Article

Fortified-Grid: Fortifying Smart Grid through Integration of TPM in IoT Devices

Giriraj Sharma [1], Saraju P. Mohanty [2]* and Amit M. Joshi [1]

[1] Department of Electronics and Communication, MNIT, Jaipur, India ; amjoshi.ece@mnit.ac.in
[2] Department of Computer Science and Engineering, University of North Texas, Texas, USA ; saraju.mohanty@unt.edu
* Correspondence: saraju.mohanty@unt.edu (SM)

Abstract: This paper presents a hardware-assisted security primitive that integrates Trusted Platform Module (TPM) in IoT devices for authentication in the smart grid. Device and data security are pivotal for the smart grid since vulnerable working ecosystem security attacks could risk grid failure. The proposed Fortified-Grid security primitive provides an innovative solution, leveraging the TPM for attestation, coupled with standard X.509 certificates. This methodology serves a dual purpose, ensuring the authenticity of IoT devices and upholding software integrity, an indispensable foundation for any resilient smart grid security system. TPM is a hardware security module that can generate keys and store them encrypted so they cannot be compromised. Formal security verification is performed using the Random or Real (ROR) Oracle model and widely accepted AVISPA simulation tool, while informal security verification uses DY and CK adversary model. Fortified-Grid can validate the attested state of IoT devices in a minimal network overhead of 1984 bits.

Keywords: Trusted Platform Module (TPM); IoT; Cyber-Physical System; Security by Design (SbD); Hardware Assisted Security (HAS); Smart Grid

Citation: Sharma, G.; Mohanty, S.P.; Joshi,A.M. Fortified-Grid: Fortifying Smart Grid through Integration of Trusted Platform Module in IoT Devices. *Journal Not Specified* **2023**, *1*, 0. https://doi.org/

Received:
Revised:
Accepted:
Published:

1. Introduction

The advancement of technology in IoT has paved the way for effective ways of communication in smart grid technology [1]. The smart grid has been replaced with a traditional grid to cater to energy demand. Smart Grid would allow two-way communication between utilities and consumers during the power transaction process. Advanced metering infrastructure (AMI) and smart metering (SM) technologies can upgrade the conventional power grid by disclosing the hidden features of electrical power. The vehicle-to-grid (V2G) network offers bidirectional energy, information transmission, and other characteristics [2]. Smart grids use various devices for monitoring, analyzing, and controlling the grid deployed at power plants, transmission systems, and consumer premises. The security and reliability of the smart grid system are the real challenges due to its heterogeneous connectivity over the network. Hence smart grids require connectivity, authentication, automation, and tracking of such devices through IoT. The Internet of Things (IoT) is a network of cyber-physical objects comprising sensors, actuators, and software communicating continuously with their surroundings. IoT devices are used in smart grids in the generation, transmission, distribution, and consumer premises at various systems such as supervisory control and data acquisition (SCADA), AMI, smart meter, etc.
Smart grid IoT devices and gateway usually communicate over wireless media; hence the security of IoT devices has been more challenging. A further attacker may compromise the data of devices collected during communication. Hence IoT devices need more security features such as authentication, encryption, proper configuration of devices, and timely updating of software [3,4]. A Raspberry Pi 4 device equipped with TPM for attestation of IoT device was proposed by [5]. The integrity of remote attestation is continuously

monitored.

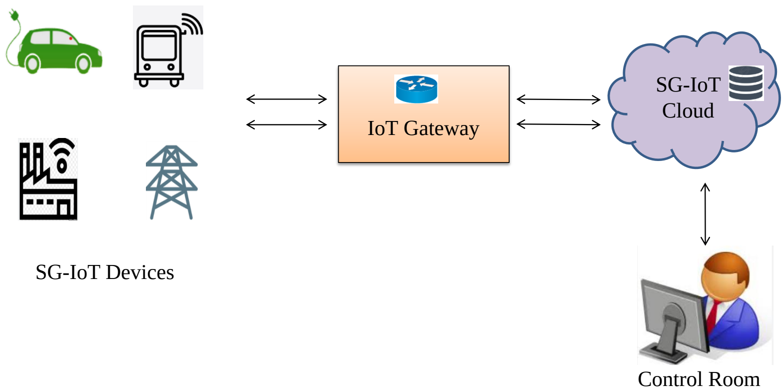

Figure 1. System level overview of Fortified-Grid.

The uses of IoT devices in daily life, such as home, office, transportation systems, smart agriculture, Industry 4.0, and healthcare systems, are increasing rapidly daily. It is estimated that about 70% of devices will be IoT-based due to continuously increasing industrialization and urbanization [6]. As per the CISCO survey report, there will be around $14.4 trillion devices by the end of 2025 [7]. There will be a huge demand for IoT devices in smart gird. IoT smart grid is expected to contribute $1.1-$2.5 trillion growth per annum. Hence, in the future, many sensors will be deployed in IoT networks. A protocol for IoT security using TPM and PUF was proposed by [8]. TPM stores the PUF key in its hence can not be accessed from outside by any adversary.
An effective mutual authentication procedure is required for trusted communication between smart grid IoT devices. Digital certificates are electronic files that prove the authenticity of devices or servers using device identity, the public key, and a cryptographic key. Certificate Authority (CA) signs the digital certificate, and all entity trusts the CA. In addition to evidence verification using a digital certificate, remote attestation checks the integrity of the IoT software state and detects any change. In the remote attestation mechanism, the state of software or memory proof of untrusted devices is exchanged with the server or other device for verification. RA mechanisms rely on Trusted Platform Modules (TPM) to generate attestation proof. The TPM protocol can provide security to manufacturers of IoT devices and the service providers with more confidence in their certificate-based authentication processes for IoT devices containing a TPM [9]. A TPMwallet security protocol based on blockchain was proposed by [10] and can provide security for IoT device.
Integrity certificate checks software updates and, according to attestation, results are decided. These certificate in IoT network is different from conventional certificate due to the different constraints of IoT devices. However, RA results rely on integrity certificates for software state guarantee [11].
The paper's organization is as follows: Section 2 defines the Prior work related to smart grid IoT device security. Section 3 highlights the research gaps and novel contributions. The Roles of the Trusted Platform Module (TPM) for Hardware-Assisted Security (HAS) for Smart Grid are covered in Section 4. Section 5 elaborates on the proposed Fortified-Grid Model. Section 6 describes the proposed scheme for TPM-based authentication in Smart Grid. Section 7 explains the security analysis of the proposed TPM-based IoT Smart Grid network. Section 8 explains the experiment result and comparison with the state-of-the-art work, while section 9 describes the conclusion and result.

2. Prior work related to smart grid IoT device security

Secure, reliable, and efficient communication is essential in the IoT-based smart grid network [12]. Various schemes have been proposed in the literature to address smart grid

IoT security and privacy challenges. A layered perspective of smart grid security using game theory is proposed by [13]. Another lightweight schemes [14], [15] provides a basic concept and introduces the idea of smart gird IoT device authentication and grid resilience. A batch authentication technique for smart grid IoT devices which is based on HMAC codes is proposed by [16].

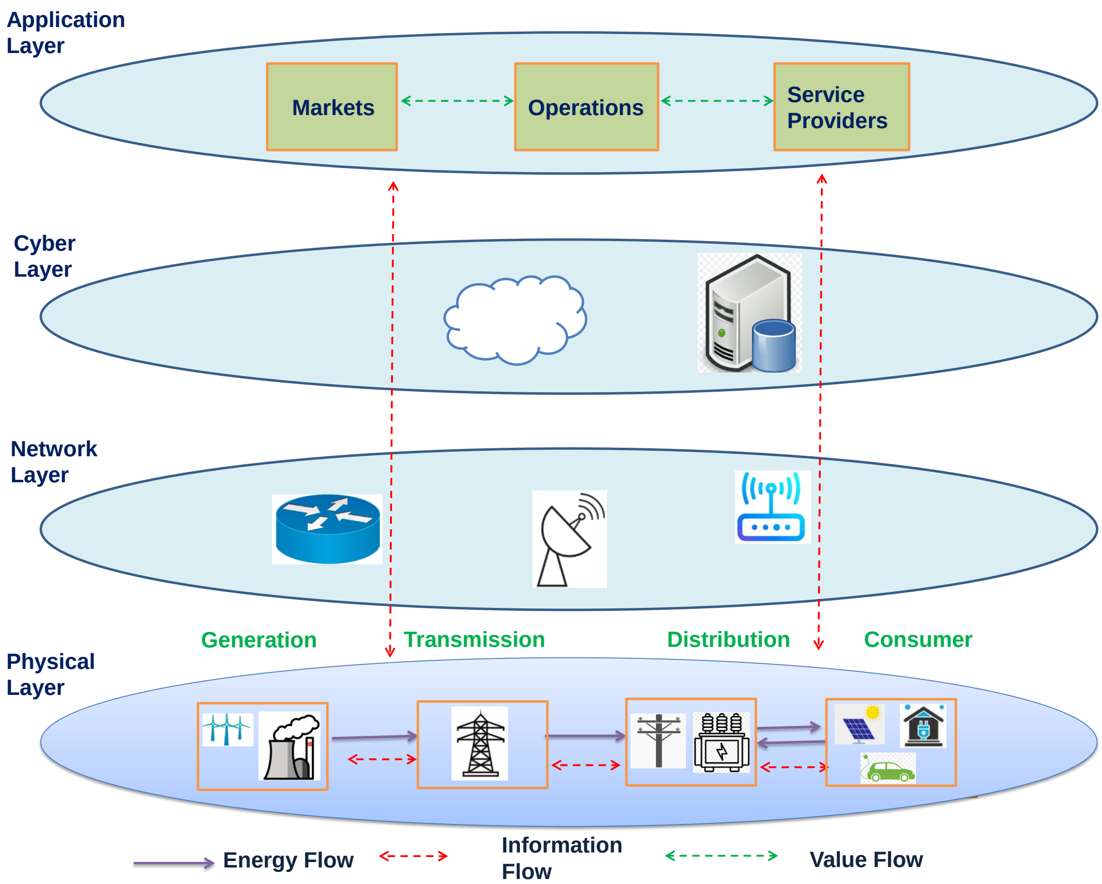

Figure 2. Four Layer IoT-aided Smart Grid Network.

In this scheme, they used identity-based signatures to perform batch authentication and used pseudonyms to prevent their identities. This scheme outperforms in terms of latency in comparison to other popular schemes. However, this scheme does not provide any solution for trust measurement. In addition, this scheme requires extra overhead due to the certificate revocation list. Scheme [17] describes attack detection and mitigation during wireless data transmissions in WSNs, MANETs, and IoT-enabled smart grid networks; the approaches are broadly classified as trust-based and cryptography-based.
A Chinese remainder theorem-based security of VANETs smart grid system suing TPD, ECDLP was proposed by [18]. However, this scheme suffers from integrity measurement and lack of security. Later secure message transmission using remote attestation and HMAC technique was suggested by [19]. More ever, the scheme proved security using the random oracle model under Diffi Helman key exchange. They use Intel-SGX, which is designed to ensure integrity against physical adversaries. However, it suffers from high communication and computation overheads. A certificate extensions-based scheme is proposed by [20]. However, this scheme was unable to protect the identity of IoT devices. [21]. Remote attestation based on the digital certificate was suggested by [22]. However, the scheme does not support hardware-assisted security and firmware integrity. A mutual authentication protocol based on DAA was suggested by [23]. This scheme addressed unmanned aerial vehicle communication security and uses asymmetric key pairing and TPM to combat malicious modular attacks [23]. Similarly, scheme [24] suggests an executable monitoring

system evidence to verify the system's status. Recently a TPM-based scheme for smart gird IoT device and server authentication is suggested by [25]. It uses remote attestation and integrity measurement methods to authenticate smart grid remote IoT devices. However scheme generates auto certificates each time during authentication, and one more entity CAB is introduced, making the protocol complicated and vulnerable.
Later scheme [26] proposed a certificate-less protocol based on a hash chain base and hash chain-less framework. However, scheme [27] demonstrated that the above scheme is vulnerable to replay attack and does not suggest any method to regenerate the hash chain.

Table 1. A Comparative analysis of different popular schemes.

Works	Primitive used	Features	Vulnerabilities
Zhang et al. 2019 [18]	TPD, ECDLP	Chinese remainder theorem based security of VANETs smart grid system.	No integrity measurement, lack of security
Zhong, et al. 2021 [19]	TPM, SGX, HMAC	connected and autonomous vehicles (CAVs) of smart grid	High overhead, Lack of proper security mechanism
Wazid, et al. 2022 [22]	TTP, Digital certificate	Less computational and communication overhead	Provide no Hardware-assisted security and firmware integrity
Khurshid, et al. 2023 [25]	TPM, RATS , X.509	Supports Hardware-assisted security and firmware integrity	Each time communicate with TTP for certificate hence large overheads
Currently Proposed (Fortified-Grid)	TPM, RATS, X.509	Hardware security for SG IoT devices, servers, and gateway, TPM ensures the integrity of firmware	Slightly higher overhead due to application of TPM

Scheme [28] pointed out that TPM is unsuitable for resource constraints devices due to space, power, and cost limitations and suggested a crypto acceleration module. However, this was unable to prove the root of trust management. A survey of remote attestation in the Internet of Things [29] proposed state of the art remote attestation scheme for attestation and summarized the basic feature of the protocol. Remote attestation gives attestation responsibility to resource-rich entities, i.e., servers, to make protocol suitable for smart grid IoT networks. To show various characteristics, existing RA is classified into five categories. However, the scheme could not demonstrate a secure attestation algorithm and security analysis. This scheme is vulnerable to replay attacks.
Most schemes discussed above have security flaws, cryptographic key security issues, or large overheads. The proposed scheme also supports adding new smart grid IoT devices after smart grid network deployment. The formal security verification of the scheme is performed using the widely AVISPA tool and ROR model against various attacks informal security verification using DY and CK adversary model.

3. Research Gaps and Novel Contributions

3.1. Problem Formulation

In the smart grid, a compromised IoT device's firmware enables device impersonation and the transmission of false messages to the server. Absence of firmware measurement allows the compromised device to be mistaken for the genuine one, causing incorrect data processing and potentially erroneous decisions, impacting the smart grid's functionality.
Numerous cryptographic schemes have been suggested to address this issue, yet these protocols often necessitate memory for storing security keys, rendering them susceptible to

diverse attacks. Trusted Platform Module (TPM) offers an innovative solution through an efficient key generation mechanism that enhances security in IoT applications. Its unique ability to generate keys using a trustworthy route, coupled with firmware integrity checks using Platform Configuration Registers (PCR), showcases both simplicity and resilience in design and implementation. This positions TPM as a dependable and robust security alternative for the smart grid environment.

3.2. Research Gaps

The following research gaps are identified from the literature survey [18,19,22,25]

- To the best of our knowledge, most IoT authentication schemes provide attestation and authentication mechanisms without considering the integrity of the device software.
- Most schemes use a cryptography key for attestation but may be vulnerable to software or intruder.
- Very few schemes provided complete authentication between IoT device to device and server for Smart grid.
- Lightweight authentication schemes as IoT devices in smart gird are generally resource constraints.

3.3. Research contribution

The novel contributions of the paper are

- The paper proposes a certificate-based authentication scheme for IoT devices containing a TPM in a smart grid.
- Device authentication utilizes a preloaded certificate and establishes a secret session key after the mutual authentication.
- Integrity of device software is ensured using TPM PCR measurement and comparison.
- The proposed scheme has validated the performance of the designed scheme on the widely acceptable AVISPA tool and Random or Real (ROR) model.
- Our analysis illustrates that the proposed model is secure, privacy-preserving, and supports minimal communicational overhead.

4. The Roles of Trusted Platform Module (TPM) for Hardware Assisted Security (HAS) for Smart Grid

IoT aided Smart grids to face various security challenges such as Integrity, Impersonation, Denial of Service (DoS), Replay attacks, Malware attacks, etc. A TPM is a cryptography co-processor hardware chip developed by the Trusted Computing Group (TCG) embedded in SG IoT devices. TPM is integrated with IoT devices, gateway nodes, and servers. In remote attestation and firmware updating, a TPM-based server away from the smart grid IoT devices collects and checks the measurement results. This section describes the technology and background information required for Fortified-Grid security and authentication.

4.1. Hardware Assisted Security (HAS)

Hardware-assisted security involves integrating specialized hardware components and functionalities to bolster the security of digital systems. These hardware elements work in conjunction with software-based security measures, adding an extra layer of defense against a range of threats. Examples encompass TPM, Hardware Security Modules (HSM), secure enclaves, and hardware-based encryption accelerators. These components provide capabilities such as secure key storage, encryption/decryption, secure boot, and isolated execution environments. By doing so, they enhance overall system security by minimizing attack opportunities and enhancing resilience against diverse cyber threats.
In smart gird IoT networks, the security of data can be posed at risk regardless of which technique is used. In these systems, different types of security challenges are, such as physical attacks, side-channel attacks, firmware or software modification, information security, privacy, protection, Bluetooth hardware security etc. However, the severity and

complexity of these attacks require a level of security that only the hardware support can ensure. Due to several advantages of TPM, we have used it with IoT devices for hardware security in our scheme. The Security by Design must be energy efficient, robust, low cost, fast and reliable.

4.2. Trusted Platform Module (TPM) for smart grid IoT devices

The TPM is an encryption co-processor built by the Trusted Computing Group (TCG). Smart gird IoT devices and server contains TPM. TPM is a hardware security module that can generate keys and store them encrypted so they cannot be compromised. Every TPM has its private Endorsement Key (EK) issued by a reliable Certified Authority (CA). It allows for easy authentication methods to be established, guaranteeing that the communication device in question includes a genuine and recognizable TPM. The security of a smart grid IoT deployment can be significantly bolstered by combining TPM features like secure boot and hardware/software attestation. The following are some of TPM's most notable characteristics:

- Key generation and secure storage:- The communication mainly occur in the smart grid system in an open environment. Hence secure storage and key generation are fundamental requirements in the smart grid network. The generation of cryptographic keys is one of the TPM's fundamental functions. The secret key is generated by a random number generator (RNG) or a secret seed. TPM can generate an infinite number of keys. Endorsement Key (EK) always remain inside the TPM, while Attestation Identification Key (AIK) is used for attestation purpose.
- Integrity management:- It is another vital feature of TPM. For the integrity of devices in smart grid IoT systems, all devices must be periodically configured because any vulnerability in any device increases the likelihood that the entire system will fail. TPM has multiple Platform Configuration Register (PCR), and the PCR hashed and stored system states. After the defined interval, each execution hash value is recomputed and compared with the previous accumulated value. As resetting or rolling back the PCR to its original state is impossible, any suspicious activity can be easily detected. Integrity measurement at system boot or startup ensures the client's trust [30].
- Remote attestation:- The advantages of the remote attestation technique for Smart grid systems include confidentiality and the defense against man in the middle (MITM). Cryptography-based systems are considered secure against various attacks, but in some instances, cryptography keys are compromised, resulting in the entire system being under threat. Therefore, validating the entity or key became imperative before allowing system access. TPM performs an attestation to validate the entity's or key's trustworthiness and authenticity. TPM generates a quote that contains the hash of the PCR state and nonce, signed by TPM. At the other end, if the TPM signature is validated, it is authenticated, and nonce ensures the freshness of the quote and avoids a replay attack.
- Authorization of an entity:- It gives an authenticated device or user the necessary permissions to access smart grid resources. Access control ensures that correctly recognized entities only access SG resources. By managing an entity's authorization, malicious attackers can alter the status or data of the entity. TPM can be used to mitigate these security threats. By defining a specific policy of entity, the PCR can be set to a specific value. So that when PCR is set to a desirable value, devices are only accessible. Hence all IoT devices are protected from unauthorized access, as all PCRs can roll back to the desired value.
- User Identification and secure communication:- Since two-way communication is one of the key differences between smart and traditional grids, it has several potential benefits, such as distributed smart sensors, distributed power generation, real-time measurements and metering infrastructure, monitoring systems, and fast response require reliable communication and information exchange. It enables smart grids to communicate effectively to provide dependable electricity generation and distri-

bution. A TPM can verify a Smart grid IoT device identity. Each device is assigned an identification key to prove its identity before initiating communication. Since the identifying key is obtained from the TPM's trusted root key, any rogue smart grid device attempting to access the system can be quickly identified. TPM generates random nonce that prevents replay attacks and secure communication between smart gird IoT devices [31].

4.3. Digital certificate extensions in SG-IoT network

An X.509 certificate is a digital certificate that uses the public key infrastructure (PKI) standard and contains an additional extension field to be used in the certificate. The digital certificate is a safeguard against various attacks. It enables IoT devices and servers to exchange information securely. X.509 v3 contains several additional fields, such as the device's unique identification string, serial number, the public part of a secret key, issuer name, validity period, signature, etc.

Certificate – X509v3 IoT profile		
version	:	v3
certificate serial number	:	abcdabcd1234
certificate issuer signature	:	Signing algorithm
Issuer name	:	CA name
validity period	:	1st jan2023 12:00:00 to 31st Dec 2024 12:00:00
Subject	:	Device name
Subject public key info	:	RSA
Issuer unique identifier	:	
Extension	:	Extension 1
Extension	:	Extension 2
Extension	:	Extension 3
Certificate authority digital signature		

Figure 3. Smart Grid IoT certificate.

4.4. Remote Attestation Procedures (RATS) in IoT-aided smart grid

In a smart grid IoT network, untrusted devices communicate or authenticate with trusted or untrusted devices. The remote attestation procedure (RATS) technique decides whether a smart gird device can trust the remote entity. This trust establishment is achieved using a two-stage challenge-response algorithm facilitated by a trusted third party (TTP), also known as a certificate authority.

The primary role of RATS is generating, transmitting, and evaluating attestation evidence. An attester generates evidence which is transmitted to verifiers for verification. Here attestation can be implemented using TPM quote, PCR values, and PCR logs evidence which provides the state of the software. During attestation, PCR computes the hash value of the current state and updates the previous store value. TPM can report the hash value of signed PCR and nonce, known as the quote.

5. The Proposed Fortified-Grid Model

5.1. Network Model

In the Fortified-Grid model, we have considered the example of a power quality monitoring system in SCADA of the proposed energy cyber-physical system (E-CPS). Power quality monitoring devices are connected to the network to monitor harmonics, voltage sags swells and unbalances. Here IoT device A connects to measure voltage fluctuations while IoT device B connects to capacitor banks. Here device A continues to monitor the voltages and, if required, instructs device B to take a corrective measure such as switching the capacitor bank and voltage regulator to improve power quality so that the customer receives quality power supply all the time. This type of device integration may be used for another part of SG-CPS.
The Fortified-Grid network model is depicted in Fig.4. Fortified-Grid consists of three entities smart grid IoT devices, Gateway Node (GWN), and server. A certificate authority (CA) is a trusted authority and may be an IoT owner, manufacturer, or trusted third party (TTP). The smart grid IoT entities contain a hardware chip of TPM, which provides true random number generation, cryptographic key generation, secure storage of key, quote, and software state measurement. Here smart grid IoT devices connected via the internet can communicate with each other in real time by establishing a secret session key.

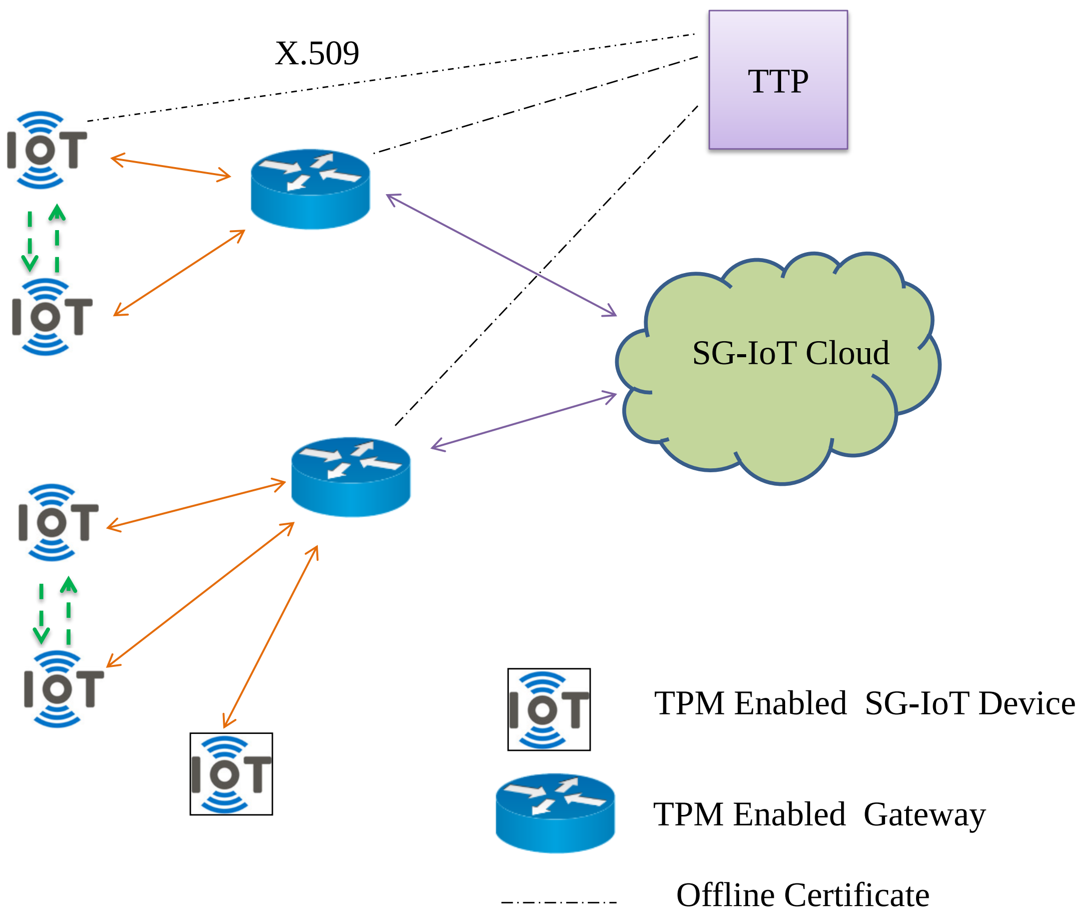

Figure 4. TPM Enabled IoT Smart Grid Network.

Before communicating with other entities, the devices prove their authenticity and integrity to each other. Generally, several schemes adopt certificate-based single-factor authentication, but our protocol considered two-factor authentications where the integrity of local devices is also validated. Only when both credentials are validated a session key is established.

5.2. Assumptions

We have assumed that TCG specifications are truly implemented in our TPM-based proposed scheme. The root of trust management is adopted correctly. We have assumed that the smart gird IoT manufacturer has installed the TPM in devices and certificates. We have also assumed that CA, GWN, and server are trusted entities and secure from internal and external attacks. We have assumed that adversary cannot manipulate the TPM configuration. Further, we have assumed that the devices are physically in accessible and the adversary is unable to perform the side-channel attack.

5.3. Threat Model

Dolev and Yao introduced the Dolev-Yao adversary model in 1983. We consider the two famous Dolev Yao (DY), and Canetti–Krawczyk (CK) adversary models for security analysis in this paper [32]. In the DY model, an adversary has the following capacity and can perform attacks below.

- An adversary can control insecure communication channels of an SG network and hence can eavesdrop, modify, alter, or block transmitted messages at smart grid IoT network.
- An adversary can obtain secrets stored in NVM for smart grid devices via a side-channel attack.
- An adversary can not compromise GWN since it is fully trusted in a smart grid system.
- An adversary can perform clone or physical attacks, a man in the middle and password guessing, etc., except they can not perform cryptanalysis in a smart grid network.

The CK adversary model is more potent than the DY model and popularly used in authentication and key exchange schemes. In addition to the above attacks, the CK adversary model can access ephemeral parameters or secret parameters stored in a memory of an entity via explicit attack. CK adversary model guarantees that information leakage in any session does not affect the security of the next session.

6. Proposed Scheme for TPM-based Authentication in Smart Grid

Table 2 defines the notations used in this scheme. The detailed sequence of the proposed security scheme is shown below. It may be classified into four steps: a) Registration, b) Initialisation, c) Remote attestation, and d) Session key generation. Detailed information about these steps is defined in the subsequent subsection.

Table 2. List of symbols

Symbols	Descriptions
P	Generator point ECC
h	one way hash function
IoT^A, IoT^B	IoT Dev A, B
N_a, N_b	Random number a, b
PCR^A, PCR^B	PCR value of A,B
${PCR_{eve}}^A$, ${PCR_{eve}}^B$	PCR event value of A,B
PCR^A_{rev},PCR^B_{rev}	PCR reference value of A,B
AIK_{pub^A}, AIK_{pub^B}	Attestation Public key of A,B
AIK_{pvt^A}, AIK_{pvt^B}	Attestation Pvt. key of A,B
$cert_A$, $cert_B$	Digital certificate of dev. A ,B
Ta, Tb	Time stamp of A ,B
$dh_A.pub$, $dh_B.pub$	Diffi Helman Public key of A ,B

6.1. Registration phase

During the registration phase, IoT devices in the smart grid obtain a digital certificate from CA offline. The TPM is equipped with Endorsement Key (EK). The attestation key (AIK) is generated using EK.

6.2. Initialisation phase

During the initialisation phase, device A generates random nonce A using TPM and sends it toward device B. Similarly, device B generates nonce Nb and sends it toward device A. Further, both devices generate and transmit PCR event values toward each side.

Algorithm 1 : Initialisation Process

IoT^A: Smart grid IoT device A creates a random nonce N_a and measure PCR event log $PCR_{eve}{}^A$
$IoT^A \rightarrow$IoT^B: N_a , $PCR_{eve}{}^A$
IoT^B: IoT device B creates a random nonce N_b and measure PCR event log $PCR_{eve}{}^B$
$IoT^B \rightarrow$IoT^A: N_b , $PCR_{eve}{}^B$

Algorithm 2 : Authentication Process

IoT^A: Smart gird IoT device A creates a TPM Quote quote$^A = (\mathrm{N}_b \| \mathrm{PCR}^A)_{AIK_{pvt^A}}, cert_A = (AIK_{pub^A})$
$IoT^A \rightarrow$IoT^B: quote^A, PCR^A, $cert_A$, Ta
IoT^B : verify the signature of CA and extracts AIK_{pub^A} from $cert_A$
IoT^B : unsign $quote^A$ and verify $quote^A$ contains expected PCR^A and N_b
IoT^B : verify if event log of PCR^A_{eve} = PCR^A
IoT^B : IoT device B creates a TPM Quote quote$^B = (\mathrm{N}_a \| \mathrm{PCR}^B)_{AIK_{pvt^B}}, cert_B = (AIK_{pub^B})$
$IoT^B \rightarrow$IoT^A: quote^B, $cert_B$, Tb
IoT^A : verify the signature of CA and extracts AIK_{pub^B} from $cert_B$
IoT^A : verify $quote^A$ contains expected PCR^B and N_a
IoT^A : verify if $PCR_{eve}{}^B$ = PCR^B
IoT^A : verify if $\Delta_t \leq Ta - Tb$

Algorithm 3 : Session Key Generation and Exchange

IoT^A: Smart gird IoT device A TPM generates ephemeral key pair dh_A , public part of ephemeral key $dh_A.pub$
IoT^A: calculates secret$^A = (dh_A.pub, N_B)_{AIK_{pvtA}}$

$IoT^A \rightarrow$IoT^B: secret^A,dh$_A.pub$, cert$_A$, Ta
IoT^B : verify the signature of CA and extracts AIK_{pub^A} from $cert_A$
IoT^B : verify $secret^A$ contains expected N_b and $dh_A.pub$
IoT^B : IoT device B TPM generates ephemeral key pair dh_B , public part of ephemeral key $dh_B.pub$
IoT^B : Calculates session key SKba = kdf($dh_B.pvt \; \| dh_A.pub \| N_b \; \| N_a$)
IoT^B: calculates secret$^B = (dh_B.pub, N_A)_{AIK_{pvtB}}$

$IoT^B \rightarrow$IoT^A: secret^B,dh$_B.pub$, cert$_B$, Tb
IoT^A : verify the signature of CA and extracts AIK_{pub^B} from $cert_B$
IoT^A : verify $secret^B$ contains expected N_a and $dh_B.pub$
IoT^A : Calculates session key SKab = kdf($dh_A.pvt \; \| dh_B.pub \| N_a \; \| N_b$)

6.3. Remote attestation phase

The previously exchanged nonce is included in this signature to avoid a replay attack. During this phase, quotes are exchanged and verified. It is done according to the Trusted Computing Group (TCG) protocol [33].
Step 1: Device A, which wants to communicate the B, generates a unique random nonce (Na) and sends it toward B, and makes a request for a PCR event log. Attesting device

PCRs (PCR^A and PCR^B) are extended with measurements. Device B generates a unique random nonce (Nb) PCR event log (PCReveB) and sends it toward A. After that, device A sends the PCR event log (PCReveA) toward B. Finally, both device exchanges none and the PCR event log to each other.
Step 2: IoT device A creates a TPM quote $quote^A$ and sends $quote^A$,PCR^A, $cert_A$ toward

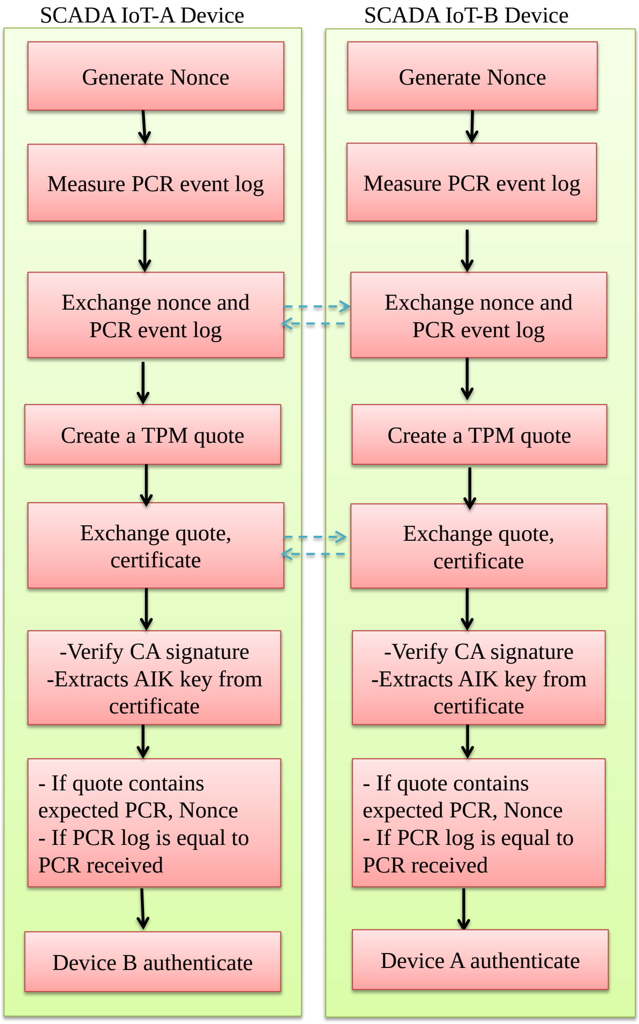

Figure 5. Attestation of SG-IoT devices.

device B.
Step 3: Device B verifies the signature of CA and extracts AIK_{pub^A} from $cert_A$ and unsign $quote^A$ and verify $quote^A$ contains expected PCR^A and N_b. Further verify if event log of $PCR^A_{eve} = PCR^A$
Step 4: Device B transmits $quote^B$, PCR^B, $cert_B$ toward device A.
Step 5: Device A verifies the signature of CA and extracts AIK_{pub^B} from $cert_B$ and unsign $quote^A$ and verify $quote^A$ contains expected PCR^B and N_a.Further verify if event log of $PCR^B_{eve} = PCR^B$
Step 6: Verify if the time difference is within threshold limit $\Delta t \leq$ Ta-Tb.
If the following condition does not satisfy device should not be authenticated:

- The device should not be trusted and discarded if the signature of TPM evidence does not match.
- The device should not be trusted and discarded if the nonce in the quote does not match the original quote, as it may be a replay message.
- The device should not be trusted and discarded if the PCR value received in the quote does not match the PCR evidence log.

- The device should not be trusted and discarded if the time difference Ta or Tb exceeds the threshold limit set for the freshness of messages.

6.4. Session key establishment phase

At first, smart grid device IoT^{A} creates fresh ephemeral key pair using TPM. Ephemeral keys are generated each time a fresh session establish. As ephemeral key pairs are generated inside the TPM, its public part is signed using the attestation key of TPM $AIK_{pvt^{A}}$. Randomly generated previously exchanged nonce is included in the secret parameter to avoid the replay of messages. Finally, device A sends $secret^{A}$,$dh_{A}.pub$, $cert_{A}$ toward device B. Device B checks whether the dh key generated by the trusted system using by verifying the signature with the certificate of device A. Device B also checks the nonce which was earlier sent and generates the session key SKab = kdf($dh_{B}.pvt \; \| dh_{A}.pub \| N_{b} \; \| N_{a}$).Similarly, Device B generates fresh ephemeral pairs using TPM. The signed public part of the pair using AIK Pvt key and sends $secret^{B}$,dh$_{B}.pub$, $cert_{B}$ toward device A. Session key generated using kdf SKab = kdf($dh_{A}.pvt \; \| dh_{B}.pub \| N_{a} \; \| N_{a}$).

7. Security analysis of proposed TPM-based IoT Smart Grid network

The proposed protocol's formal security is examined using the ROR oracle model and the automatic security verification tool AVISPA. In contrast, informal security is examined in various attack situations.

7.1. Security verification using AVISPA tool

We formally verify our security protocol using this subsection's popular AVISPA simulation tool. The role of each entity is defined using the HLPSL programming language.

```
% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSION
S
PROTOCOL
/home/span/span/testsuite/results
/sg.if
GOAL
as specified
BACKEND
OFMC
COMMENTS
STATISTICS
parse time:0.00sec
search Time:0.53sec
visitedNodes:425  Nodes
```

```
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSI
ONS
PROTOCOL
/home/span/span/testsuite/res
ults/sg.if
GOAL
as specified
BACKEND
CL-AtSe
STATISTICS
Analysed: 0 states
Reachable: 0 states
Translation: 0.18 seconds
Computation: 0.00 seconds
```

Figure 6. AVISPA OFMC and CL-Atse

It uses two popular backends for the program's execution, i.e., OFMC and Cl-AtSe. The results show that our protocol is safe. The security of the protocol is verified on both backends. AVISPA shows different security attacks during the protocol simulation in the intruder section if the protocol is unsafe. This protocol uses the Dolev–Yao model as the intruder model [34].

7.2. Formal verification using Random or Real oracle model

Formal security verification is based on the ROR model, which measures protocol security by evaluating the probability of SK cracking on the repeated game round in the smart grid. The proposed ROR model assumes that the adversary $\mathcal{A}$ can interact with other communicating entity Y = (IoT^{A}, IoT^{B}, GWN), here $\prod_{A_i}^{x}$,$\prod_{B_j}^{y}$, $\prod_{G_k}^{z}$ can perform the following queries :

- Send (Y, M): In this query, $\mathcal{A}$ can send message M to Y in the smart grid and receive a specific entity's response.
- Execution (Y): $\mathcal{A}$ uses this query to launch a passive attack in the smart grid. It can eavesdrop on all message transmitted between $\prod_{A_i}^{x}$, $\prod_{B_j}^{y}$ and $\prod_{G_k}^{z}$.
- Reveal (Y): $\mathcal{A}$ can get the session key SK of $\prod_{A_i}^{x}$, $\prod_{B_j}^{y}$ by executing this query.
- Corrupt (Y): If this query is executed, it will get the long-term session key SK in the smart grid.
- Test (Y): $\mathcal{A}$ can send a query to any participant in V2G, and it tosses up a coin. If C=1 $\mathcal{A}$, obtain the correct secret key.If C=0, a randomly selected value of the same bit string equal to SK is returned.

Theorem: Assume that $\mathcal{A}$ is a running polynomial-time adversary and performs the queries, then the probability that $\mathcal{A}$ can break protocol is

$$Adv_{\mathcal{P}}^{SK}(\mathcal{A}) \leq \frac{q_s}{2^{l-2}} + \frac{3q_h^2}{2^l} + 2max\{C^{'}.q_s^{'}, \frac{q_s}{2^l}\}$$

where q_s and q_t indicates the number of send and TPM query respectively, l represent the number of bits and $C^{'}$ is a constant [35].

Proof: We present the proof of theorem with the help of seven game rounds $G_m = \{0,1,2,3,4,5,6\}$. $Succ_P^{G_m}$ indicates the probability of winning in various rounds of the game, and $Adv_{\mathcal{P}}^{SK}$ indicates the advantage of breaking the protocol.

- **Game$_0$** : In the first round of game G_0 does not make any query. The probability of $\mathcal{A}$ successfully cracking is:

$$Adv_{\mathcal{P}}^{SK}(\mathcal{A}) = 2\Pr\left[Succ_P^{G0}\right] - 1. \tag{1}$$

- **Game$_1$** : In this round $Game_1$ performs Execute (Y) operation. $\mathcal{A}$ intercepts only message QuoteA, QuoteB, CertA, CertB transmitted over insecure communication channel. Since the value of dhA.pvt and dhB.pvt are unknown $\mathcal{A}$ can not calculate the secret session key SKab and SKba. Hence probability of $Game_1$ is same as $Game_0$.

$$|\Pr\left[Succ_P^{G1}\right] = \Pr\left[Succ_P^{G0}\right] \tag{2}$$

- **Game$_2$** : In this round $Game_2$ performs Send (Y) operation other than $Game_1$. As per Zipf's law probability of $Game_2$ is

$$|\Pr\left[Succ_P^{G2}\right] - \Pr\left[Succ_P^{G1}\right]| \leq \frac{q_s}{2^l} \tag{3}$$

- **Game$_3$** : In this round $Game_3$ performs one more query (Y) operation and one less operation Send (Y). According to the birthday paradox probability of occurring collusion during the hash query simulation is

$$|\Pr\left[Succ_P^{G3}\right] - \Pr\left[Succ_P^{G2}\right]| \leq \frac{q_t^2}{2^{l+1}} \tag{4}$$

- **Game$_4$** : In this game $\mathcal{A}$ uses $\prod_{A_i}^{x}$,$\prod_{B_j}^{y}$ to acquire the IoT^A or IoT^B secret dh key $dh_A.pvt$. Assume that $\mathcal{A}$ acquire the IoT^A dh key $dh_A.pub$. Because $\mathcal{A}$ can not calculate the value of $dh_A.pvt$, it can not calculate the SK,where SKab = kdf($dh_A.pvt$ $\|dh_B.pub\|N_a$ $\|N_b$). Therefore the probability of $Game_4$ is

$$|\Pr\left[Succ_P^{G4}\right] - \Pr\left[Succ_P^{G3}\right]| \leq \frac{q_s}{2^l} + \frac{q_t^2}{2^{l+1}} \tag{5}$$

- **Game$_5$** : $\mathcal{A}$ uses Corrupt (Y) to capture the parameters in $secret^A$ is $dh_B.pub$,N_A. Therefore the probability of $Game_5$ is

$$|\Pr\Big[Succ_P^{G5}\Big] - \Pr\Big[Succ_P^{G4}\Big]| \leq max\{C^{'}.q_s^{'}, \frac{q_s}{2^l}\} \tag{6}$$

- **Game$_6$** : In this game, $\mathcal{A}$ can guess session key SKab and SKba. The session key remains independent from oracle and other parameters. Hence the probability of $Game_6$ is

$$|\Pr\Big[Succ_P^{G6}\Big] - \Pr\Big[Succ_P^{G5}\Big]| \leq \frac{q_t^2}{2^{l+1}} \tag{7}$$

Hence the probability that $\mathcal{A}$ can guess is

$$|\Pr\Big[Succ_P^{G6}\Big]| = \frac{1}{2} \tag{8}$$

based on equation (1) - (8), we obtain the following result

$$\begin{aligned}
\frac{1}{2}Adv_{\mathcal{P}}^{SK}(\mathcal{A}) =& |\Pr[Succ_P^{G0}] - 1/2.| \\
=& |\Pr[Succ_P^{G0}] - \Pr[Succ_P^{G6}]| \\
=& |\Pr[Succ_P^{G1}] - \Pr[Succ_P^{G6}(\mathcal{A})]| \\
\leq& \sum_{n=0}^{5} \Pr[Succ_P^{G_{n+1}}(\mathcal{A})] - \Pr[Succ_P^{G_n}(\mathcal{A})] \\
=& \frac{q_s}{2^{l-1}} + \frac{3q_t^2}{2^l} + max\{C^{'}.q_s^{'}, \frac{q_s}{2^l}\}
\end{aligned} \tag{9}$$

Based on equations (1) -(8), we got (10), which proves the theorem.

$$Adv_{\mathcal{P}}^{SK}(\mathcal{A}) \leq \frac{q_s}{2^{l-2}} + \frac{3q_t^2}{2^l} + 2max\{C^{'}.q_s^{'}, \frac{q_s}{2^l}\} \tag{10}$$

7.3. Informal security analysis :

This section examines several security threats using the informal security analysis, which is extensively used to demonstrate the cryptographic protocol's features. The protocol can withstand numerous attacks, such as replay, man-in-the-middle, impersonation, and anonymity attacks.

Preposition 1: The proposed scheme can mitigate Man in middle attacks.

Proof :- During a MiTM attack, an intruder in smart gird inserts themselves between IoT^A and IoT^B message exchanges and obtains control of their communication. Suppose an intruder intercepts relayed transmissions and attempts to alter $quote^A$,PCR^A, $certA$ or $quote^B$, PCR^B, $certB$ by impersonating a legal entity in front of the other. This is not possible until the adversary obtains the ($quote^A$ or $certA$) of the IoT^A / IoT^B. Without knowledge of the quote, an adversary can not calculate PCR. Further, authentication is terminated if N_a, N_b is not the same. Consequently, the adversary cannot perform the MITM attack under the analyzed scenarios.

Preposition 2: The proposed scheme can resist the replay attack

Proof:- In this attack, an intruder can not use the message $quote^A$ or $quote^B$ as N_a / N_b and Ta, Tb changes in each session; hence the adversary can not reuse message $quote^A$ or $quote^B$ in each session, as new quote message is generated.

Preposition 3 : The proposed protocol can ensure message integrity

Proof:- In the smart grid, IoT^A and IoT^B generate a new session key in each session. IoT^A and IoT^B produce fresh (dhA, dhB, N_a, N_b) and new timestamps (Ta, Tb). The message confirms the integrity and authentication of the message data transmission.

Preposition 4: The proposed protocol can mitigate DoS attack

Proof:- In this attack, an adversary may flood the network by delivering unwanted and bogus packets to all protocol entities of smart gird. In our proposed scheme, every entity immediately verifies the received messages by bogus messages and checks the freshness of the timestamp. IoT^A and IoT^B generate a new session key in each session. IoT^A and IoT^B produce fresh (N_a , N_b) and new timestamps (Ta, Tb). Hence protect against DOS attack.

Preposition 5:The proposed protocol is resilient against backward and forward key secrecy

Proof:- Only a legitimate IoT^A can generate $dh_A.pvt$, hence calculating fresh SKab = kdf($dh_A.pvt \,\|dh_B.pub\|N_a \,\|N_b$) . Similarly, legitimate IoT^B can generate fresh SKba = kdf($dh_B.pvt \,\|dh_A.pub\|N_b \,\|N_a$). If any session key is compromised, it does not help to recover the past or future session keys. Hence it provides session key security against any attack.

Preposition 6 :The proposed protocol support anonymity

Proof:- Anonymity means the identity of the IoT^A and IoT^B is not disclosed during communication. In TPM-SGIoT, every IoT^A and IoT^A have TPM, which generates unique AIK during registration with GWN, and the key is not transmitted during communication. More ever, the dh of IoT^A and IoT^B is different in each session. Thus an adversary can not identify the same IoT^A or IoT^B in a different session.

8. Experimental Results

This section provides a detailed comparison of the computational and communication overheads of various schemes. Specifically, it focuses on comparing the computational costs of different schemes. The computations involving large integers are performed using GMP library version 6.1.2, while pairing calculations utilize PBC library version 0.5.14. The experimental setup employs Ubuntu 16.04 as the operating system, an Intel Core i7-6700 CPU running at 4GHz, and a memory capacity of 16GB.

Table 3. Execution time of different cryptographic operation

Cryptographic operation	Time (μs)
Hash (Th)	0.138
Random Number (Trng)	0.535
Encryption (Te)	4.420
Decryption (Td)	4.420
Bilinear pairing (Tbp)	42.11

Table 3 shows some basic operation execution times, Table 4 shows comparison of the computation overhead, while Table 5 shows comparison of the communicational overheads of different schemes.

8.1. Computational overhead analysis

In this subsection we compare our scheme computational cost with [18],[19],[22] and [25]. To achieve authentication, scheme [18] will cost 6Te+3Th = 23.75 μs. Scheme [19] will cost 2Tbp+3Th = 84.48 μs. Similarly scheme [22] will cost 12Tem+23Th = 56.26 μs and scheme [25] will cost 4Trn+6Te+6Td+2Th = 37.78 μs respectively.
The propose scheme will cost 4Trn+4Te+4Td = 37.78 μs. However, the computational cost of our scheme is more than the scheme of [18], but our scheme has the added advantage of the TPM-IoT security layer for a secure smart grid network.

Table 4. Computational Cost Comparison.

Scheme	Authentication cost	Session cost	**Total cost (μs)**
Zhang, et al. [18]	5Te+2Th	Te+Th	23.75
Zhong, et al. [19]	2Tbp+Th	2Th	84.48
Wazid, et al. [22]	6Tem+11Th	6Tem+12Th	56.26
Khurshid, et al. [25]	2Trn+3Te+3Td	2Trn+3Te+3Td+2Th	55.18
Fortified-Grid	2Trn+2Te+2Td	2Trn+2Te+2Td+2Th	**37.78**

8.2. Communicational overhead analysis

As mention earlier, the certificate cost is 160 bits, the timestamp 32 bits, the secret concatenation (quote and secret) 160 bits, the random nonce 160 bits, and the public DH key is 320 bits. The communication cost of our scheme Fortified-Grid and other popular schemes is shown in Table 5. In this subsection, the Fortified-Grid communicational cost is compared with [18],[19],[22] and [25] a for the attestation and key procedures. The communication cost of scheme [22] will be 2176 bits and scheme [18] cost will be 672 bits. Similarly scheme [19] cost will be 2848 bits while scheme [25] cost will be 2800 bits.
In Fortified-Grid, during authentication quotes, PCR and certificates are exchanged. Hence overhead A to B (160+32+160) =352 bits, and similarly, B to A is (160+32+160) =352 bits. During a key exchange between A and B, overhead is (160+160+320)=640 bits. Hence total overhead on both sides is 1280 bits. As a result, the total communication overhead in our scheme is (704+1280=1984 bits). The communication cost of our scheme Fortified-Grid is less than the scheme of [22], [19], [25]. However, it is more than the scheme of [18].

Table 5. Communication Cost Comparison

Scheme	**Total cost (bits)**
Zhang, et al. [18]	672
Zhong, et al. [19]	2848
Wazid, et al. [22]	2176
Khurshid, et al. [25]	2368
Fortified-Grid	**1984**

However, it has added the advantage of the TPM-IoT security layer for a secure smart grid network. The results show that our scheme provides security against all major attacks.

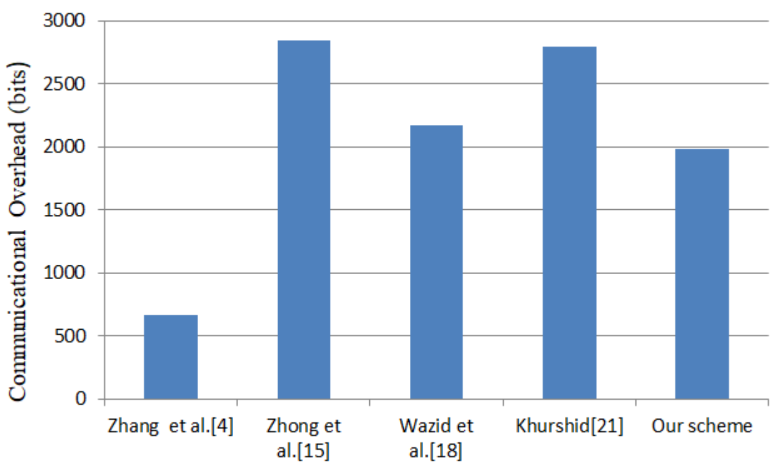

Figure 7. Comparison of Smart Grid IoT overhead

8.3. Discussion

This subsection presents the challenges, advantages and limitation of the proposed TPM based attestation scheme.

- The major challenges for secure IoT redeployment in smart gird are secret key leakage, firmware compromise and hardware based route of trust. To mitigate these challenges, we propose a X.509 certificate based TPM protocol.
- The proposed scheme addresses the hardware security, secret key storage, integrity measurement and remote firmware up-gradation challenges. TPM Protects form ransomware or any other kind of hacks and malware.
- However scheme have limitation such as dynamic addition of new node,TPM is unsuitable for resource constraints devices due to space, power, and cost limitations. Researches are needed to reduce the cost and power consumption for wide application of TPM in security. A trusted third party or certificate authority (CA) is required for validation of digital certificate X.509. The results are also compared with other state-of-the-art methods, where our proposed model outperforms other related work in terms of computational overheads and robustness.

9. Conclusion

This paper presents a smart grid security framework through the integration of TPM in IoT devices. TPM prevents malicious modification in firmware during the secure boot and authentication process. This framework relies on the IETF RATS attestation scheme based on TPM2.0 to generate integrity proof and evidence and utilizes X.509 certificates that are loaded into the TPM of IoT devices for authentication and session key generation. The certificates for IoT devices are created by the TTP's using a private key only. The security advantages of integrating TPM in IoT devices also open the potential for more widespread use in other CPS. We have proposed integrating the Fortify-Grid mechanisms into existing standards to facilitate its adoption in the emerging smart grid.
The threat model uses the CK adversary and ROR model for security verification. A detailed security analysis using the ROR model, AVSIPA, and CK adversary model shows that our proposed scheme is safe against attacks such as man in the middle, replay, denial of service, etc. In addition, integrity measurements are only maintained in Fortify-Grid, whereas other compared schemes do not fulfill these requirements. Our scheme's computational overhead is less than other popular schemes with enhanced security.

Acknowledgement

The authors thank SMDP-C2SD Lab, Malaviya National Institute of Technology Jaipur, and Visvesvaraya PhD. Scheme of (MeiTY) Ministry of Electronics & IT, Govt. of India for supporting simulation tools to perform the experiments. The results of the research work are carried out at SMDP-C2SD Lab, MNIT Jaipur.

Compliance with Ethical Standards

The authors declare that they have no conflict of interest and there was no human or animal testing or participation involved in this research. All data were obtained from public domain sources.

References

1. Wang, B.; Ma, H.; Wang, F.; Dampage, U.; Al-Dhaifallah, M.; Ali, Z. M.; Mohamed; M. A. : An IoT-Enabled Stochastic Operation Management Framework for Smart Grids. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24* , 1025–1034.
2. Sharma, G.; Joshi, A.M.; Mohanty, S.P. An efficient physically unclonable function based authentication scheme for V2G network. In Proceedings of the IEEE International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS), Jaipur, India, 2021, pp. 421-425.
3. Kim, Y.; Hakak, S.; Ghorbani, A. Smart grid security: Attacks and defence techniques. *IET Smart Grid* **2022**,*6*, 103–123.

4. Kim, K.T., Lim, J.D. and Kim, J.N., 2022, February. An iot device-trusted remote attestation framework. In 2022 24th International Conference on Advanced Communication Technology (ICACT) (pp. 218-223). IEEE.
5. D. G. Berbecaru and S. Sisinni, "Counteracting software integrity attacks on IoT devices with remote attestation: a prototype," 2022 26th International Conference on System Theory, Control and Computing (ICSTCC), Sinaia, Romania, 2022, pp. 380-385
6. Jain, A. and Joshi, A.M. Device authentication in IoT using reconfigurable PUF. In Proceedings of the 2nd IEEE Middle East and North Africa COMMunications Conference (MENACOMM), India, 2019, pp. 1-4 .
7. Sharma, G.; Joshi, A.M.; Mohanty, S.P. sTrade: Blockchain based secure energy trading using vehicle-to-grid mutual authentication in smart transportation. *Sustainable Energy Technologies and Assessments* **2023** *57*, 103296.
8. Bathalapalli, V.K., Mohanty, S.P., Kougianos, E., Iyer, V. and Rout, B., 2023, June. PUFchain 4.0: Integrating PUF-based TPM in Distributed Ledger for Security-by-Design of IoT. In Proceedings of the Great Lakes Symposium on VLSI 2023 (pp. 231-236).
9. Goudarzi, A.; Ghayoor, F.; Waseem, M.; Fahad, S.; Traore, I. A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook. *Energies* **2022** *15(19)*, 6984-6994.
10. W. -Y. Chiu, W. Meng and W. Li, "TPMWallet: Towards Blockchain Hardware Wallet using Trusted Platform Module in IoT," 2023 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 2023, pp. 336-342.
11. Jain, H.; Kumar, M.; Joshi, A.M. Intelligent energy cyber physical systems (iECPS) for reliable smart grid against energy theft and false data injection., *Electrical Engineering* **2021**, 1-16 .
12. Sharma, R.; Joshi, A.M.; Sahu, C.; Sharma, G.; Akindeji, K.T.; Sharma, S., Semi Supervised Cyber Attack Detection System For Smart Grid. In Proceedings of the 30th Southern African Universities Power Engineering Conference (SAUPEC), 2022, pp. 1-5.
13. Zhu, Q., Multilayer cyber-physical security and resilience for smart grid., *Smart grid control: overview and research opportunities*, **2019** 225-239.
14. Haggi, H., Song, M. and Sun, W.,A review of smart grid restoration to enhance cyber-physical system resilience., In Proceedings of the IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia), pp.4008-4013 2019.
15. Puthal, D ; Mohanty, S.P. Proof of authentication: IoT-friendly blockchains., *IEEE Potentials* **2018** *,38(1)*, pp.26-29 .
16. Xu, L., Guo, Q., Yang, T. and Sun, H., Robust routing optimization for smart grids considering cyber-physical interdependence., *IEEE Trans. Smart Grid* **2018**, *10(5)*, 5620-5629.
17. Halle, P.D.; Shiyamala, S., Secure advance metering infrastructure protocol for smart grid power system enabled by the Internet of Things., *Microprocessors and Microsystems* **2022**, *95*, 104708-104718.
18. Zhang, J.; Cui, J., Zhong ; H., Chen, Z.; Liu, L. PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. *IEEE Trans. Dependable Secure Comput.***2019**, *18(2)*, 722-735.
19. Zhong, H.; Cao, W.; Zhang, Q.; Zhang, J.; Cui, J. Toward trusted and secure communication among multiple internal modules in CAV., *IEEE Internet Things J* **2021**,*8(24)*,.17734-17746.
20. Fuchs, A.; Kern, D.; Krauß, C.; Zhdanova, M. HIP: HSM-based identities for plug-and-charge., In Proceedings of the 15th International Conference on Availability, Reliability and Security , pp. 1-6 2020.
21. Dave, A.; Wiseman, M.; Safford, D.; SEDAT: Security Enhanced Device Attestation with TPM2. 0. arXiv preprint arXiv:2101.06362 **2021**.
22. Wazid, M.; Das, A.K.; Shetty, S. TACAS-IoT: Trust Aggregation Certificate-Based Authentication Scheme for Edge-Enabled IoT Systems., *IEEE Internet Things J***2022**, *9(22)*, 22643-22656
23. Chen, L.; Qian, S.; Lim, M.; Wang, S. An enhanced direct anonymous attestation scheme with mutual authentication for network-connected UAV communication systems., *China communications* **2018**, *15(5)*,61-76.
24. Kabir, S.; Gope, P.; Mohanty, S.P. A Security-enabled Safety Assurance Framework for IoT-based Smart Homes. *IEEE Trans. Ind. Appl.* **2022**, *59(1)*, 6-14
25. Khurshid, A.; Raza, S. AutoCert: Automated TOCTOU-secure digital certification for IoT with combined authentication and assurance., *Computers & Security* **2023** *,124*, 102952-102962.
26. Huang, H.F. and Liu, K.C., A new dynamic access control in wireless sensor networks. In Proceedings of the IEEE Asia-Pacific Services Computing Conference (pp. 901-906). 2008.

27. Kim, H.S.; Lee, S.W. Enhanced novel access control protocol over wireless sensor networks. *IEEE Trans. Consum. Electron.***2009**, *55(2)*, 492-498
28. Broström, T.; Zhu, J.; Robucci, R.; Younis, M., IoT boot integrity measuring and reporting.*ACM SIGBED Review***2018**, *15(5)*, 14-21 .
29. Kuang, B.; Fu, A.; Susilo, W.; Yu, S.; Gao, Y. A survey of remote attestation in Internet of Things: Attacks, countermeasures, and prospects. *Computers & Security* **2022**, *112*, p.102498.
30. Biswas, S.; Sharif, K.; Li, F.; Maharjan, S.; Mohanty, S.P. ;Wang, Y. PoBT: A lightweight consensus algorithm for scalable IoT business blockchain., *IEEE Internet Things J* **2019**, *7(3)*, 2343-2355 .
31. Puthal, D.; Obaidat, M.S.; Nanda, P., Prasad; M., Mohanty; S.P. ; Zomaya, A.Y. Secure and sustainable load balancing of edge data centers in fog computing., IEEE Communications Magazine, 56(5), pp.60-65 (2018).
32. Shen, J.; Zhou, T.; Wei, F., Sun; X. and Xiang; Y. Privacy-preserving and lightweight key agreement protocol for V2G in the social Internet of Things., *IEEE Internet Things J* **2017**, *5(4)*, 2526-2536.
33. TPM, T.,2.0 Automotive Thin Profile For TPM Family 2.0. **2018**.
34. Armando, A.; Basin, D., Boichut; Y., Chevalier, Y.; Compagna, L.; Cuéllar, J.; Drielsma, P.H.; Héam, P.C., Kouchnarenko, O.; Mantovani, J.; Mödersheim, S.,The AVISPA tool for the automated validation of internet security protocols and applications. In Computer Aided Verification: In Proceedings of the 17th International Conference, CAV 2005, Edinburgh, Scotland, UK, pp. 281-285 (2005).
35. Malani, S.; Srinivas, J.; Das, A.K.; Srinathan, K.; Jo, M. Certificate-based anonymous device access control scheme for IoT environment. *IEEE Internet Things J* **2019**, 9762-73.