Privacy Preserving Multi Factor Authentication Protocol for Next Generation Grids Deployed in Smart Cities

Osama Ahmed and Hiroshi Kamabe

Gifu University, Gifu City, Japan
osama.ahmed.v2@s.gifu-u.ac.jp, kamabe.hiroshi.m8@f.gifu-u.ac.jp

Abstract

The Internet of Things (IoT) plays a pivotal role in addressing critical challenges, such as enhancing reliability and power quality, within the framework of the next-generation grid environment. It also contributes significantly to the implementation of next generation grid initiatives in the context of smart city development. In this environment, secure access to services by automated meters from service providers through public channels is imperative. However, such public channel communication exposes vulnerabilities that adversaries can exploit. In recent times, numerous researchers have undertaken diverse research endeavors to identify and address the most pressing issues associated with the next-generation grid. Fundamental security prerequisites encompass crucial aspects of security analysis, specifically adhering to the CIA principles, which encompass confidentiality, integrity, and authentication. The development of lightweight security protocols is unique due to the presence of resource-constrained objects, like automated meters, within the next-generation grid. As a result, we present a lightweight multi factor authentication scheme that is designed to enhance the security of automated meters in the infrastructure of the next-generation grid. The protocol we have proposed undergoes a comprehensive analysis to assess its robustness against established security threats. Ultimately, we conduct a thorough performance evaluation to showcase its efficacy and suitability for real-world implementation.

Keywords: Multi Factor Authentication, Next Generation Grids, SHA256, Random Oracle Model(ROM)

1 Introduction

The Internet of Things (IoT) is an infrastructure that connects a variety of objects to one another via the Internet. The establishment of connections between these objects and other sources enables seamless data gathering and information transfer, depending on specific requirements. In the realm of IoT, objects fall into two categories: physical and virtual.

Physical objects, like smart phones, digital cameras, sensors, drones, and automobiles, are utilized for data collection. In contrast, virtual objects have the responsibility of managing and controlling information, like electronic tickets and digital wallets. These IoT devices possess a degree of intelligence that allows them to make autonomous decisions, reducing the need for human intervention.

One of the key advantages of IoT, is its ability to establish secure connections between computer-based systems and real-world physical systems, even when they are located remotely. This integration process not only proves to be cost-effective but also enhances data accuracy by reducing human involvement to a minimum level while ensuring data integrity and confidentiality.

The 7th International Conference on Mobile Internet Security (MobiSec'23), Dec. 19-21, 2023, Okinawa, JAPAN, Article No. 57

The smartness of a city is attained through the seamless integration of diverse IoT devices with various service-oriented information systems, all while upholding robust authentication protocols. To transform a city into a smart city, it is crucial to establish secure and seamless information sharing between its residents and these service-oriented information systems, employing advanced cryptographic authentication methods. Additionally, the success of smart cities relies heavily on the implementation of next-generation grids, which must incorporate encryption and authentication mechanisms to ensure the efficient and secure delivery of electricity supply.

Next-generation grids not only enhance efficiency but also create opportunities for energy conservation. Moreover, they make it possible to efficiently coordinate between the city's control center and other infrastructure domain operators, which is crucial for maintaining public safety and overall well-being.

In this cutting edge Next-Generation grid ecosystem, each premises is equipped with an automated meter, providing end users and utility companies with exceptionally accurate data concerning electricity consumption[1]. Moreover, in this framework, a data collector facilitates automated meter interfaces for all energy-consuming devices within households.

Despite the use of power line communication for wired connections, the prevailing method for data collection and transmission within a Next-Generation grid architecture is wireless communication. To facilitate this, every automated meter includes a short-range wireless interface at its diagnostics port, allowing for seamless access to digital meter readers and real-time diagnostic tools.

Although power line communication is utilized for wired connections, the predominant method for data collection and transmission is wireless communication, which constitutes the standard mode of communication within a Next-Generation grid architecture. [2]. The diagnostics port of every automated meter has a short-range wireless interface, making it easy to access digital meter readers and diagnostic tools in real-time.

Furthermore, within a designated neighborhood, each automated meter transmits its data especially electricity usage readings to a "home area network (HAN) gateway," which serves as a consolidation point for the transmitted readings. Subsequently, this aggregated data is forwarded to a designated "premise area network (PAN) portal," under the management of the utility company. Here, "Advanced Metering Infrastructure (AMI) head-end" server assumes a crucial role by collecting and securely storing data from automated meters prior to its integration into the official network. Various methods are at hand to organize this data effectively before its extraction and utilization.

In the architectural framework of the Next Generation Grid, multiple entities convey information through a shared public communication channel [3]. Consequently, as the channel is shared and public so it is now prone to numerous type of security threats. Authentication and key agreement are recognized as indispensable security services to safeguard the integrity and confidentiality of the Next Generation Grid environment.

In recent years, there has been an introduction of numerous authentication and key agreement protocols within the field of cryptography. However, many of these protocols come with a substantial computational overhead, rendering them impractical for entities with constrained resources. Additionally, the majority of the proposed solutions exhibit deficiencies in essential security features. These shortcomings include inadequate anonymity preservation, susceptibility to privileged-insider attacks, vulnerability to man-in-the-middle attacks, exposure to impersonation attacks, and limited protection against replay attacks. Subsequently, Multi-Factor Authentication (MFA) emerged as a solution to elevate security measures and enable the continuous protection of computing devices and critical services against unauthorized access[4].

MFA achieves this by incorporating more than two categories of credentials. Predominantly, MFA relies on biometrics, encompassing the automated recognition of individuals based on their behavioral and biological characteristics. This advancement substantially enhances security, as it necessitates users to furnish evidence of their identity through the presentation of two or more distinct factors[5].

These identified limitations and concerns have motivated our research efforts towards the development of a novel multi factor authentication scheme. This scheme not only offers resilience against physical attacks but also addresses the security vulnerabilities and constraints present in existing Next Generation Grid authentication protocols. Consequently, our contributions encompass the introduction of an effective mutual authentication methodology tailored to keep an eye on automated meters within the Next Generation Grid infrastructure.

1. We have developed a three factor authentication scheme for automated meters and service providers, placing particular emphasis on providing a comprehensive description of the system setup and the adversarial model.

2. Subsequently, we have devised a lightweight authentication mechanism that leverages elementary cryptographic operations, including bitwise exclusive-OR (XOR) and one-way cryptographic hash functions.

3. The protocol we propose guarantees the security of session keys and demonstrates strong resilience against both active and passive adversaries.

4. A thorough security analysis confirms that the presented scheme has been enhanced with additional security features.

5. When compared to similar techniques, the presented scheme necessitates considerably lower costs for communication and processing.

2 Related Work

In recent years, numerous security solutions have emerged for securing the next-generation grid infrastructure. Mahmood et al. introduced an authentication scheme tailored to the Next Generation Grid environment [6]. This protocol primarily focuses on authenticating Home Area Network (HAN), which includes both Building Area Network and Smart Meter. Although, it is imperative to note that the protocol presented in [6] lacks robust security measures and is susceptible to impersonation attacks. Additionally, it does not ensure user anonymity. Li et al. introduced the concept of a Public-Key Infrastructure (PKI) to formulate an authentication system [7]. Similarly, Wazid et al. designed an efficient and lightweight authentication scheme for smart grid applications based on Elliptic Curve Cryptography (ECC) [8]. In contrast, Mahmood et al. proposed an ECC-based authentication scheme for smart grids, yet it lacks critical security features, such as protection against insider attacks, resistance to password guessing attacks, and the assurance of user anonymity [9].

Abbasinezhad-Mood and Nikooghadam introduced an ECC-based authentication protocol that facilitates the establishment of a session key between smart meters and service providers for secure communication [10]. Notably, this protocol has the advantage of eliminating the need for certificate overhead management. However, it has shortcomings in ensuring the privacy of smart meters and preventing replay attacks. Moreover, it lacks support for the inclusion of new smart meters after the initial deployment.

Considering the diverse range of security schemes that have been developed for Internet of Medical Things (IoMT) [11] and vehicular cloud computing [12], these advancements have served as a catalyst for us to formulate a security protocol customized for the smart grid environment.

Likewise, Fouda et al. introduced an Authentication Key Agreement (AKA) protocol specifically designed for smart meters [13]. Their claim is that this protocol enables secure session key establishment for smart meters and smart equipment in each session.

Similarly, Wu and Zhou have devised a key management mechanism tailored to enhance the security of communication between data collectors and smart meters [2]. Subsequently, Xia and Wang [14] identified limitations in Wu and Zhou's scheme [2] and introduced an improved version that employs a trusted mediator for the establishment of session keys between service providers and smart meters.

In response to the demands of a smart grid environment, Chaudhary et al. outlined an Elliptic Curve Cryptography (ECC)-based key agreement authentication system [15]. Nevertheless, it is crucial to highlight that this scheme is vulnerable to device-capturing attacks [15].

Additionally, Bera et al. introduced an authentication scheme for smart grid infrastructure that incorporates ECC and hash-based techniques [16]. However, the protocol described in [16] falls short in guaranteeing the anonymity of smart meters and is susceptible to desynchronization attacks.

In related work, Abbasinezhad and colleagues [10, 17] presented an authentication method for key agreements utilizing hash functions, specifically tailored for smart grid environments. Nevertheless, this method proves ineffective in countering man-in-the-middle and impersonation attacks.

Conforming to to the need for robust resistance against desynchronization attacks, Das et al. proposed an ECC-based authentication technique using HASH [18]. Conversely, Srinivas et al. introduced a security scheme that, unfortunately, exposes vulnerabilities to man-in-the-middle attacks, masquerading, and privacy infringements on anonymity [19].

Furthurmore, Tsai and Lo introduced an identity-based signature protocol aimed at facilitating mutual authentication between smart meters and service providers, ensuring secure communication [20]. However, this scheme exhibits several limitations, including susceptibility to offline password-guessing attacks, privileged-insider attacks, challenges in preserving smart meter privacy, and session key (SK) security issues [20].

Besides, Odelu et al. [21] conducted a comprehensive cryptanalysis of Tsai and Lo's protocol [20] to uncover its security flaws. As elucidated by Odelu et al. [21], the protocol outlined in [20] not only falls short in defending against secret key leakage attacks but also lacks the capacity to ensure user privacy. Consequently, to rectify these deficiencies, Odelu et al. [21] introduced an enhanced authentication protocol tailored for the smart grid environment.

Scheidt et al. devised a method which involves authenticating a user's identity for system access[22]. It does so by using multiple factor-based data instances associated with the user. The process includes creating a modified data instance from a second data instance, generating a key from a first data instance, using that key to recover data from the modified instance, and comparing it with the second instance to calculate an authentication value. The user's access to the system is then determined, with access being granted or restricted based on the validity of the authentication value.

Kim et al. explores user authentication methods, which use factors like knowledge, possession, biometrics, or behavior to verify identity[4]. With the evolving risks in online settings, authentication methods have diversified. The study assesses authentication methods across web portals, electronic transactions, financial services, and e-government to identify their character-

istics and challenges. It proposes a tailored user authentication level system model for diverse online services.

Table 1 offers insights into diverse cryptographic primitives, advantages, and issues associated with existing schemes. It underscores the pressing need to develop a robust authentication and key agreement protocol for the Next Generation Grid infrastructure capable of mitigating the security vulnerabilities identified in prior literature. In this study, we proposed a robust yet lightweight protocol specifically designed to enhance security in the Next Generation Grid environment.

Table 1: Cryptographic techniques, qualities and challenges of existing schemes

Protocol	Cryptographic Techniques	Qualities	Challenges
Rana et al.[23]	Hash-based	Key agreement Resists replay and impersonation	Prone to device capturing attack Susceptible to desynchronization attack
Srinivas et al.[19]	Signature Based Elliptic Curve Cryptography Privileged Insider Attack	Mutual Authentication Authenticated session key agreement	Prone to masquerading attack Vulnerable to man-in-the-middle attack Violates anonymity
Bera et al.[16]	Elliptic Curve Cryptography Message Authentication Code	P2P Communication Mutual Authentication Provide intractability	Clock synchronization problem User anonymity not offered
Das et al.[18]	ECC Based Hash Based Signature Based	Mutual Authentication Secure session key establishment	Vulnerable to desynchronization attack

3 Cryptographic Preliminaries

3.1 System Model

In this ongoing decade, researchers have increasingly focused on advancing the build up of the next-generation Grid, particularly in the fields of distribution and communication. Several communication models have been introduced in the literature [24, 25, 3] to investigate and advance these objectives.

This article explores a system model that encompasses both distribution and transmission systems. The distribution network (DN) employs two primary methods: transmission substations (TSs) located at distribution substations (DS) and power plants (PP), to facilitate the efficient delivery of electricity to end users from power plants. The responsibility for transmitting electricity from the power plant to the TS falls under the jurisdiction of the TS, while the distribution of electricity to feeders is managed by DN. Subsequently, intermediate level voltage is changed into a low voltage suitable for consumption by consumer's appliances.

The hierarchical network structure for distribution consists of the Premises Area Network (PAN), Neighborhood Area Network (NAN), and Building Area Network (BAN). In practice, a single BAN can encompass multiple PANs. Each NAN comprises numerous BANs, and each Distribution Substation (DS) serves a specific neighborhood area. Multiple DSs collectively shelter neighborhoods. Hence, every DS is associated with one NAN, each NAN accommodates several BANs, and every BAN has the capacity for multiple PANs.

Automated meters play a crucial role in establishing a bidirectional communication link between power providers and consumers. These meters are equipped with dual interfaces: one

Table 2: Mathematical Notations

Notations	Description
AM	Automated Meter
$PANPortal$	Premises Area Network Portal
CSP	Cryptographic Service Provider
PIN	Personal Identification Number
UID_u	Identity of u_{th} AM (32 Byte)
UID_f	Identity of f_{th} $PANPortal$ (32 Byte)
r	Prime random number (32 Bytes)
x	Private key of CSP (32 Bytes)
SK	Session Key
$\oplus$, $\|$	XOR and Concatenation
$h(.)$	SHA-256 cryptographic hash function

serves for communication purposes, functioning as gateways (GWs), while the other is dedicated to power reading. These automated meters are strategically positioned at different hierarchical levels, identified as BAN-GW, NAN-GW, and PAN-GW. Electric power consumers can monitor their present electricity utilization levels using these automated meters and, additionally, have the capability to control their consumption by activating or deactivating specific appliances.

3.2 Adversarial Model

Dolev-Yao adversarial model [26], posits the following security capabilities for the adversary:

1. An adversary A, can intercept all communications taking place between various entities through the public channel, including those involving AM, PAN Portal, and CSP.
2. The A possesses the capability to modify, re transmit, or retain the messages transmitted over the public channel.
3. If A acquires the identity of AM, A can trace its communications.

3.3 Mathematical Notation Table

Table 2 provides a comprehensive list of the notations used in the design of the proposed protocol.

4 Our Proposed Scheme

In this section, we proposed our scheme for monitoring automated meters within the next generation infrastructure. The scheme is structured into three phases: (i) Automated Meter

(AM) Registration phase, (ii) Premises Area Network (PAN) Portal Registration phase, and (iii) Login and Mutual Authentication phase.

AM and PAN Portal registrations are securely conducted through a private channel. However, in our proposed strategy, the login and mutual authentication phases take place via a public channel. During mutual authentication, the Cryptographic Service Provider (CSP) plays a determining role in verifying the legitimacy of both the AM and PAN Portal. Upon successful authentication, a session key is established among the participating entities.

Once the session key is established, the AM, PAN Portal, and CSP can communicate securely with each other. The Session Key (SK) adds an additional layer of security since it is discarded after each use in setting up a secure communication channel. This means that the SK mechanism achieves end-to-end encryption, enhancing the overall security of the communication process.

4.1 Automated Meter (AM) Registration Phase

In the infrastructure of the Next Generation Grid, digital homes are outfitted with automated meters to monitor electricity usage. These automated meters collect data from end-users, including load devices, energy consumption measurements, and supplementary information, which is then relayed to the Cryptographic Service Provider (CSP) via the PAN Portal.

Prior to installation, any new automated meter must undergo a registration process with the CSP to attain valid status. In this process, the automated meter sends a registration request to the CSP, accompanied by its unique identity and PIN for registration purposes. Upon receiving a registration request from the automated meter, the CSP verifies whether the provided identity already exists within its database or not. If that do not exist then CSP proceeds to the further steps of registration. The registration request will be initiated by AM by selecting its unique ID and a PIN. With that information SID_u is calculated by $h_1(UID_u \oplus PIN_u)$. The next two parameters are sent towards CSP, UID_u and SID_u, respectively. Upon receiving the required information having knowledge of the private key it calculates K_u by $h_1(UID_u \| x)$ along with $\overline{L}_u = SID_u \oplus K_u$ and $M_u = h_2(K_u \| UID_u \| SID_u)$ as shown in Table 3.

Table 3: Automated Meter Registration Phase

AM		*CSP*
User input UID_u		
User selects PIN_u		
Compute $SID_u = h_1(UID_u \oplus PIN_u)$	$\xrightarrow{UID_u, SID_u}$	$K_u = h_1(UID_u \| x)$ $\overline{L}_u = SID_u \oplus K_u$ $M_u = h_2(K_u \| UID_u \| SID_u)$
Store	$\xleftarrow{\overline{L}_u, M_u}$	
$\overline{L}_u$ and M_u into smart card		

4.2 Premise Area Network (PAN) Portal Registration Phase

The PAN Portal plays a crucial role by gathering data from numerous automated meters (AM) located in neighboring areas. Subsequently, this collected data is relayed to the cryptographic service provider. However, prior to this operation, the PAN Portal must establish its legitimacy within the system by registering with the Cryptographic Service Provider (CSP). Furthermore, it is important to note that the PAN Portal faces limitations in terms of available computational

power and memory resources. Additionally, the PAN Portal is tasked with the responsibility of storing and managing information pertaining to all the interconnected automated meters.

To initiate this registration process, the PAN Portal dispatches a registration request to the CSP, along with its unique identity (UID) and PIN, transmitted securely. Upon receiving the identity, the CSP conducts an initial check within its database to determine whether the received UID already exists. If a matching UID is found in the database, the CSP will automatically decline the registration request. Otherwise CSP computes $K_f = h_1(UID_f \| x)$ in addition to $\overline{L}_f = SID_f \oplus K_f$ and $M_f = h_2(K_f \| UID_f \| SID_f)$ and store the information at the PAN Portal shown in the Table 4.

Table 4: PAN Portal Registration Phase

$PANPortal$		CSP
Input UID_f		
Fog Node selects PIN_f		
Compute $SID_f = h_1(UID_f \oplus PIN_f)$	$\xrightarrow{UID_f, SID_f}$	$K_f = h_1(UID_f \| x)$ $\overline{L}_f = SID_f \oplus K_f$ $M_f = h_2(K_f \| UID_f \| SID_f)$
Store $\overline{L}_f$,M_f	$\xleftarrow{\overline{L}_f, M_f}$	

4.3 Login and Authentication Phase

This subsection elucidates the login and authentication phase within the framework of our proposed scheme. Given that the communication transpires over an inherently insecure public channel, involving diverse entities, including the automated meter, PAN Portal, and CSP, it is imperative to establish a robust mutual authentication mechanism to safeguard the integrity and confidentiality of the communication. It is worth mentioning that the process of hashing the SHA256 of two terms is represented as h_1. Likewise, for three terms, it is denoted as h_2. Correspondingly, the representations for four and five terms are h_3 and h_4, respectively. In our scheme, mutual authentication among the AM, PAN Portal, and CSP is accomplished through the following steps:

1. Firstly, AM inputs its UID_u and PIN_u after putting its smart card and furnishes K'_u and M_u. After checking the validity of the AM, it generates random number and computes $X_1 = r_1 \oplus K'_u$ and $A_u = h_2(UID_u \| K'_u \| r_1)$. Then, AM sends X_1, SID_u and A_u to the PAN Portal on the public channel.

2. Upon receiving X_1, SID_u and A_u from AM, PAN Portal generates a random number and calculate $K'_f = \overline{L}_f \oplus SID_f$, $X_2 = r_2 \oplus K'_f$ and $A_f = h_2(UID_f \| K'_f \| r_2)$.
Afterwards, PAN Portal relays X_1, X_2, SID_u, SID_f, A_u and A_f to the CSP.

3. CSP receives the parameters from PAN Portal and determines the authenticity of AM and PAN Portal by validating A_u and A_f, respectively. These values can be computed based on the fact that the CSP possesses comprehensive data regarding all the Automated Meters (AM) and the PAN Portal, inclusive of their respective Unique Identifiers (UIDs) and associated Personal Identification Numbers (PINs). If these are validated then CSP generated the random number and calculate $G_1 = (r_1 \| r_1) \oplus (r_2 \| r_3)$, $G_2 = (r_2 \| r_2) \oplus (r_1 \| r_3)$, $SK = h_3((r_1 \oplus r_2 \oplus r_3) \| G_1)$, $A_1 = h_4(UID_u \| K_u \| SK \| r_1 \| r_3)$

and $A_2 = h_4(UID_f \| K_f \| SK \| r_2 \| r_3)$. After calculation of all these parameters $U_u = h_1(r_1 \oplus SID_u)$ and $U_f = h_1(r_2 \oplus SID_f)$ are calculated. Finally, CSP responds to PAN Portal with G_1, G_2, U_u, U_f, A_1 and A_2.

4. After receiving parameters from CSP, PAN Portal computes $r_1 \| r_3 = G_2 \oplus r_2 \| r_2$, $SK = h_3((r_1 \oplus r_2 \oplus r_3) \| G_1)$ in addition to this it verifies $U_f \stackrel{?}{=} h_1(r_2 \oplus SID_f)$ and $A_2 \stackrel{?}{=} h_4(UID_f \| K_f \| SK \| r_2 \| r_3)$. If the equation is satisfied then PAN Portal assumes that CSP is authorised. Moreover, send G_1, U_u and A_1 to AM.

5. On the arrival of the parameters, AM computes $r_2 \| r_3 = (r_1 \| r_1) \oplus G_1$, $SK = h_3((r_1 \oplus r_2 \oplus r_3) \| G_1)$, $U_u \stackrel{?}{=} h_1(r_1 \oplus SID_u)$ and $A_1 \stackrel{?}{=} h_4(UID_u \| K_u \| SK \| r_1 \| r_3)$ is verified. If the equation is justified then a session is created among all the devices.

Finally, login and authentication phase is presented in Table 5.

5 Formal Security Analysis

In this section, we perform a formal security analysis of the proposed protocol. To establish the formal security of our protocol, we employ the Random Oracle Model (ROM). The ROM is a widely accepted framework for assessing the security of key establishment protocols and signature schemes [27]. In this model, the hash function is treated as if it behaves like a truly random function, generating a unique random value for each new query. Several assumptions have been taken into account during the course of this analysis.

5.1 Security Model

To evaluate the security of our proposed protocol against well-known attacks, we initiated this analysis by constructing a comprehensive security model. Below, we provide a detailed analysis of the security model we have considered:

- **Participants:** A network comprising a significant number of participants is governed by an authentication protocol denoted as $\prod$. Within this network, participants can be classified as either an AM, PAN Portal, or a CSP. Each participant's entities can serve as oracles, and it is feasible for every oracle to become involved in the particular execution of $\prod$. An instance of the appearance of AM in a particular session is represented as $\prod_U^k$.
- **Attacker Model:** It is assumed that an attacker has the capability to intercept and manipulate the public communication channel. The A can strategize and initiate multiple sessions among participating entities. A is capable of executing the following queries in any possible sequence.

    1. **Send:** This query entails a scenario where an adversary , denoted as A, transmits a message M to the oracle $\prod_U^k$. Upon receiving message M, the oracle engages in computations aligned with the prescribed protocol, subsequently furnishing responses based on these computations.
    2. **Reveal:** In this query model, when the oracle $\prod_U^k$ accepts, the adversary A has the capability to obtain a session key SK. Conversely, if the oracle $\prod_U^k$ does not grant acceptance, the adversary A receives a null value in response.

Table 5: Login and Authentication Phase

AM	PAN Portal	CSP
Input UID_u and PIN_u $K_u^{'} = \overline{L}_u \oplus SID_u$ $M_u \stackrel{?}{=} h_2(K_u^{'} \| UID_u \| SID_u)$ Generate: $r_1 \in Z_p^*$ $X_1 = r_1 \oplus K_u^{'}$ $A_u = h_2(UID_u \| K_u^{'} \| r_1)$		
$\xrightarrow{X_1, SID_u, A_u}$	$K_f^{'}$=$\overline{L}_f \oplus SID_f$ $M_f \stackrel{?}{=} h(K_f^{'} \| UID_f \| SID_f)$ Generate: $r_2 \in Z_p^*$ $X_2 = r_2 \oplus K_f^{'}$ $A_f = h_2(UID_f \| K_f^{'} \| r_2)$	
	$\xrightarrow{X_1, X_2, SID_u, SID_f, A_u, A_f}$	$K_u = h_1(UID_u \| x)$ r_1=$X_1 \oplus K_u$ $A_u \stackrel{?}{=} h_2(SID_u \| K_u \| r_1)$ $K_f = h_1(UID_f \| x)$ r_2=$X_2 \oplus K_f$ $A_f \stackrel{?}{=} h_2(UID_f \| K_f \| r_2)$ Generate $r_3 \in Z_p^*$ $G_1 = (r_1 \| r_1) \oplus (r_2 \| r_3)$ $G_2 = (r_2 \| r_2) \oplus (r_1 \| r_3)$ $SK = h_3((r_1 \oplus r_2 \oplus r_3) \| G_1)$ $A_1 = h_4(UID_u \| K_u \| SK \| r_1 \| r_3)$ $A_2 = h_4(UID_f \| K_f \| SK \| r_2 \| r_3)$ $U_u = h_1(r_1 \oplus SID_u)$ $U_f = h_1(r_2 \oplus SID_f)$
	$r_1 \| r_3 = G_2 \oplus (r_2 \| r_2)$ $SK = h_3((r_1 \oplus r_2 \oplus r_3) \| G_1)$ $U_f \stackrel{?}{=} h_1(r_2 \oplus SID_f)$ $A_2 \stackrel{?}{=} h_4(UID_f \| K_f \| SK \| r_2 \| r_3)$	$\xleftarrow{G_1, G_2, U_u, U_f, A_1, A_2}$
$r_2 \| r_3 = (r_1 \| r_1) \oplus G_1$ $SK = h_3((r_1 \oplus r_2 \oplus r_3) \| G_1)$ $U_u \stackrel{?}{=} h_1(r_1 \oplus SID_u)$ $A_1 \stackrel{?}{=} h_4(UID_u \| K_u \| SK \| r_1 \| r_3)$	$\xleftarrow{G_1, U_u, A_1}$	

3. **Corrupt:** In this query model, the adversary A has the ability to initiate a query directed at the participant U, thereby obtaining the participant's private key in return.
4. **Test:** If the oracle $\prod_U^k$ has approved the request and possesses a session key SK, the subsequent sequence of events unfolds. A coin, represented as 'b', is flipped. If the outcome of the coin flip is 'b' = 0, the session key is relinquished to the adversary. Conversely, if the coin lands as 'b' = 1, a random session key is generated from the distribution that aligns with the intended session key distribution. This specific query serves the purpose of assessing the adversary's effectiveness and is not indicative of any genuine adversarial capabilities. It is essential to consider the adversary posing this query only once.

In the context of key agreement without authentication, the adversary possesses the ability to execute Send, Reveal, Corrupt, and Test queries[28]. It's important to emphasize that, even under adaptive chosen message attacks, the adversary's capabilities are limited to finite queries [28, 29, 30]. For a more comprehensive understanding of additional security requirements pertaining to mutual authentication and key exchange protocols, you can find detailed descriptions in [28, 31, 29, 30].

1. ID Attack: An adversary can send specific identities to acquire the private keys associated with those identities[31, 29].
2. Understanding session key security: Adversary A has acquired knowledge of certain past session keys, but remains incapable of compromising forthcoming session keys. This level of knowledge can be obtained through *Reveal* queries.
3. Impersonation Attack: An adversary is unable to impersonate any participants to gain access to information about a session key from other participants.
4. Perfect Forward Secrecy: The proposed ID-based authenticated key exchange protocol achieves partial forward secrecy. In the event that the server's private key is compromised by an adversary, it is possible to recover previous session keys from the transcript. However, in the case of $User$ being compromised, the adversary should not gain access to knowledge about the previous session keys.

6 Performance Comparison

This section provides a thorough performance evaluation, comparing the security features of our scheme with other related schemes, including those by Rana et al. [23], Jia et al. [32], and Ever et al. [33]. Our analysis encompasses various aspects, including security attributes, communication costs, and computational costs. Subsequent subsections offer a detailed comparison and analysis of these aspects, as indicated in Table 6.

6.1 Computational cost evaluation

The computational overhead is determined by comparing the time required for executing essential cryptographic operations during both the login and authentication phases of our proposed protocol and related protocols. Since the registration phase occurs only once, we concentrate solely on the cryptographic operations during the login and authentication phases to evaluate the computational overhead of our protocol and its related counterparts [23, 32, 33]. In

Table 6: Comparison of computation and communication overhead.

Protocols	**Automated Meter**	**CSP**	**PAN Portal**	**Aggregated Computation Overhead**	**Aggregated Communication Overhead**
Ours	17$hash$	28$hash$	17$hash$	3.25164 ms	5376 bits
Rana et al.[23]	23$hash$	36$hash$	18$hash$	3.52468 ms	6912 bits
Jia et al.[32]	19$hash$ + 2E_m	36$hash$ + 3E_m	17$hash$ + 2E_m	4.12329 ms	7232 bits
Ever et al.[33]	35$hash$ + 4E/D	18$hash$ + 2E/D	27$hash$ + 2E/D	5.81686 ms	6208 bits

our proposed protocol computational time for all the entities that are AM,PAN Portal and CSP are calculated as: (17×0.002)+(28×0.00063)+(17×0.192)≈ 3.25164ms. Similarly, we can calculate the computational cost of other authentication protocols which are shown in Table 6. To estimate the processing cost, we take into account the utilization of the hash function, point multiplication, and symmetric encryption/decryption. The detailed computation cost comparison is provided in Table 6. This table clearly depicts that the computational cost of our proposed protocol is far less than its counterparts.

6.2 Communication Cost Evaluation

In this section, we conduct a comparison of communication costs for both the registration and authentication phases, taking into account similar schemes [21, 34, 35, 36]. We evaluate the total number of bits exchanged among the three entities: (i) AM, (ii) PAN Portal, and (iii) CSP during the registration process. To calculate the communication cost, it is necessary to specify the size in bytes of all the inputs. Finally, we sum up all the values involved in a specific process to determine the communication cost of an authentication scheme.
In case of our proposed protocol during login and authentication phase messages flows in between different entities carrying different information. The flow of information starts form AM to PAN Portal and it contains X_1, SID_u and A_u. Then from PAN Portal to CSP and later in reverse order from CSP to PAN Portal and at last from PAN Portal to AM. In the complete Login and Authentication Phase four different messages are transferred which in terms generate (15 × 256)+(3× 512)=5376 bits. Whereas Rana et al. [23] transferred (13×256)+(7×512)=6912 bits, in addition to this Jia et al.[32] communicate (8×256)+(4×512)+(7×392)=7232 bits. The communication overhead of Ever et al. [33] is calculated in the same way. Thus, the communication overhead of Ever et al. is (8×256)+(2×512)+(8×392)=6208. The combined communication overhead of our protocol and competing protocols is presented in Table 6. It is evident from the table that our protocol requires fewer bits for communication compared to the competing protocols.

7 Security features Comparison

The security assessments of our proposed system and other similar systems, as outlined in [21, 34, 35, 36], are presented in Table 7. Main point of concern is this that other counterparts cannot secure the system efficiently as shown in the table. Rana et al. [23] scheme is also the

robust one but still it cannot provide security against Perfect Forward secrecy and man in the middle attack moreover, it does not support multi factor authentication. The table illustrates that our scheme demonstrates resilience against a variety of security attacks.

Table 7: Summary of security features

Attacks	**Our**	**Rana et al.[23]**	**Jia et al.[32]**	**Ever et al.[33]**
Multi Factor Authentication	✓	×	×	×
Perfect Forward Secrecy	✓	×	✓	✓
Man in the Middle Attack	✓	×	✓	✓
Resilience against Automated Meter impersonation Attack	✓	✓	✓	✓
Resilience against PAN Portal impersonation attack	✓	✓	✓	✓
Resilience against Service Provider impersonation attack	✓	✓	✓	✓
Provides Mutual Authentication	✓	✓	×	✓
Supports Anonymity	✓	✓	✓	✓
Prevents Insider attack	✓	✓	×	×
Free from clock synchronization problem	✓	✓	×	×
Prevents stolen verifier attack	✓	✓	✓	✓
Ephemeral secret leakage (ESL) attack	✓	✓	×	×

8 Conclusion

Communication among various entities, including automated meters AM, premise area networks PAN Portals, and the cryptographic service provider CSP, occurs over public channels within the next-generation grid environment. Automated meters are usually located in open areas accessible for public, making them prone to both physical and cyber attacks. In this article, we have designed a multi factor authentication scheme to mitigate these physical and cyber threats. Our thorough security analysis exhibit the effectiveness of our scheme in resisting various types of attacks. Furthermore, our system excels in terms of communication and computing costs when compared to alternative schemes. The Next-Generation grid environment comprises various entities, including automated meters (AM), premise area networks (PAN) Portals, and the cryptographic service provider (CSP), communicating over public channels. Automated meters play a pivotal role in measuring and transmitting electricity consumption data but are exposed to physical and cyber threats due to their public placement. To address these vulnerabilities, our article introduces a robust multi-factor authentication scheme. This solution is meticulously crafted to mitigate the inherent risks, enhancing the protection of these critical grid components. Our research confirms the effectiveness of the proposed protocol in safeguarding against a spectrum of attacks, including impersonation, man-in-the-middle, key disclosure and identity disclosure. Moreover, our protocol guarantees secure mutual authentication, anonymity, and the integrity of demand response data. To bolster the credibility of our findings, we conducted a formal security analysis using the ROM model. Furthermore, when compared to other contemporary protocols, our proposed solution stands out. It exhibits a comparable cost cutting while delivering a heightened level of security and enhanced functionalities. This underscores the protocol's value as a robust and efficient choice in the domain of secure data transmission and authentication.

References

[1] A. Humayed, J. Lin, F. Li, B. Luo, Cyber-physical systems security—a survey, IEEE Internet of Things Journal 4 (6) (2017) 1802–1831.

[2] D. Wu, C. Zhou, Fault-tolerant and scalable key management for smart grid, IEEE Transactions on Smart Grid 2 (2) (2011) 375–381.

[3] W. Wang, Y. Xu, M. Khanna, A survey on the communication architectures in smart grid, Computer networks 55 (15) (2011) 3604–3629.

[4] J.-J. Kim, S.-P. Hong, A method of risk assessment for multi-factor authentication, Journal of Information Processing Systems 7 (1) (2011) 187–198.

[5] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, Y. Koucheryavy, Multi-factor authentication: A survey, Cryptography 2 (1) (2018) 1.

[6] K. Mahmood, S. A. Chaudhry, H. Naqvi, T. Shon, H. F. Ahmad, A lightweight message authentication scheme for smart grid communications in power sector, Computers & Electrical Engineering 52 (2016) 114–124.

[7] X. Li, F. Wu, S. Kumari, L. Xu, A. K. Sangaiah, K.-K. R. Choo, A provably secure and anonymous message authentication scheme for smart grids, Journal of Parallel and Distributed Computing 132 (2019) 242–249.

[8] M. Wazid, A. K. Das, N. Kumar, J. J. Rodrigues, Secure three-factor user authentication scheme for renewable-energy-based smart grid environment, IEEE Transactions on Industrial Informatics 13 (6) (2017) 3144–3153.

[9] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, A. K. Sangaiah, An elliptic curve cryptography based lightweight authentication scheme for smart grid communication, Future Generation Computer Systems 81 (2018) 557–565.

[10] D. Abbasinezhad-Mood, M. Nikooghadam, An anonymous ecc-based self-certified key distribution scheme for the smart grid, IEEE Transactions on Industrial Electronics 65 (10) (2018) 7996–8004.

[11] K. Mahmood, W. Akram, A. Shafiq, I. Altaf, M. A. Lodhi, S. H. Islam, An enhanced and provably secure multi-factor authentication scheme for internet-of-multimedia-things environments, Computers & Electrical Engineering 88 (2020) 106888.

[12] W. Akram, K. Mahmood, X. Li, M. Sadiq, Z. Lv, S. A. Chaudhry, An energy-efficient and secure identity based rfid authentication scheme for vehicular cloud computing, Computer Networks 217 (2022) 109335.

[13] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, X. S. Shen, A lightweight message authentication scheme for smart grid communications, IEEE Transactions on Smart grid 2 (4) (2011) 675–685.

[14] J. Xia, Y. Wang, Secure key distribution for the smart grid, IEEE Transactions on Smart Grid 3 (3) (2012) 1437–1443.

[15] S. A. Chaudhry, H. Alhakami, A. Baz, F. Al-Turjman, Securing demand response management: A certificate-based access control in smart grid edge computing infrastructure, IEEE Access 8 (2020) 101235–101243.

[16] B. Bera, S. Saha, A. K. Das, A. V. Vasilakos, Designing blockchain-based access control protocol in iot-enabled smart-grid system, IEEE Internet of Things Journal 8 (7) (2020) 5744–5761.

[17] D. Abbasinezhad-Mood, A. Ostad-Sharif, M. Nikooghadam, S. M. Mazinani, A secure and efficient key establishment scheme for communications of smart meters and service providers in smart grid, IEEE Transactions on Industrial Informatics 16 (3) (2019) 1495–1502.

[18] A. K. Das, B. Bera, S. Saha, N. Kumar, I. You, H.-C. Chao, Ai-envisioned blockchain-enabled signature-based key management scheme for industrial cyber–physical systems, IEEE Internet of Things Journal 9 (9) (2021) 6374–6388.

[19] J. Srinivas, A. K. Das, X. Li, M. K. Khan, M. Jo, Designing anonymous signature-based authenticated key exchange scheme for internet of things-enabled smart grid systems, IEEE Transactions on Industrial Informatics 17 (7) (2020) 4425–4436.

[20] J.-L. Tsai, N.-W. Lo, Secure anonymous key distribution scheme for smart grid, IEEE transactions on smart grid 7 (2) (2015) 906–914.

[21] V. Odelu, A. K. Das, M. Wazid, M. Conti, Provably secure authenticated key agreement scheme for smart grid, IEEE Transactions on Smart Grid 9 (3) (2016) 1900–1910.

[22] E. M. Scheidt, E. Domangue, Multiple factor-based user identification and authentication, uS Patent 7,131,009 (Oct. 31 2006).

[23] M. Rana, K. Mahmood, M. A. Saleem, F. Al-Turjman, M. S. Kolhar, C. Altrjman, Towards a provably secure authentication protocol for fog-driven iot-based systems, Applied Sciences 13 (3) (2023) 1424.

[24] C. Efthymiou, G. Kalogridis, Smart grid privacy via anonymization of smart metering data, in: 2010 first IEEE international conference on smart grid communications, IEEE, 2010, pp. 238–243.

[25] Z. Lu, X. Lu, W. Wang, C. Wang, Review and evaluation of security threats on the communication networks in the smart grid, in: 2010-Milcom 2010 Military Communications Conference, IEEE, 2010, pp. 1830–1835.

[26] D. Dolev, A. Yao, On the security of public key protocols, IEEE Transactions on information theory 29 (2) (1983) 198–208.

[27] M. Bellare, P. Rogaway, Random oracles are practical: A paradigm for designing efficient protocols, in: Proceedings of the 1st ACM Conference on Computer and Communications Security, 1993, pp. 62–73.

[28] M. Jakobsson, D. Pointcheval, Mutual authentication for low-power mobile devices, in: Financial Cryptography: 5th International Conference, FC 2001 Grand Cayman, British West Indies, February 19–22, 2001 Proceedings 5, Springer, 2002, pp. 178–195.

[29] J. C. Choon, J. Hee Cheon, An identity-based signature from gap diffie-hellman groups, in: Public Key Cryptography—PKC 2003: 6th International Workshop on Practice and Theory in Public Key Cryptography Miami, FL, USA, January 6–8, 2003 Proceedings 6, Springer, 2002, pp. 18–30.

[30] M. Bellare, D. Pointcheval, P. Rogaway, Authenticated key exchange secure against dictionary attacks, in: International conference on the theory and applications of cryptographic techniques, Springer, 2000, pp. 139–155.

[31] D. Boneh, M. Franklin, Identity-based encryption from the weil pairing, in: Annual international cryptology conference, Springer, 2001, pp. 213–229.

[32] X. Jia, D. He, N. Kumar, K.-K. R. Choo, Authenticated key agreement scheme for fog-driven iot healthcare system, Wireless Networks 25 (2019) 4737–4750.

[33] Y. K. Ever, Secure-anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks, IEEE systems journal 13 (1) (2018) 456–467.

[34] J. Wang, L. Wu, K.-K. R. Choo, D. He, Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure, IEEE Transactions on Industrial Informatics 16 (3) (2019) 1984–1992.

[35] J. Lee, S. Yu, M. Kim, Y. Park, A. K. Das, On the design of secure and efficient three-factor authentication protocol using honey list for wireless sensor networks, IEEE Access 8 (2020) 107046–107062.

[36] S. Garg, K. Kaur, G. Kaddoum, J. J. Rodrigues, M. Guizani, Secure and lightweight authentication scheme for smart metering infrastructure in smart grid, IEEE Transactions on Industrial Informatics 16 (5) (2019) 3548–3557.