An Anonymous Identity-based With Bilateral Protocol for Smart Grid

Jennifer Batamuliza[1] and Damien Hanyurwimfura[2]
[1]College of Business and Economics, University of Rwanda, Rwanda
[2]College of Science and Technology, University of Rwanda, Rwanda

Abstract: *Smart Grid (SG) is a modern digital metering system that was introduced by researchers to take over the traditional electricity infrastructure that existed before by gathering and putting in use the data generated by smart meters and ensure efficiency and reliability in the two directional flow of electricity and data for both the service providers and smart meters. Leakage of customers' identity causes inconvenience to the customer because he is exposed to theft in his household. Secure anonymous key distribution scheme for SG has been proposed as solution to secure data transfer between service provider and customer. Existing secure anonymous key distribution scheme for SG brings challenge such as being inefficient, having traceability issues and do not stop replay attack hence vulnerable to DoS attacks. In this paper a Secure efficient anonymous identity-based with bilateral protocol is proposed to address the weakness in existing anonymous key distribution schemes. , With this protocol, both smart meter and service provider in (SG) identify each other anonymously in efficient way achieving un-traceability and restisting Replay and DoS attack.*

Keywords: *Identity-based, anonymous, bilateral protocol, smart grid, smart meters*.

Received February 20, 2021; accepted March 7, 2021
https://doi.org/10.34028/iajit/18/3A/6

1. Introduction

Smart Grid (SG) is a new electricity management and distribution system technology that is being adopted by many countries replacing the old system that was used in the distribution and management of electricity. It is a two ways digital technology where electricity and information flow are transmitted at the same time. SG uses devices called smart meters which are installed at the home or office recording real time electricity usage and after it sends the information in a real time manner to the service provider for billing purpose. Smart meter gathers information of power usage in a building in a real time manner and then sends information to the service provider who is responsible for power distribution. With development of smart cities, smart grids have been adopted and used to enhance the way people are living. This smart city is made up of smart and very intelligent systems and infrastructures for example using smart traffic system, smart hospitals, smart parking (ways of parking system to avoid misusing of space by different car owners or drivers) and smart grid infrastructure [10].

Advanced metering architecture is a technology, which is used for collection, measurement, analyzing and storing of data from devices through a sensors smart meter enabled.

This technology is a combination of software, hardware, and communication networks and consumers devices. Advanced Metering Infrastructure (AMI) gathers energy data usage from the smart meter and later forwards the data to a utility firm and also provides communication link between the two for remote management. Remote management is load balancing, remotely connecting and disconnecting power, and smart meter updates. The data collected from smart meters can be used in many ways like helping the consumer to know how much electricity used by different devices or appliances at home hence putting him in a position of cutting his bills, should there be any need to do so, it could be for billing purpose, load forecasting and outage management. This can also detect theft of electricity which happens in most cases, Anomalous Reading and Meter Status to prevent revenue. Demand response is a signal sent by AMI controller end to make some changes or updating of smart meter Information [18]. Moreover, Service providers are able to coordinate announcements, policies, reports, bills, and rates with the consumers who are the owners of the smart meters. The consumer also checks and keeps monitoring their energy consumption patterns. To avoid condition of most annoying black out of power generation station failure AMI controller can shut off smart meter [26]. It also encourages the use of power in off peak time to avoid high costs that is incurred during peak hours [1]. In an AMI, there are many smart meters, depending on the scale of the smart grid system. Those smart meters collect information about how power is consumed and send them to the service provider for billing and for data analytics for prediction of future energy consumption [9]. The new technology helps the user

spend efficiently on power, as he/she is able to know which devices consume more and which devices consume less electricity [2]. With this new technology, blackouts are also avoided [11].

Smart grid not only comes with benefits into this modern power industry, but also risks as well as complexity for protecting the smart grid systems from different security threats. As smart grid becomes reality, security threats are also increasing rapidly.

Some schemes have been proposed to deal with security issues mostly found in smarts grids but some security issues have not well addressed.

This paper is an extension of the paper by Batamuliza and Hanyurwimfura [4] which proposed a certificateless signcryption for key distribution scheme and allows for both decryption and verification by authorized users and provide Key Generation Center to only partial key. In this paper, we propose an anonymity in identity-based with bilateral protocol to ensure un-traceability and Replay and DoS attack resilience that was not available in the previously proposed protocol.

Other existing protocols are generally not good for smart grid deployment because of insecurity [12, 16, 23].

User anonymity is applied to conceal clients' information. Badly, the smart meter has less processing power hence big computations cannot be handled [8, 20] hence authenticated key management scheme. The Mutual authentication was used in a way that both user and service providers can easily authenticate one another mutually. Computation of a session key is to be used by both client and service provider as they exchange information. Private Key cryptography is used to allow both client and service provider to use the same key. Unfortunately, if the key is discovered all communication will be in clear. A Public Key Infrastructure is a system that supports [13] the deployment of asymmetric cryptography. It manages certificates to produce trust in public keys. Registration Authority (RA) checks whether the entity possesses matching private key and public key. Afterwards the Certification Authority (CA) gives certificates by giving signatures attaching public keys and their owners. The above scheme isn't good because management of certificates needs a lot of space. An identity based public key cryptosystem [15] in which the Public keys are computed from the system identities such as an e-mail address was proposed. Private keys are given to users by a trusted authority with a master key afterwards the user encrypts without consulting any directory and without looking a certificate. Recently Elliptic curve cryptography has been adopted over RSA [7, 17] because of its advantages over RSA and Discrete Logarithm Problem (DLP). Its security depends on the elliptic curve logarithm problem. The Elliptic curve has small key and small computation cost [6]. The small key will be used in smart meter efficiently because smart meters have small processing chip. Balode *et al.* [3] proposed optimized identity-based encryption from Bilinear Pairing.

All existing schemes are limited on traceability that can allow the theft of the transmitted data between service provider and the customer. This paper introduces an anonymous identity based with bilateral protocol to provide un-traceability and ensure resilience to Replay and DoS attack in the smart grid.

2. Related Works

A key management scheme [6] for SG was proposed. This scheme combines both symmetric key and elliptic curve asymmetric. The main specific objectives of their schemes were to introduce scalability, strong service, fault tolerance, accessibility plus efficiency. Xia and Wang [25] discovered vulnerability against man-in-the-middle attacks in that scheme proposed by Binbin and Hontgu [5]. Thwe and Htet [22] proposed a key distribution protocol that overcomes man-in-the-middle attacks and also reduce the cost in performing certificate verification from Public Key cryptography. It was discovered that the scheme proposed by Xia and Wang [25] was not resistant to impersonation attack and unknown key share. Their scheme also do not support smart meter anonymity that is needed by smart meters and service servers to achieve privacy. Xia and Wang proposed [25], an identity- based and authenticated key agreement protocols following many identity- based key agreement protocols that have been proposed all of which didn't seem secure. Wang *et al.* [24] used an effective way to construct pairing-friendly elliptic curves with low hamming weight 4 under embedding degree 1. This scheme based on the analysis of the complex multiplication. This scheme do not have anonymity which is a way of securing smart meter by hiding its identity as the smart meter authenticates itself to the service provider. Zaho *et al.* [27] proposed a password protected smart card scheme which is a remote authentication between client and remote server that is used for protection against card reader impersonation without the smart card later. Diffie-Hellman protocol [21] also has been used but all these proposed schemes do not consider anonymity. They all don't put into consideration anonymity which is very critical especially during information exchange between both parties. Tsai and Lo [23] proposed a scheme for secure communication to be achieved between smart meter and service provider. Tsai and Lo [23] brought the idea of anonymity after surveying a number of proposed schemes and finding that all these schemes do not achieve privacy needed because of lack of anonymity. Therefore they proposed a scheme that introduced anonymity for the first time. They used identity- based signature scheme and identity based encryption scheme for the key distribution scheme. A smart meter can anonymously access service provided

by the service provider without the help of a trusted anchor in the authentication session using one private key.

2.1. Proposed Paper Contribution

Existing secure anonymous key distribution scheme for (SG) brings challenge such as being inefficient, having traceability issues and do not stop replay attack hence vulnerable to DoS attacks. In this paper, we incorporate the Secure efficient anonymous identity-based with bilateral protocol to allow both smart meter and service provider in (SG) identify each other anonymously in order to provide efficiency and, achieve un-traceability and ensure Replay and DoS attack resilience.

3. Preliminaries

3.1. Notations

Elliptic Curve Computational Diffie-Hellman Problem (EC-CDH) Let G_p be an ECC group of order p, where p is a prime; the point P is the generator of G_p. The elliptic curve computational Diffie-Hellman problem in G_p: Given a random instance $(P,aP,bP) \in G_p$, compute abP. The CDH problem in G is to compute the element abP. Table 1 gives the notations and descriptions.

Table 1. Notations and descriptions.

Notations	Descriptions
SM	Smart Meter
SP	Service Provider
PKG	Public Key Generator
ECC	Elliptic Curve Cryptography
DHP	Diffie-Hellman Problem
PKI	Public Key Infrastructure
DoS	Denial of service
CA	Certificate Authority
CDH	Computational Diffie-Hellman Assumption
F_p	A prime Finite Field
E/F_P	The elliptic Curve Over F_p

3.2. System Model

- The proposed system model consists of three types of entities: the Public Key Generator (PKG), the Service provider (SP), and the Smart Meter (SM) as shown in Figure 1.
- Four steps are involved in the proposed system model such as: Initialization, Registration, Authentication and lastly Service. All these steps are described below to show how the three entities interact with one another following the above steps.
  - *Smart meter*: all smart meter clients are supposed to be preloaded with public parameters inside them (initialization) and are registered with the PKG before they can access the electricity services provided by SP.
  - *Service provider*: Utility companies are service providers for the smart meter users and they also need to be preloaded with public parameters (initialized) and registered (Registration) with the PKG before they serve as Service Providers (SPs) to offer electricity and energy services in general remotely to smart meter clients.
  - *Public key generator*: PKG is in charge of the registration of both smart meters and service providers. In general, PKG is assumed to be a commercial organization instead of a fully trusted third party. To derive the commercial benefits, it is very likely for the PKG to illegally collect a client's personal information by impersonating the SP or access the service offered by SPs free of charge by impersonating the legitimate smart meter client.
- The smart meter client can authenticate anonymously itself to the service provider and they can start communicating independently without involving PKG and without PKG knowing their shared key then service provider authenticates itself anonymously to the smart meter. Hence meaning that there is mutual authentication of the two entities. Services can then be provided.

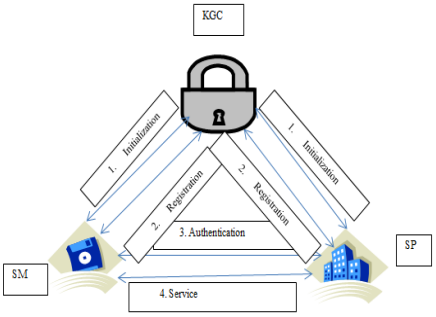

Figure 1. System model for anonymous identity based protocol.

3.3. Secure Efficient Anonymous Identity-Based with Bilateral Protocol

The main contribution of this paper is that with the Secure efficient anonymous identity-based with bilateral, both smart meter and service provider in Smart Grid both Identify each other anonymously unlike previous protocols where only one hides its identity.

3.3.1. Bilinear Pairings

Below we define those properties of bilinear. Let us assume that G_1 be an additive cyclic group, G_2 be a multiplicative cyclic group, and P be a generator of G_1, where G_1 and G_2 have the prime order q.
The bilinear pairing equation e: $G_1 \times G_1 \rightarrow G_2$ satisfies the following properties.

1. Bilinear: Given $P_1, P_2, Q_1, Q_2 \in G_1$, $e(P_1 + P_2, Q_1) = e(P_1, Q_1)e(P_2, Q_1)$, and $e(P_1, Q_1 + Q_2) = e(P_1, Q_1)e(P_1, Q_2)$.
2. Besides, given $a, b \in Z_q$, $e(aP, bQ) = e(abP, Q) = e(P,abQ)=e(P,Q)ab=e(bP,aQ)$.

Non degenerate: There exists $P \in G_1$ and $Q \in G_1$ such that $e(P, Q) = 1$, where 1 is the identity element of G_2.

3. Computable: For any $P, Q \in G_1$, the value $e(P, Q)$ is efficiently computed.

3.3.2. System Components

This protocol focuses on secure communication between smart meters and service providers in a smart grid. Hence, there are three roles in our scheme:

1. A trust anchor.
2. Service providers SP.
3. A smart meter SM.

A smart meter will be in charge of gathering the data from a house using the sensors that are installed in the house then after the sensors will send the gathered data to the service provider. A service provider will monitor the electricity usage and later send information about consumption to the user or owner of the smart meter in a real time manner. In our scheme, we have the trusted third party that is responsible for distributing the private keys of both the service provider and the smart meter when registration is taking place and then keeps the private keys in a tamper proof module and thus prevents it from leaking to hackers who may use it to break the security of the scheme.

3.3.3. Proposed Scheme

We show the proposed scheme in this section. The proposed scheme is divided into three phases:

1. *System Setup*: let us assume that G_1 be an additive cyclic group, G_2 be a multiplicative cyclic group, and P be a generator of G_1, where G_1 and G_2 have the prime order q.

The PKG chooses a bilinear pairing map e: $G_1 \times G_1 \rightarrow G_2$ satisfies the following properties. PKG first chooses master key $x \in_R Z^*_p$ and computes master public key $P_{Pub} = x \cdot P$ and computes g=e(p, p) After that, PKG chooses five secure hash functions as follows:

H_1:$\{0,1\}^* \times G \rightarrow Z^*_p$,
H_2: $\{0, 1\}^* \times G \times \{0, 1\}^* \rightarrow Z^*_p$,
H_3: $\{0, 1\}^* \times G^5 \rightarrow Z^*_p$,
H_4: $\{0, 1\}^* \times G^5 \rightarrow \{0, 1\}^*$,
H_5: $\{0, 1\}^* \times G^4 \times \{0, 1\}^* \rightarrow Z^*_p$.

PKG publishes the system parameters $\{G_1, G_2, P, e, H, H_1, H_2, H_3, H_4, q, P_{\text{pub}}, g\}$ and keeps the master key x secretly.

2. *Extraction*: there are two types of extractions that will be needed:
    1. *Smart Meter Extraction*: whenever a smart meter SM is willing to do registration with the trusted third party, it will send its identity ID to that trusted third party through a very protected and secured channel. After the trusted third party receives the ID from that smart meter it will compute the private key D= $(1/x+ q) P$ for that SM, whereby $q=H_1$(ID) will be the corresponding public key for that SM. After, the trust third party will send D and $\{G_1, G_2, P, e, H, H_1, H_2, H_3, H_4, q, P_{\text{pub}}, g\}$ to that SM through a very protective and secured channel. After getting D and $\{G_1, G_2, P, e, H, H_1, H_2, H_3, H_4, q, P_{\text{pub}}, g\}$ from that trusted third party, that SM will store them in a very secured tamper proof module to avoid from being hacked by hackers or the man in the middle attack.
    2. *Service Provider Extraction*: the service provider SP should also send its identity SID to that same trusted third party. That trusted third party will utilize the SP's identity SID and its own master private key s to calculate the master private key of the SP where K= (1/ x + h) P and h= H1(SID) is the matching public key of SP. Afterwards, that trusted third party will send K and {G1, G2, P, e, H, H1, H2, H3, H4, q, Ppub, g} to the SP through a secured channel. The SP will calculate H1(SID)P + Ppub, and keep {G1, G2, P, e, H, H1, H2, H3, H4, q, Ppub, g}, K, and H1(SID)P +Ppub in its tamper-proof module after receiving K and {G1, G2, P, e, H, H1, H2, H3, H4, q, Ppub, g} from the trusted third party.
3. *Authentication*: in this step, SM and SP will mutually authenticate each other without the help from the trusted third party. The SM and SP will do the below steps.

This also describes the protocol for smart grid anonymous key agreement based on the ID-based. In a smart grid anonymous key agreement protocol, the initiator has a smart meter and similarly the service provider hides.

1. *SM* chooses $U \in_R$ G and computes $h = H_0(U, SP)$
2. *SP* then picks $V \in_R$ G, computes $c = H_0(V, SM)$.
3. *A* chooses $r' \in R$ Z^*_q, computes $U = r' Q_{SM} - (U + h Q_{SM})$.
4. Similarly, *SP* chooses $r' \in_R Z^*_q$, computes $V = r' Q_{SP} (V + c Q_{SP})$.
5. *SM* and *SP* exchange $S \in U$ and $S \in V$
6. *SM* and *SP* compute session key sk_{SM} and sk_{SP}.

$$sk_{SM} = K(e((r' + h)S_{SM}, (V + c Q_{SP})))$$
$$= K((r'Q_{SM} + h Q_{SM}, (V + c Q_{SP}))^s)$$
$$= K(e(u+(u + h Q_{SM}) + h Q_{SM}, (V + c Q_{SP})^s))$$
$$= K(e((u + h Q_{SM}) + h Q_{SM}, (V + c Q_{SP})^s))$$
$$= K(e((u + h Q_{SM}) + h Q_{SM}, V + (V + c Q_{SP})^s)) + c Q_{SP})^s)$$
$$= K(e((u + h Q_{SM}), (r' + c)S_{SP}))$$
$$= K(e((u + h Q_{SM}) + h Q_{SM}, r' Q_{SP} + c Q_{SP})^s) = sk_{SP}$$

3.4. System Analysis

Besides the conventional security properties for key agreement protocols, the security of smart grid anonymous key agreement protocol also depends on anonymity as shown. These properties are found in the security requirements of the key agreement protocol.

1. Validity: this means that if there are two uncorrupted oracles complete matching sessions then both oracles should hold the same session key.
2. Indistinguishability: In particular, this implies authenticity.
3. Anonymity. Smart grid anonymous key agreement protocol has unconditional anonymity if Smart meter is unable to identify the real initiator better than a random guess.

If the protocol satisfies bilateral privacy, the same requirement applies on the responding party.

It is straightforward to see that our proposed protocol is valid.

3.5. Security Strength

Anonymity in the proposed protocol means that except for the requesting smart meter client and the requested service provider, any outsider (including the PKG) is unable to link a particular protocol session to a particular identity. Smart meter authenticates itself to a requested Service provider and that service provider authenticates itself to the client at the same time and both parties are assured of the others' identity.

- *Proof*: the security of the proposed protocol is defined by two security games between the challenger CH and an adversary A1 or A2 respectively.

To capture the attack launched by the outside adversary, A1 is simulated as the attacker who can replace the public key of any entity in the system, but cannot access the PKG's master secret key. To catch the attack mounted by the malicious PKG, A2 is assumed to be an attacker who has the ability to access the master-key with the restriction that any user's public key cannot be replaced by A2.

4. Performance Evaluation

The proposed scheme has 2 pairing, one pairing at smart meter side and one at service provider side yet each pairings computation time is 20.01ms hence total computation time becoming 40.02ms but our scheme is still more cost effective compared to the existing protocol like Kabalci [11] which has 4 pairings. The proposed scheme doesn't have man in the middle attack too.

4.1. Comparison with Previous Protocols

The proposed protocol was compared with three existing works that solve similar problem in terms of efficiency, computation cost, mutual authentication, anonymity, etc., Table 2 below shows the comparison among the three protocols. In addition to security features available to those existing protocols, the proposed scheme add two more features such un-traceability and resilience on Replay and DoS attack, which is an indication of the improvement and the contribution of the previous proposed protocols.

Table 2. Comparison with previous protocols.

Security features	Xia and Wang [25]	Tsai and Lo [23]	Batamuliza and Hanyurwimfura [4]	The proposed identity-based scheme
Mutual Authentication	No	Yes	Yes	Yes
Anonymity	No	Yes	Yes	Yes
Pairing Costs	No	Yes	No	Yes
Man-In-The-Middle-Attack	No	Yes	No	No
Un-traceability	No	No	No	Yes
Replay and DoS attack resilience	No	No	No	Yes

Anonymity is found in both [4] and our new scheme, thus smart meter can anonymously authenticate itself to the service provider hence Smart Meter information is kept as a secret. Unlike Xia and Wang scheme [25] which has no anonymity. The new proposed scheme and previous scheme [4] both have mutual authentication thus they can authenticate each other.

In term of computation cost in authentication phase, we assume that T_{mp} is the time to perform one multiplication point operation, T_m is the time to perform one multiplication operation, T_p is the time to perform one bilinear pairing operation, T_e is the time to perform one modular exponentiation operation, T_s is the time to perform one symmetric encryption/decryption operation, T_{cert} is the time to perform a certificate generation operation, $T_{cert-ver}$ is the time to perform a certificate verification operation and T_H is the time to perform a Map-To-Point operation.

Table 3. Comparison on computation cost in authentication phase.

Protocol	Smart Meter	Service Provider	KGC
Xia and Wang [25]	T_s+4T_h	$4T_h$	T_s
Tsai and Lo [23]	$4T_{mp}+T_e+5T_h$	$4T_p + 3T_{mp} + T_e+5T_h$	0 T_s
Batamuliza and Hanyurwimfura [4]	$4T_{mp} + T_m$	$7T_{mp}$	0
The proposed identity-based scheme	$T_{mp} + T_m$	$2T_{mp+} T_p$	T_p

In these schemes, running time of the operations is got from the use of MIRACL. Windows xp operating system equipped with PIV3-GHz processor and 512 M bytes memory. The proposed ECC- based protocol use Koblitz elliptic curve y2 = x3+ax+b mod p with a, b ∈ FP. Running time of the involved cryptographic operations on AP and client are listed in Table 4 below. The proposed scheme consumes less time compared to other 2 as Such as in [23] at service provider 4 pairings are needed therefore (4×20.01) = 80.02ms is needed which is big also exponential is needed at the service provider side whose time is 11.20 as shown in Table 4 below whereas in our scheme at smart meter and service provider side we have no exponential and we only have two pairings one on smart meter and one on service provider hence the cost is not very high compared to others. In the scheme of Xia and Wang [25], a smart meter identity is forwarded to the Key generation Center; hence, the scheme doesn't have anonymity hence vulnerable to certain attacks and does not support perfect forward secrecy. Our scheme has only 2 pairings. Additionally, in smart meter side exponential in Fp2 l. Therefore our scheme is better because of less computation time at smart meter side and less computation cost. Our scheme also has anonymity. We conclude that our scheme is better than the three schemes hence suitable.

Table 4. Cryptographic operation time in milliseconds.

Operations	Time
ECC-based scalar multiplication	0.83
Exponential in F_p^2	11.20
Pairing - based scalar multiplication	6.38
Pairing	20.01

5. Conclusions

An anonymous identity-based with bilateral protocol for smart grid is proposed and solved the problem of traceability and replay and DoS attack. With this new protocol, both smart meter and service provider in Smart Grid identify each other anonymously in efficiecient way, achieving un-traceability and restisting on Replay and DoS attacks that was missing in the previous protocol. Comparing with other existing scheme solving similar problem in terms of security and computation cost, the proposed scheme is more efficient and secure, it offers less computation time at smart meter side and less computation cost as well.

Acknowledgment

I would like to thank African Center of Excellence Data Science a project supported by World Bank for sponsoring this work.

References

[1] Aalamifar F. and Lampe L., "Cost-Efficient Qos-Aware Data Acquisition Point Placement for Advanced Metering Infrastructure," *IEEE Transactions on Communications*, vol. 66, no. 12, pp. 6260-6274, 2018.

[2] Baimel D., Tapuchi S., and Baimel N., "Smart Grid Communication Technologies- Overview, Research Challenges and Opportunities," *in Proceedings of International Symposium on Power Electronics, Electrical Drives, Automation and Motion, SPEEDAM*, Capri, pp. 116-120, 2016.

[3] Balode N., Gade S., Shinde M., and Kore K., "Optimized Identity-Based Encryption from Bilinear Pairing," *International Journal of Advance Scientific Research and Engineering Trends*, vol. 3, no. 3, pp. 2456-0774, 2018.

[4] Batamuliza J. and Hanyurwimfura D., "A Secure and Efficient Anonymous Certificateless Signcryption for Key Distribution Scheme for Smart Grid," *in Proceedings of the 21st International Arab Conference on Information Technology*, 6 of October, pp. 1-7, 2020.

[5] Binbin Y. and Hongtu L., "Anonymous Authentication Key Agreement Scheme with Pairing-Based Cryptography for Home-Based Multi-Sensor Internet of Things," *International Journal of Distributed Sensor Networks*, vol. 15, no. 9, 2019.

[6] Debiao H., Huaqun W., Muhammad K., and Lina W., "Lightweight Anonymous Key Distribution Scheme for Smart Grid Using Elliptic Curve Cryptography," *IET Communications*, vol. 10, no. 14, pp. 1795-1802, 2016.

[7] Erfaneh V., Majid B., Mohammad R., and Mohammad R., "A Secure ECC-Based Privacy Preserving Data Aggregation Scheme for Smart Grids," *Computer Networks*, vol. 129, pp. 28-36, 2017.

[8] Gungor V., "Smart Grid Technologies: Communication Technologies and Standards," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 4, pp. 529-539, 2011.

[9] Gungor V., "Smart Grid Technologies: Communication Technologies and Standards," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 4, pp. 529-539, 2011.

[10] Jin J., Gubbi J., Marusic S., and Palaniswami M., "An Information Framework for Creating A Smart City Through Internet of Things," *IEEE Internet Things Journal*, vol. 1, no. 2, pp. 112-121, 2014.

[11] Kabalci Y., "A Survey on Smart Metering and Smart Grid Communication," *Renewable and Sustainable Energy Reviews*, vol. 57, pp. 302-318, 2016.

[12] Kamto J., Qian L., Fuller J., and Attia J., "Light-Weight Key Distribution and Management for Advanced Metering Infrastructure," *in Proceedings of IEEE GLOBECOM Workshops*, Houston, pp. 1216-1220, 2011.

[13] Karuppiah M., Das K., Li X., Kumari S., Wu F., Chaudhry S., and Niranchana R., "Secure Remote User Mutual Authentication Scheme with Key Agreement for Cloud Environment," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 1-17, 2018.

[14] Lanjun D., Jie X., Xuefei C., Hui L., Jie C., Yueyu Z., and Xiaotong F., "Efficient Identity-Based Authenticated Key Agreement Protocol With Provable Security for Vehicular Ad Hoc Networks," *International Journal of Distributed Sensor Networks*, vol. 14, no. 4, pp. 1-14, 2018.

[15] Li Q., Hsu C., Choo K., and He D., "A Provably Secure and Lightweight Identity-Based Two-Party Authenticated Key Agreement Protocol for Vehicular Ad Hoc Networks," *Security and Communication Networks*, 2019.

[16] Liu N., Chen., Zhu L., Zhang J., and He Y., "A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid," *Transactions on Industrial Electronics*, vol. 60, no. 10, pp. 4746-4756, 2013.

[17] Mahmood K., Shehzad A., Husnain N., Saru K., Xiong L., and Arun K., "An Elliptic Curve Cryptography Based Lightweight Authentication Scheme for Smart Grid Communication," *Future Generation Computer Systems*, vol. 81, pp. 557-565, 2017.

[18] McHenry M. and Mark P., "Technical and Governance Considerations for Advanced Metering Infrastructure/Smart Meters: Technology, Security, Uncertainty, Costs, Benefits, and Risks." *Energy Policy*, vol. 59, pp. 834-842, 2013.

[19] Mona M., Sahar G., and Magdy N., "Privacy-Preserving for Distributed Data Streams: Towards l-Diversity" *The International Arab Journal of Information Technology*, vol. 17, no. 1, pp. 52-64, 2020.

[20] Preeti C., Ankita S., and Rifaqat A., "Cryptanalysis and Improvement of a Secure Mutual Authentication Scheme for Remote Users," *International Conference on Electrical, Computer and Communication Technologies*, Coimbatore, pp. 1-9, 2019.

[21] Singhal A., "Diffie Hellman Key Exchange" https://www.gatevidyalay.com/diffie-hellman-key-exchange-asymmetric-encryption, Last Visited, 2021.

[22] Thwe P. and Htet M., "Prevention of Man-In-The-Middle Attack in Diffie-Hellman Key Exchange Algorithm using Proposed Hash Function," *International Journal of Advances in Scientific Research and Engineering*, vol. 5, no. 10, 2019.

[23] Tsai L. and Lo W., "Secure Anonymous Key Distribution Scheme for Smart Grid," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 906-914, 2016.

[24] Wang M., Dai G., Choo K, Jayaraman P., and Ranjan R., "Constructing Pairing-Friendly Elliptic Curves under Embedding Degree 1 for Securing Critical Infrastructures," *Plos*, vol. 11, no. 8, 2016.

[25] Xia J. and Wang Y., "Secure key distribution for the smart grid," *IEEE Transactions Smart Grid*, vol. 3, no. 3, pp. 1437-1443, 2012.

[26] Yang Z., Ping S., Sun H., and Aghvami H., "Crb-Rpl: A Receiver-Based Routing Protocol for Communications in Cognitive Radio Enabled Smart Grid," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 7, pp. 5985-5994, 2017.

[27] Zhao Y., Li S., and Jiang L., "Secure and Efficient User Authentication Scheme Based on Password and Smart Card for Multi server Environment," *Security and Communication Networks*, pp. 1-13, 2018.

Jennifer Batamuliza received her Bachelor degree of Engineering in Computer Engineering and Information Technology from University of Rwanda (Former KIST) in 2012. She received her Master degree of Engineering in Computer Science and Technology from the University of Electronic Science and Technology of China, China in 2016. She is a lecturer at Adventist University of Central Africa (AUCA) in Information Technology faculty and she is the associate director of research and consultancy at Adventist University of Central Africa (AUCA). She is currently Pursuing PhD in Data science in Data mining. Her research interest includes cryptographic protocols, Data mining, Machine learning, cloud computing and network security.

Damien Hanyurwimfura received his Bachelor degree of Engineering in Computer Engineering and Information Technology from University of Rwanda (Former KIST) in 2005. He obtained his Master degree of Engineering in Computer Science and Technology and Ph.D. degree in Computer Science and Technology from Hunan University, China in 2010 and 2015 respectively. He is currently working as the Acting Director and Head of PhD Studies and Research at the African Center of Excellence in Internet of Things (ACEIoT), College of Science and Technology, University of Rwanda. He has been selected to participate in Postdoctoral Researchers' Networking Tour 2018 organized by DAAD, Germany on the theme: Artificial Intelligence Coming of Age – Research and Development in Germany, September 23rd to 29th 2018. He is a member of Rwanda Academy of Sciences (RAS), Rwanda China Alumni Organization (RCAO) and University of Rwanda Alumni. He is a Technical Program Committee member for many international peer reviewed conferences. He has published and co-authored more than 25 research papers in leading international journals and conferences. His research interests covers most aspect of data mining, machine learning, Computer security, watermarking, Internet of Things, hate speech detection and recommender systems.