinear map on elliptic curve is defined as follows,

Bilinear Map: A pairing is a bilinear map $\hat{e} : G_1 \times G_2 \to G_r$ between three given groups $\mathrm{G}_{1,}$ G_2 and G_r of exponent q. Paring has three properties such as Bilinear, Non-degenerate and Computable.

- Bilinear: $\forall\,(P_1, P_2) \in G_1 \times G_2, \forall\,(a, b) \in Z_q^* \times Z_q^*$, we have a bilinear pairing which is a map $\hat{e}\,(aP_1, bP_2) = e(P_1, P_2)^{ab}$.
- Non-degenerate: There exist non-trivial points $P_1 \in G_1, P_2 \in G_2$ both of order of q such that $\hat{e}\,(P_1, P_2) \neq 1$.
- Computable: $\hat{e}$ can be efficiently computable.

By the above features, Bilinear Diffie-Hellman problem in the space of $(G_1, G_2, \hat{e})$ is defined as follows:

Input parameters: $(aP_1, bP_1, cP_1)\,, a, b, c \in Z_q^*, Output : \hat{e}(P_1, P_1)^{abc}$.

Once, ID-based authentication is accomplished through KGC, key agreement between the communicating parties is essential to establish secure communication. Key agreement based on elliptic curve cryptography and Bilinear Diffie-Hellman play key role in exchange of shared key securely among SM and DSO.

A. ID-BASED AUTHENTICATION KEY AGREEMENT PROTOCOL

The proposed ID-based authentication key agreement protocol has three phases: 1) Setup, 2) Key generation and 3) Key agreement.

Among the three phases, master key of KGC and cryptographic hash functions are chosen in setup phase. Private keys of corresponding public keys of the devices are computed in key generation phase. Finally, in the last phase, key agreement among SM and DSO is accomplished.

B. SETUP PHASE

An elliptic curve is defined in finite field F_p. Let group of points E[q] of order q on elliptic curve. Then generate a set of pairing parameters of required size. Select a random value m $\in Z_q^*$ as the master key and compute $R = mP_2$. Select two cryptographic hash functions H_1, H_2 where $H_1 = \{0, 1\}^* \to G_1$; and $H_2 = \{0, 1\}^* \times \{0, 1\}^* \times G_2 \times G_2 \times G_r \to \{0, 1\}^*$;

C. KEY GENERATION PHASE

KGC keeps this master key m as privileged information and publicize other parameters. For SM, KGC generates public key and private key pairs using its Identity ($\mathrm{SM_{ID}}$). Public Key of SM is $P_{SM} = H_1\,(SM_{ID})$ and Private Key of SM is $d_{SM} = mP_{SM}$. The same process of generating public and private keys for DSO is as follows. Public Key of DSO is $P_{DSO} = H_1\,(DSO_{ID})$ and Private Key of DSO is $d_{DSO} = mP_{DSO}$.

D. KEY AGREEMENT PHASE

SM and DSO select u, v randomly from Z_q^* and perform the following steps. In step1, SM computes and sends $E_{SM} = uP_2$ to DSO. DSO computes and sends $E_{DSO} = vP_2$. In step2, SM and DSO computes common key as follows,

SM computes K such that,

$K = \hat{e}\,(uP_{DSO}, R)\,.e(d_{SM}, E_{DSO}), uE_{DSO} = uvP_2;$

DSO computes K such that,

$K = \hat{e}\,(uP_{SM}, R)\,.e(d_{DSO}, E_{SM}), vE_{SM} = uvP_2.$

Finally, in step 3, the session key

$SK = H_2(SM_{ID}, DSO_{ID}, E_{SM}, E_{DSO}, uvP_2, K).$

The first two phases are called as authentication phase and the third phase is key agreement phase. Fig. 10 illustrates the above phases.

V. IMPLEMENTATION RESULTS

In order to evaluate the performances of certificate based authentication scheme and the proposed ID based authentication and key agreement scheme, a realistic scenario of SM and DSO communication over a WAN is considered. The SM and DSO communication in this scenario is adopted from [3]. Figure 11 illustrate the communication between SM and DSO through WAN. It consists of SM connected to household devices such as roof top Photo Voltaic (PV), home appliances etc. SM communicates the measured data to DSO in IEC 61850 format.

A testbed for realizing the above discussed SM and DSO communication is set up. Fig. 11 Illustrates the test-setup with two devices: 1) computer with Intel® Core (TM) i5-3210M CPU @ 2.50 GHz with 8 GB RAM and 2) Raspberry PI 4 Model B terminal with 4GB RAM. Where computer terminal emulates DSO system and Raspberry PI emulates SM. For simplicity, KGC module is also simulated in computer system along with DSO. It can also be implemented in a separate terminal.

A. PERFORMANCE EVALUATION OF CERTIFICATE BASED AUTHENTICATION

Certificate-based authentication mechanism described in section III is implemented using OpenSSL libraries [18]. As first step, the SM obtains a signed certificate form CA. Using OpenSSL libraries the a CSR for SM is generated and

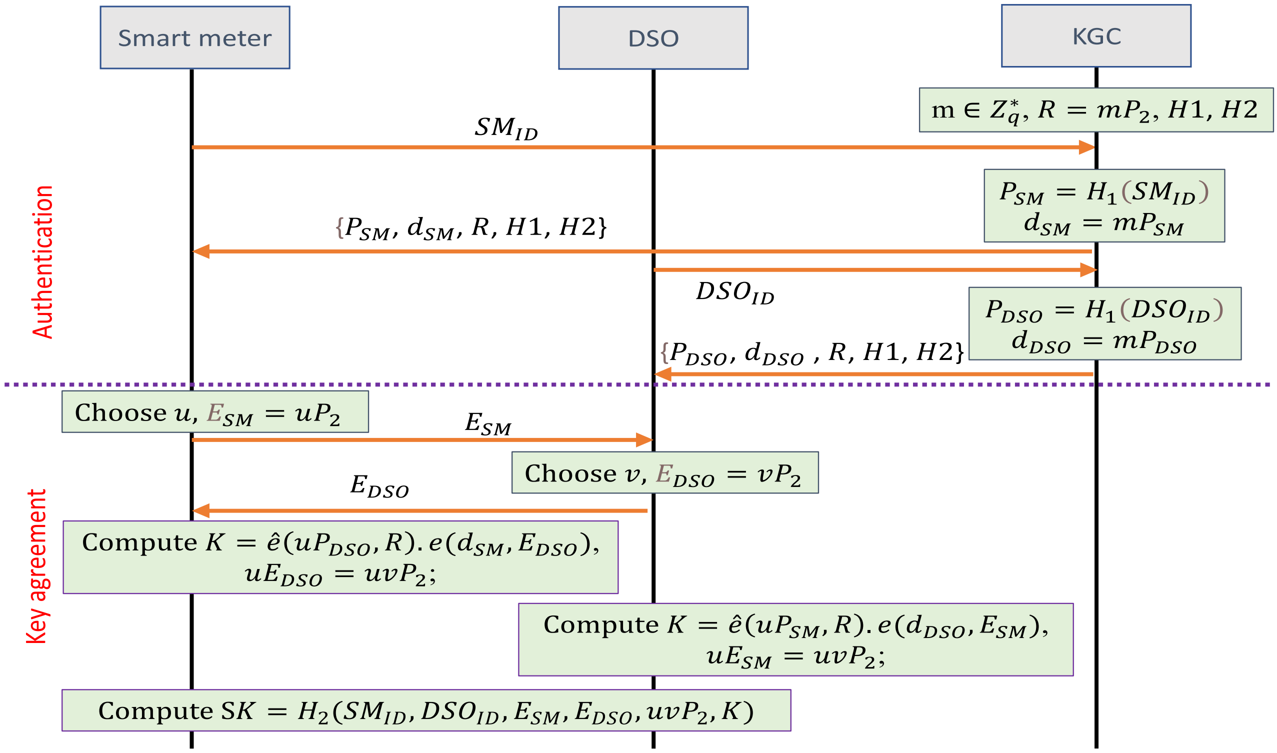
Smart meter
DSO
KGC
Authentication
$m \in Z_q^*,\ R = mP_2,\ H1,\ H2$
SM_{ID}
$P_{SM} = H_1(SM_{ID})$
$d_{SM} = mP_{SM}$
$\{P_{SM}, d_{SM}, R, H1, H2\}$
DSO_{ID}
$P_{DSO} = H_1(DSO_{ID})$
$d_{DSO} = mP_{DSO}$
$\{P_{DSO}, d_{DSO}, R, H1, H2\}$
Key agreement
Choose u, $E_{SM} = uP_2$
E_{SM}
Choose v, $E_{DSO} = vP_2$
E_{DSO}
Compute $K = \hat{e}(uP_{DSO}, R).e(d_{SM}, E_{DSO})$, $uE_{DSO} = uvP_2$;
Compute $K = \hat{e}(uP_{SM}, R).e(d_{DSO}, E_{SM})$, $uE_{SM} = uvP_2$;
Compute SK $= H_2(SM_{ID}, DSO_{ID}, E_{SM}, E_{DSO}, uvP_2, K)$

FIGURE 10. ID based authentication and Key agreement protocol.

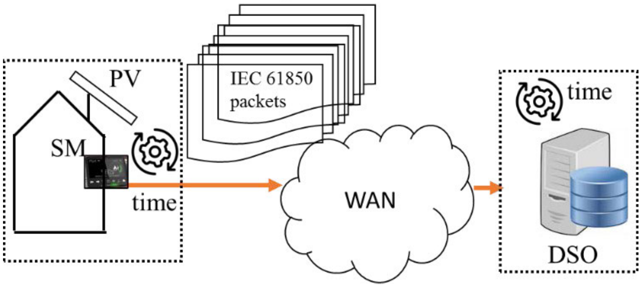

FIGURE 11. SM and DSO communication through WAN.

TABLE 1. Computational times for certificate-based authentication mechanism.

Algorithm	Key size / Curve	CSR Size (bytes)	Certificate Size (bytes)
RSA	1024	745	1029
	2048	1045	1241
ECDSA	secp224r1	485	700
	Secp192r1	426	656
	secp384r1	590	782
	secp521r1	696	883
	prime256v1	509	700

TABLE 2. Computational times for certificate-based authentication mechanism.

Type of Encryption		Certificate verification computational time (ms)	
Algorithm	**Key size / Curve**	**DSO module**	**SM module**
RSA	1024	22	35
	2048	27	43
ECDSA	secp224r1	20	28
	Secp192r1	18	26
	secp384r1	25	33
	secp521r1	27	36
	prime256v1	20	29

sent to CA. The CA returns a signed certificate generated by RSA or ECDSA algorithms. Table 1 lists the different CSR and certificate sizes obtained for different RSA and ECDSA algorithms using the OpenSSL implementations. To perform mutual authentication and share a session key between SM and DSO, a TLS handshake communication is established. In TLS handshake communication, each certificate is verified using the credentials of CA as shown in Fig. 8.

Computational times for certificate verification at both devices were calculated for RSA based certificates with 1024 and 2048 key sizes and ECDSA based certificates with different NIST-defined elliptic curves such as 'secp224r1', 'secp256k1', 'secp384r1',' secp521r1' and prime256v1 which were listed in TABLE 2.

It is observed that ECDSA based certificates with different NIST defined curves outperforms RSA based certificates. Among the all the curves "secp224r1" gives least computational time on Raspberry PI device emulating SM. On the other hand, "Secp192r1" provides the best results for DSO emulated by the laptop terminal.

TABLE 3. Computational times for ID-based authentication and key agreement mechanism.

Type of Encryption		Computational time (ms)
Algorithm	Curve	
Key generation by KGC	secp192r1	8
	secp224r1	10
Point Multiplication in key agreement	-	7
Computation of K using bilinear pairing	-	6
Hash function to generate SK	-	2
Total time for the curves secp192r1/secp224r1		23/25

B. PERFORMANCE EVALUATION OF ID BASED AUTHENTICATION AND KEY AGREEMENT MECHANISM

The proposed ID-based mechanism is implemented using 'tinyec' python library in PyPI [19]. Tinyec library functions enable to write code on arithmetic operations on elliptic curves. It has two major functions curve() and point() which describes an elliptic curve on a finite field and point belongs to elliptic curve respectively. A random integer value is picked up as m value to generate public key and private key pairs of SM and DSO using their Identity information (SM_{ID}, DSO_{ID}). Both public and private keys are generated by KGC and send to SM and DSO. Computation times obtained for generating key pairs for elliptic curves secp192r1 and secp224r1 are 8 ms and 10 ms respectively. Further, KGC also generates a common value R using point multiplication operation with prevailed information m and shares only to communicating parties. Common value R play crucial role in generating a shared key SK which further used to generate session key K. SM initially sends E_{SM} value to DSO and DSO responds with $E_{DSO.}$ Using the 'tinyec' library, the E_{SM} and E_{DSO} were computed in 7 ms by employing the point multiplication operation over elliptic curve. In next step, SM generates a shared key using its private key, public key of DSO, R value and invitation value of DSO. This leads to bilinear mapping operation which was computed in 6 ms. Finally, a session key is generated by applying hash function on public parameters of both SM and DSO along with shared key (SK) which resulted in 2 ms computational time.

Using time function in python time module computational times for each operation in ID-based authentication and key agreement protocol are captured and listed in Table 3. All these operations are performed by KGC and not by individual terminals such as SM. Various key operations mentioned in the table are key generation by KGC, point multiplication in key agreement, computation of K value using bilinear pairing and hash function to generate SK value. Total time of authentication and key agreement is 23ms for the curve secp192r1.

Table 5 shows the comparison of computational times of different authentication and key agreement protocols in the literature with the proposed ID based authentication and key agreement protocol. From the Table 4 it is observed that proposed authentication and key agreement protocol has relatively very low computational burden.

TABLE 4. Comparison of computational times of different schemes.

	[17]	[17]	Proposed
Hardware Platform	MICAZ	MICAZ	Raspberry PI
Scheme name	SKM	SKM^+	-
Computational time	7.35s	7.77s	0.023s

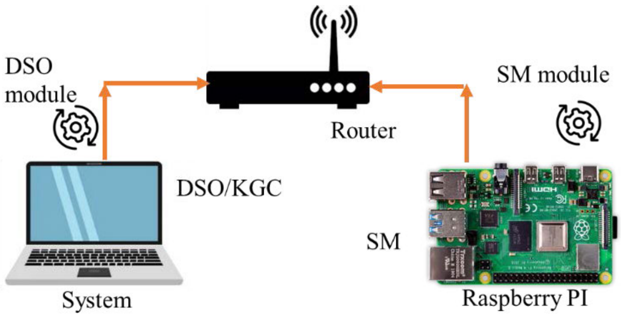

FIGURE 12. Testbed to evaluate certificate based and ID-based authentication mechanisms.

TABLE 5. Computational times for encryption and decryption.

Algorithm	Encryption time (ms)	Decryption time (ms)
AES 128	0.025	0.027
AES 256	0.03	0.031

When compared with certificate-based mechanism, computational times of ID-based authentication and key agreement are far better. This fact makes ID-based scheme more suitable for securing the communication between SM and DSO. Once the key agreement is established, the PCD is encrypted using AES 128 and AES 256 encryption algorithms. The size of PCD data is considered from [3] and performed encryption and decryption operations using AES function in python PyCrypto module. Table 5 gives the computational times for encryption and decryption algorithms on Raspberry PI terminal using AES 128 and AES 256 symmetric algorithm. For both mechanisms discussed, i.e. certificate-based and ID-based, these values are identical. As it can be observed, the values are on the order of microseconds and well within the computational capacity of a SM.

VI. CONCLUSION

Smart grid network is the next generation power system. It enables real time monitoring, control, and protection in the electrical infrastructure. Introduction of DERs necessitates two-way communication between the system operate and the end users. AMI network plays a crucial role at consumer side that enables many applications like demand response, power consumption billing and energy market trading. Security is of utmost importance in AMI networks compromising which may lead to several attacks such as Impersonation, Data Integrity and Replay. Authentication and key agreement play key role in eliminating the attacks. This paper analyzes two authentication mechanisms for their suitability in AMI: certificate and ID-based mechanism. Furthermore, a test bed has been developed and these mechanisms have been implemented in separate terminals. After experiments, computational times have been noted. It is observed that ID-based authentication and key agreement mechanism is far better than heavy loaded certificate-based mechanism. The key advantage of the ID-based mechanism is that heavy computations are performed with in KGC and not in individual terminals. This is especially beneficial for SMs which have very limited computation capacity.

REFERENCES

[1] V. Namboodiri, V. Aravinthan, S. N. Mohapatra, B. Karimi, and W. Jewell, "Toward a secure wireless-based home area network for metering in smart grids," *IEEE Syst. J.*, vol. 8, no. 2, pp. 509–520, Jun. 2014.

[2] S. M. S. Hussain, S. M. Farooq, and T. S. Ustun, "Implementation of blockchain technology for energy trading with smart meters," in *Proc. Innov. Power Adv. Comput. Technol. (I-PACT)*, Vellore, India, Mar. 2019, pp. 1–5.

[3] S. M. S. Hussain, A. Tak, T. S. Ustun, and I. Ali, "Communication modeling of solar home system and smart meter in smart grids," *IEEE Access*, vol. 6, pp. 16985–16996, 2018.

[4] A. S. Sani, D. Yuan, W. Bao, and Z. Y. Dong, "A universally composable key exchange protocol for advanced metering infrastructure in the energy Internet," *IEEE Trans. Ind. Informat.*, vol. 17, no. 1, pp. 534–546, Jan. 2021.

[5] T. S. Ustun, S. M. Farooq, and S. M. S. Hussain, "A novel approach for mitigation of replay and masquerade attacks in smartgrids using IEC 61850 standard," *IEEE Access*, vol. 7, pp. 156044–156053, 2019.

[6] X. Liu, P. Zhu, Y. Zhang, and K. Chen, "A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2435–2443, Sep. 2015, doi: 10.1109/TSG.2015.2418280.

[7] A. Mohammadali, M. S. Haghighi, M. H. Tadayon, and A. Mohammadi-Nodooshan, "A novel identity-based key establishment method for advanced metering infrastructure in smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2834–2842, Jul. 2018, doi: 10.1109/TSG.2016.2620939.

[8] S. M. Farooq, S. M. S. Hussain, and T. S. Ustun, "Elliptic curve digital signature algorithm (ECDSA) certificate based authentication scheme for advanced metering infrastructure," in *Proc. Innov. Power Adv. Comput. Technol. (I-PACT)*, Vellore, India, Mar. 2019, pp. 1–6.

[9] Y. Lee, E. Hwang, and J. Choi, "A unified approach for compression and authentication of smart meter reading in AMI," *IEEE Access*, vol. 7, pp. 34383–34394, 2019.

[10] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675–685, Dec. 2011.

[11] M. Suárez-Albela, T. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "A practical evaluation of a high-security energy-efficient gateway for IoT fog computing applications," *Sensors*, vol. 17, no. 9, p. 1978, 2017.

[12] H. Nicanfar, P. Jokar, and V. C. M. Leung, "Smart grid authentication and key management for unicast and multicast communications," in *Proc. IEEE PES Innov. Smart Grid Technol.*, Perth, WA, Australia, Nov. 2011, pp. 1–8.

[13] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An efficient Merkle-tree-based authentication scheme for smart grid," *IEEE Syst. J.*, vol. 8, no. 2, pp. 655–663, Jun. 2014.

[14] N. P. Smart, "An ID-based authenticated key agreement protocol based on the Weil pairing," *Electron. Lett.*, vol. 38, no. 13, pp. 630–632, 2002.

[15] L. Chen and C. Kudla, "Identity based authenticated key agreement from pairings," in *Proc. IEEE Comput. Secur. Found. Workshop*, 2003, pp. 219–233.

[16] H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, "Efficient authentication and key management mechanisms for smart grid communications," *IEEE Syst. J.*, vol. 8, no. 2, pp. 629–640, Jun. 2014.

[17] Z. Wan, G. Wang, Y. Yang, and S. Shi, "SKM: Scalable key management for advanced metering infrastructure in smart grids," *IEEE Trans. Ind. Electron.*, vol. 61, no. 12, pp. 7055–7066, Dec. 2014.

[18] I. Ristic, *Bullet Proof SSL and TLS*, London, U.K.: Feisty Duck, 2014.

[19] *Python Tinyec Library*. Accessed: Nov. 20, 2020. [Online]. Available: https://pypi.org/project/tinyec/

[20] P. Nsonga, S. M. S. Hussain, I. Ali, and T. S. Ustun, "Using IEC 61850 and IEEE WAVE standards in ad-hoc networks for electric vehicle charging management," in *Proc. IEEE Online Conf. Green Commun. (OnlineGreenComm)*, Piscataway, NJ, USA, Nov. 2016, pp. 39–44.

[21] S. M. Farooq, S. M. S. Hussain, and T. S. Ustun, "Survey of authentication techniques in vehicular ad-hoc networks (VANETs)," *IEEE Intell. Transp. Syst. Mag.*, early access, May 12, 2020, doi: 10.1109/MITS.2020.2985024.

[22] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, document RFC 5280, 2008. [Online]. Available: https://www.rfc-editor.org/info/rfc5280

[23] S. Farooq, S. Hussain, S. Kiran, and T. Ustun, "Certificate based authentication mechanism for PMU communication networks based on IEC 61850-90-5," *Electronics*, vol. 7, no. 12, p. 370, Dec. 2018.

[24] T. Dierks and E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.2*, document RFC 5246, Aug. 2008.

[25] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*. Berlin, Germany: Springer, 1984, pp. 47–53.

[26] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.

[27] *AVISPA-Automated Validation of Internet Security Protocols*. Accessed: Nov. 20, 2020. [Online]. Available: http://www.avispa-project.org

[28] A. Molina-Markham, G. Danezisy, K. Fu, P. Shenoy, and D. Irwin, "Designing privacy-preserving smart meters with low-cost microcontrollers," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, Kralendijk, Bonaire, Mar. 2012, pp. 239–253.

SHAIK MULLAPATHI FAROOQ (Senior Member, IEEE) received the B.Tech. degree in information technology and the M.Tech. degree in computer science from Jawaharlal Nehru Technological University, Hyderabad, India, and the Ph.D. degree in computer science and engineering from Yogi Vemana University, Kadapa, India, in 2020. He was a Visiting Researcher with the Fukushima Renewable Energy Institute, AIST (FREA), Japan, in 2018. He is currently an Assistant Professor with the Department of Computer Science and Engineering, Madanapalle Institute of Technology and Sciences, Madanapalle, India. His research interests include cryptography, cyber physical systems, cybersecurity in vehicular networks, and power systems. He is a member of IE, India.

S. M. SUHAIL HUSSAIN (Member, IEEE) received the Ph.D. degree in electrical engineering from Jamia Millia Islamia (Central University), New Delhi, India, in 2018.

He is currently an AIST Postdoctoral Researcher with the Fukushima Renewable Energy Institute, AIST (FREA), Koriyama, Japan. His research interests include power system communication, cybersecurity in power systems, substation automation systems, IEC 61850 standards, electric vehicle integration, and smart grid. He was a recipient of the IEEE Standards Education Grant from the IEEE Standards Education Committee for implementing project and submitting a student application article from 2014 to 2015. He serves as the Guest Editor for the IEEE Transactions on Industrial Informatics.

TAHA SELIM USTUN (Member, IEEE) received the Ph.D. degree in electrical engineering from Victoria University, Melbourne, VIC, Australia.

He was an Assistant Professor of electrical engineering with the School of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA, USA. He is currently a Researcher with the Fukushima Renewable Energy Institute, AIST (FREA), and leads the Smart Grid Cybersecurity Laboratory. He has edited several books and special issues with international publishing houses. He has taken active roles in organizing international conferences and chairing sessions. He has been invited to run specialist courses in Africa, India, and China. He has delivered talks with the Qatar Foundation, the World Energy Council, the Waterloo Global Science Initiative, and the European Union Energy Initiative (EUEI). His research interests include power systems protection, communication in power networks, distributed generation, microgrids, electric vehicle integration, and cybersecurity in smartgrids. He is a member of the IEEE 2800 Working Groups and the IEC Renewable Energy Management Working Group Eight. He serves as an Associate Editor for IEEE Access and a Guest Editor for the IEEE Transactions on Industrial Informatics. He also serves as a Reviewer for reputable journals.

ATIF IQBAL (Senior Member, IEEE) received the B.Sc. degree (Hons.) and the M.Sc. degree in engineering (power system and drives) from Aligarh Muslim University (AMU), Aligarh, India, in 1991 and 1996, respectively, the Ph.D. degree from Liverpool John Moores University, Liverpool, U.K., in 2006, and the D.Sc. (Habilitation) degree in control, informatics and electrical engineering from the Gdansk University of Technology, in 2019. He has been a Lecturer with the Department of Electrical Engineering, AMU, since 1991, where he was a Full Professor, in August 2016. He is currently a Full Professor with the Department of Electrical Engineering, Qatar University, and a Former Full Professor with the Department of Electrical Engineering, AMU. He has published widely in International journals and conferences. He has authored/coauthored more than 420 research articles, four books, and several chapters in edited books. He has supervised several large-research and development projects worth more than multimillion USD. He has supervised and co-supervised several Ph.D. students. His research interests include power electronics, variable speed drives, renewable energy sources, smart grid, complex energy transition, active distribution networks, electric vehicles drivetrain, sustainable development and energy security, distributed energy generation, and multiphase motor drive systems. He is a Fellow of IET, U.K., and IE, India. He was a recipient of the Maulana Tufail Ahmad Gold Medal for the B.Sc.Engg. degree (electrical) from AMU in 1991. He was also a recipient of the Outstanding Faculty Merit Award from 2014 to 2015 and the Research Excellence Awards from Qatar University, Doha, Qatar, in 2015 and 2019. He received several best research papers awards, such as the IEEE ICIT in 2013, IET-SEISCON in 2013, SIGMA in 2018, the IEEE CENCON in 2019, the IEEE ICIOT in 2020, and Springer ICRP in 2020. He serves as the Vice-Chair for the IEEE Qatar Section. He serves as an Associate Editor for the IEEE Transactions on Industrial Electronics and IEEE Access. He also serves as the Editor-in-Chief for *I'manager Journal of Electrical Engineering*, a Former Associate Editor for the IEEE Transactions on Industry Application, and a Former Guest Associate Editor for the IEEE Transactions on Power Electronics.

• • •