



# An Efficient ARIA-RSA-SHA256 Hybridized Encryption Algorithm for Metering Data in Smart Grid Network Systems

Anita Philips\*, Dr. J. Jayakumar\*\*

\*Dept. of Electrical & Electronics, Karunya University, Coimbatore 641114, India

\*\*Dept. of Electrical & Electronics, Karunya University, Coimbatore 641114, India

(anucornee@yahoo.com, jayakumar@karunya.edu)

‡Corresponding author: Anita Philips, Dept. of Electrical & Electronics, Karunya University, Coimbatore 641114, India Tel.: +91 9944033545; E-mail address: anucornee@yahoo.com

*Received: 07.03.2023 Accepted:01.05.2023*

**Abstract** - Digitizing the traditional electrical power grid and transitioning the grid operations to Smart Grid functionalities could yield very efficient results. Despite all the advantages, smart grid networks pose a serious threat of cyber-attacks emerging at the various nodes of the system. The cyber threat models could vary from a minimal effect on the system to even massive power outages disrupting the entire system. One of the vulnerable and crucial nodes of the smart grid where security breaches can occur is the Advanced Metering Infrastructure component of the smart grid. Hence, it becomes essential for efficient security protocols in place, to secure the metering data originating from the consumer premises through smart meters. In this paper, we have explored the cryptographic encryption algorithms, which are most effective in securely transmitting data from smart meters to utility centers and vice versa. In particular, using the approach of combining the strengths of asymmetric and asymmetric public key algorithms to provide hybrid functionalities is very efficient in Internet of Things (IoT) systems. Therefore, in this research work, we propose an enhanced hybrid security protocol with ARIA encryption algorithm and Rivest–Shamir–Adleman (RSA) key encryption algorithm with SHA256 hash digital signature for the secure transmission of metering data in smart grid networks. The results of this hybrid application in smart grids show significant improvement in the defined performance metrics.

**Keywords** - Cyber security; Hybrid security; Symmetric encryption; Asymmetric encryption; ARIA encryption algorithm; RSA cryptographic algorithm; Digital Signature; Advanced metering infrastructure; Smart grid

## 1. Introduction

The current electrical grid system exists in its four major components and functionalities namely power generation, transmission, distribution and energy consumption. Replacing the traditional grid with smart technologies are widespread now, which successfully provides intelligent predictive analytics on the end-to-end data and operations and establish a drastic price reduction in generation and consumption along with meeting the perfect energy demand-supply balance.

The Smart Grid (SG) system includes automation and controllable power devices in the whole energy value chain

from production to consumption. Particularly, the computing and two-way communication capabilities of the SG aids to exchange real-time information between utilities and consumers, thus achieving the desirable balance of energy supply and demand. During this communication life cycle of SG, and the energy transfer from production to user, the utility companies receive information like current electricity consumption and the amount of transferred potential energy. This information will be crucial for forecasting the times of high demand, detect power failure and save excess power thus meeting the energy demands efficiently. State of the art technologies in Grid systems and recent developments in SG research are listed in [1]. SG networks are playing a crucial

role in today's energy sector, as many countries are fully digitizing the electrical grid system in a fast pace. Consequently, the Advanced Metering Infrastructure (AMI) of the SGs becomes a vital element of concern, as they record the consumption data in real time. The crucial component of the SG network is the AMI as this houses the critical data required for the successful operation of the entire SG network [2]. The AMI is comprised of smart meters, data collectors, and communications network. AMI transmits the user's electricity consumption information to the Meter Data Management System (MDMS) or other data management systems. The consumption component of the SG comprises of the smart meter which is deployed in the consumer premises and transmits control data and consumption data to and from the utility center [3] as shown in Fig 1.

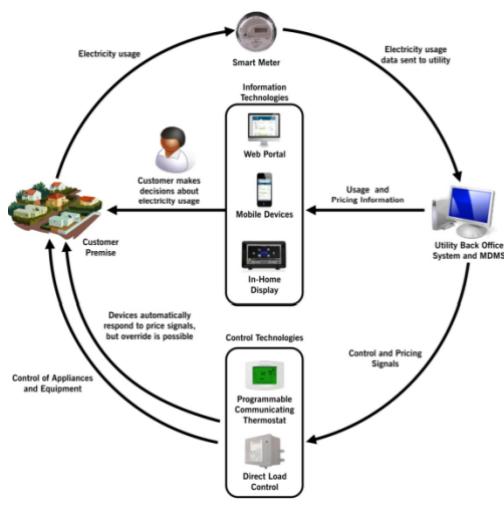


Fig 1. Data flow in AMI [4]

Despite the advantages of the AMI in the customer premises to collect and transmit the real time energy consumption related data, there are accompanying cyber security challenges to meet. Thus, advantages and challenges in the context of AMI were analysed in [5]. In [6], a novel cybersecurity model for wireless communication networks is proposed to discuss the threats and security attacks. Similarly, applicable solutions are discussed in [7], to prevent possible vulnerabilities and attacks in the Smart Grid. Cryptography algorithms are the most common and effective techniques used for data encryption. The two basic types of encryption are symmetric algorithm that uses a single key for encryption and decryption and asymmetric algorithm that uses both public and private keys for encrypting and decrypting respectively. In the existing literature, the approach of combining the strengths of asymmetric and asymmetric public key algorithms to provide hybrid functionalities is proved very efficient. For example, in [2], the authors have suggested the hybrid encryption architecture for SG using the Blowfish, RSA, and MD5 algorithms where the data is encrypted using Blowfish and the

secret key of the Blowfish is encrypted using the RSA algorithm. The challenge in this work is that the Blowfish symmetric algorithm has a smaller flexible block size of 64 bits and the MD5 hash is significantly known for collision attacks. Another work of a lightweight authentication scheme is proposed in [3] where AES and RSA are used for session key generation followed by message authentication using hash-based functions. Here, the hybrid authentication scheme is efficient, however, the lightweight capabilities of AES can be enhanced in the ARIA algorithm. To overcome the above-said weaknesses, a hybrid protocol of combining the ARIA symmetric algorithm with RSA key encryption and digital signature using SHA256 proves to be efficient. Therefore, in our proposed research work, we have explored the following significant research ideas related to the secure transmission of metering data in a smart grid using a novel hybrid security protocol.

- Application of the ARIA algorithm, a symmetric encryption algorithm authorised in the South Korean industry and similar to the Advanced Encryption Standard (AES) technique but with the additional functionality of two S-boxes.
- The message encryption from the consumer smart meters established with the ARIA symmetric algorithm.
- RSA public key encryption algorithm applied for the key encryption.
- Additional security with digital signature using hash value generated with SHA256 hash function.
- Combination of the ARIA symmetric algorithm with the RSA key encryption algorithm and SHA256 digital signature to provide an efficient hybrid security protocol for the metering data transmission in SG.

The paper is further organised as follows. Section II summarizes the related works in this research area. Section III describes the technical background of the proposed concept. Section IV explains the proposed hybrid methodology for securing the metering data of SGs. Section V shows the results of the experiments and further discussion. Section VI concludes the paper.

## 2. Related Works

Various hybrid security architectures remain in literature for achieving end-to-end security in smart grids. For example, in [8], the authors have suggested the hybrid encryption architecture for SG using the Blowfish, RSA and MD5 algorithms. Here, the data is encrypted using Blowfish and the secret key of the Blowfish is encrypted using RSA algorithm. Further, to add the functionality of data integrity, a one-way hash function using MD5 is utilised. Another hybrid encryption scheme for SG is proposed in [9] where public and symmetric encryption algorithms are used in combination. AES and Elliptic curve integrated encryption scheme (ECIES) with a precomputation step are used to provide faster encryption along with data integrity and confidentiality. In the hybrid architecture proposed in [10], the complexity of RSA is combined with the ElGamal algorithm with Euclidean

inverse modulo process to provide faster and efficient encryption.

In the hybrid protocol suggested in [11], the mutual authentication between smart meters is achieved using Diffie-Hellman exchange protocol followed by hash techniques for message authentication. A digital envelop is obtained in [12], where the data encapsulation is achieved using the symmetric AES algorithm and the key encapsulation is achieved using the public ECC encryption algorithm. Here, the strengths of asymmetric and symmetric algorithms are used to provide efficient hybrid crypto-systems. In [13], the Binary phase shift keying (BPSK) method is combined with RSA encryption, where the data from smart meters is encrypted with RSA and is transmitted with BPSK to the utility centres. A lightweight authentication scheme is proposed in [14] where AES and RSA are used for session key generation followed by message authentication using hash based functions. In [15], a trusted third party server is constituted with one server used for data encryption and another server for data transmission. Here, vector machine-learning algorithm establishes the node-to-node authentication of SG network.

The hybrid protocol suggested by authors in [16] uses a Elliptic curve based key authentication and key agreement scheme for SG which results in improvement of communication and computation costs and execution time. An identity based sign-cryption scheme is proposed in [17] to improve the performance in terms of computational overhead and cipher text size. The authors in [18] suggest a hybrid security protocol for the unicast, multicast and broadcast communication of the AMI of SG using public key cryptography and symmetric key encryption. The multi-hop property of Wireless Mesh Networks (WMN) is used along with symmetric encryption algorithm for the message authentication code to establish a secure protocol for SG communication in [19]. Utilising the lower key sizes of Elliptic Curve Cryptography (ECC) in [20], a lightweight authentication scheme is proposed to provide secure SG communication with reduced costs.

Owing to the enhanced benefits of the hybrid approaches in establishing security goals, many hybrid architectures find application in various Internet of Things (IoT) systems. The most common security algorithms used in hybrid approaches are identified as AES symmetric encryption and ECC public encryption system [21]. Similarly, another study shows that the ECC is a common and successful asymmetric algorithm in terms of less computational overhead [22]. However, the combination of RSA algorithm with other symmetric algorithms also is popular due to the significant improvement in the encryption strength as the key length increases [23]. On intense review of the literature, many combinational approaches are tested and proved to establish security in metering infrastructure of SGs. Some of the existing works on hybrid security protocols in SG are listed in Table 1.

Related work	Security algorithms / protocols proposed	Significant performance metrics / security feature achieved
D. M. Menon and N. Radhika [2015]	Blowfish, RSA and MD5 algorithms	Data Integrity
S. Khasawneh and M. Kadoch [2018]	AES and Elliptic curve integrated encryption scheme (ECIES)	Data Integrity and Confidentiality
Preethi S., et al [2015]	RSA with ElGamal algorithm	Encryption speed
M. M. Fouda et al [2011]	Diffie-Hellman exchange protocol followed by hash techniques	Message Authentication
S. Khasawneh and M. Kadoch [2017]	AES algorithm and the public ECC encryption algorithm	Data and key encapsulation
A. K. Asundi et al [2019]	Binary phase shift keying (BPSK) method combined with RSA encryption	Encryption strength and speed
K. Mahmood et al [2016]	AES and RSA followed by hash based functions.	Message authentication
I. Parvez, M. Aghili, and A. Sarwat [2017]	Dual servers with vector machine learning algorithm	Node-to-node authentication
D. Abbasinezhad-Mood and M. Nikooghadam [2018]	Elliptic curve based key authentication and key agreement scheme	Computation cost and execution time
K. Alharbi and X. Lin [2016]	Identity based sign-cryption scheme	Computation overhead

**Table 1.** Hybrid security protocols in SG

Related work	Security algorithms / protocols proposed	Significant performance metrics / security feature achieved
N. George, S. Nithin, and S. K. Kottayil [2016]	Public key cryptography and symmetric key encryption	For unicast, multicast and broadcast communications
T. Rizzetti et al [2018]	Multi-hop property of Wireless Mesh Networks (WMN) with symmetric encryption algorithm	Message authentication
K. Mahmood et al [2017]	Elliptic Curve Cryptography (ECC) based algorithm	Lightweight authentication scheme

The hybrid approaches overcome the weaknesses of the symmetric algorithm in which secure key distribution can be difficult and that of the asymmetric algorithm which can result in high computational complexity and time. Hence, combining certain features of both types of algorithms could prove to provide improvement in speed, better key management and a more secure system, especially in SG, which collects and transmits critical real-time consumption data.

### 3. Background

In general, the three core security goals of data security are as listed below

1. Confidentiality – Only authorized parties can access computer-related assets.
2. Integrity – Modifications permitted only for authorized parties or through authorized ways.
3. Availability – Assets are accessible to authorized parties at appropriate times.

Together these principles provide reliable access to appropriate information for the authorized people, applications, and machines. The prominent threat in AMI is identified as the cyber security attacks, which may lead to data leakage, privacy breach and even compromising of the smart meters [24]. Therefore, it becomes essential to have proven security protocols in place to ensure smooth transmission of data from the consumer end to the utility centres, which in turn will provide prefect energy supply-demand balance [25] [26]. The authentication and access control measures are to be

established in any system to meet the security challenges [27] that may be classified as in Table 2.

Table 2. Description of attack models

Type of threat	Security property violated	Description of the threat
Spoofing	Authentication / Confidentiality	Impersonates an authorized device or person
Traffic analysis	Confidentiality	Passive attack to analyse network traffic patterns
Information disclosure	Confidentiality	Providing information to unauthorized parties
Modification	Integrity	Unauthorized modification of data
Masquerading	Integrity	Identity theft to enable data theft
Reply attack	Integrity	Delay, repeat or replay a valid transmission of data
Repudiation	Non-repudiation	Entity denies the action / transaction performed
Tampering with data	Integrity	Modifying data on physical devices, memory etc.
Denial of Service (DoS) / Distributed DoS	Availability	Makes services inaccessible to authorized users
Elevation of privilege	Authorization	Providing higher access to unauthorized users

The basic and fundamental goal of cryptography is to establish confidentiality of data or information transmitted through encryption methods. An encryption algorithm is a mathematical procedure for performing encryption on data with an algorithm in which the information changed into meaningless cipher text and requires the use of a key to transform the data back into its original form. The successful operation of the encryption algorithms in terms of computation speed, complexity, and efficient security of data solely depends on the management of cryptographic keys. Therefore, cryptographic encryption algorithms are one of the most popular technologies used to provide the data security goals in the AMI. Here, the adversaries may pose the most destructive active attack in which the data itself modified to produce injected false data or a passive attack where the data stolen and the customer privacy is at risk. The common cyber-attacks that can happen during the encryption process of the data transmission are illustrated in Fig 2.

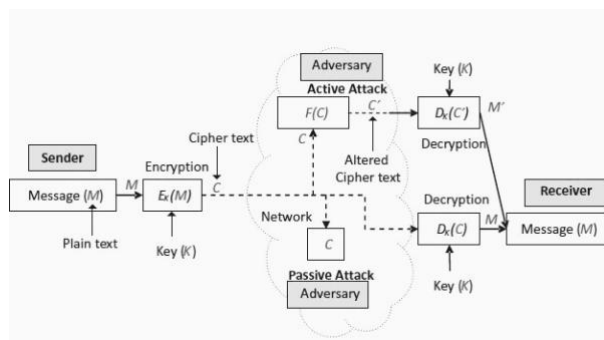


Fig 2. Possible threats in encryption [28]

In general, cryptography plays a major role in network security and the basic goals are the accomplishment of data confidentiality, data authentication, data integrity, non-repudiation and access control in any smart / digital communication [29]. For achieving these goals, either symmetric or asymmetric encryption algorithms are applied based on the performance metric which are required the most for any particular smart environment. For example, the SG networks mainly depend on the customer premises smart meter for recording the consumption data, which requires secure transmission to the utility centres. Any type of cyber-attacks like device tampering, false data injection, data leakage, data misuse and denial of service attacks could lead to erroneous data transmission, which in turn will disrupt the supply demand balance of the entire SG system significantly. Hence, utmost secure encryption protocols need to be in place to ensure data integrity and authentication in such systems. The common features of symmetric and asymmetric encryption algorithms are shown in the following Table 3.

Table 3. Symmetric vs Asymmetric key encryption

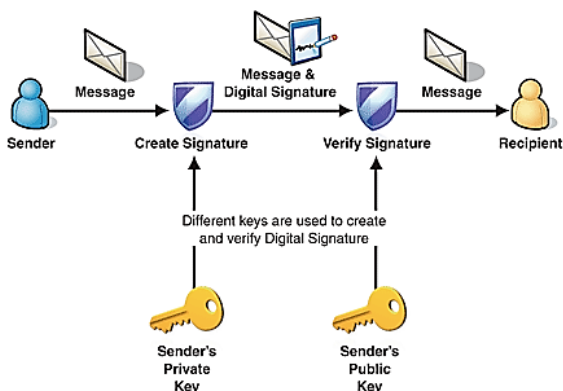
Attributes	Symmetric	Asymmetric
<b>Keys</b>	Single key is shared between all parties	One party has a public key, other party has the private key
<b>Key Exchange</b>	Out-of-band	Symmetric key is encrypted and sent with the message, so the key is distributed by in-bound means
<b>Speed</b>	Less complex algorithm and faster	Complex algorithm and slower
<b>Number of Keys</b>	Grows exponentially as users grow	Grows linearly as users grow
<b>Use</b>	Bulk encryption like databases, files and communication paths	Key encryption and distributing keys
<b>Security entity provided</b>	Confidentiality	Confidentiality, integration, authentication and non-repudiation

Symmetric key encryption algorithms can be utilised for applications like database encryption, sender identity validation, pseudo-random number generation and hashing [30]. As symmetric algorithms use a single key for the encryption / decryption processes, the strength of security wholly depends on the nature of the cryptographic key and the key lengths. Block ciphers that act on fixed size block of data are the common type of symmetric algorithm used for most applications. The key sizes and the block sizes should be adequately large enough to provide stronger security, at the same time balancing the computation complexity. The most popular symmetric algorithms are Data Encryption Standard (DES), (AES), 3DES, Rivest Cipher 4 RC4, RC5 and Blowfish algorithms.

Public key cryptography or asymmetric encryption techniques are mainly used to provide digital signatures to the messages transmitted assuring the data security entities of data integrity, non-repudiation and data authentication [31]. Data integrity ensures that the message received at the utility end is real, accurate, and unaltered by any adversaries or unauthorised parties through security threats like man-in-the-

middle attacks. Data authentication verifies the sender and ensures that the message is from the reliable source that is from the respective smart meters in the case of SG systems. Non-repudiation assures that the source cannot deny that the message originated from them and their participation in the transaction, thereby ensuring authenticity.

Of the two keys generated in public key algorithms, the sender encrypts the message by using the digital signature created with their own private key. On the receiving end, the digital signature is used to verify and decrypt by using the sender's public key. Finally, the signature-verifying algorithm executed to ensure data integrity. The commonly used asymmetric algorithms are Rivest-Shamir-Adleman (RSA), Diffie-hellmann algorithm, Digital Signature Algorithm (DSA) and Elliptic Curve Cryptography (ECC). Hash functions produce digest values after computation on the information received. This can be used as digital signatures for verifying the authenticity of the data. The process of using digital signature to transmit messages securely in a network communication is illustrated as in Fig 3.



**Fig 3.** Digital Signature using Asymmetric key encryption [32]

#### 4. Proposed Hybrid Model for Application in SG

##### 4.1. Methodology

According to the security requirements of cryptographic modules by the Federal Information Processing Standards (FIPS) of National Institute of Standards and Technology (NIST), the cryptographic algorithms are listed under the categories of symmetric key encryption / decryption, digital signatures, message authentication and hashing [33] [34]. One of the best-known symmetric block ciphers, the AES encryption algorithm with 128 up to 256 key lengths prove to be very secure in many applications. In addition, many adaptations of symmetric algorithm have been established like ARIA, which uses a permutation and substitution structure, SM4 the symmetric block cipher similar to AES [35], Camellia algorithm with smaller key size options [36], IDEA the symmetric key block cipher algorithm and SEED the 128 bit key block cipher. An adaptation of the AES algorithm, the ARIA encryption algorithm is used in this paper owing to its

improved security performance without compromising the speed and its suitability to use in low-end devices.

ARIA is a 128-bit block cipher with 128-, 192-, and 256-bit keys to encrypt 128-bit blocks in 12, 14, and 16 rounds, depending on the key size. The algorithm consists of a key scheduling part and data randomizing part and is named a national standard in Korea [37].

ARIA encryption algorithm is known to be resistant to many security attacks, some of the attacks are identified in [38], using the cryptanalysis methods. The most common multiset and collision attacks are well managed in ARIA as compared to AES algorithm because of the diffusion layer present in ARIA. Because of the irregular key structures, slide attacks are also not possible in ARIA. Moreover, as the ARIA algorithm uses the mathematical functions of substitution boxed, it derives the advantages of the algebraic properties.

According to [39], the linear cryptanalysis performed on ARIA algorithm shows that, the reduced round algorithm is weak against the possible attacks, whereas the full round ARIA is found to be stable.

When compared to the traditional symmetric encryption algorithms, the ARIA algorithm provides security against multiset and collision attacks, which generally make use of the slow diffusion rounds. The ARIA encryption algorithm uses a diffusion layer of branch 8, resulting in faster diffusion and the distinguisher used is proved to be stronger with every round. In addition, the distinguisher is extended in top and bottom causing the need of more key bytes to be guessed during multiset and collision attacks.

With the above said advantages of ARIA encryption algorithm in the context of low-computational capable devices, it is proven to provide improved security, performance and efficiency. Therefore, in this paper, we propose the combination of ARIA symmetric algorithm for message encryption and an enhanced RSA algorithm for the key encryption secured with SHA256 generated hash value used for digital signature.

The SHA256 hash function is used in this hybrid protocol owing to its advantages of improved security. It is more secure than the other hash algorithms, as  $2^{256}$  possible hash values are possible and therefore collisions are almost unlikely [40].

Thus, this hybrid protocol can result in more secure transmission of energy consumption data from residential smart meters towards the utility centres. The encryption block diagram for the proposed hybrid security protocol is illustrated in Fig 4.

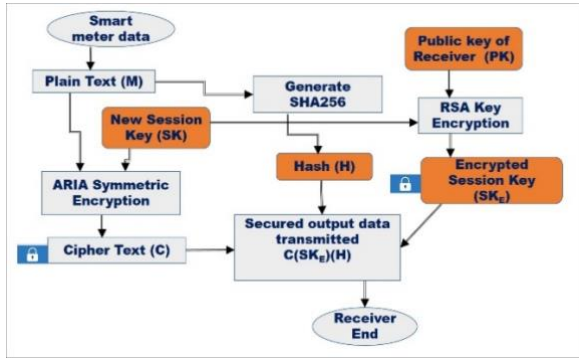


Fig 4. Hybrid security protocol - Encryption

The encryption and decryption processes of the proposed hybrid security protocol is explained in the following steps:

1. The plain text (M) is encrypted to cipher text (C) using the symmetric ARIA algorithm with session key (SK).
2. Hash value (H) generated from the plain text using SHA256 hash function.
3. Session key (SK) is encrypted using RSA algorithm with public key (PK)
4. Secured output data generated with cipher text (C), encrypted session key (SKE) and hash value (H).
5. On receiving the output C(SKE) (H), the session key SKE is decrypted using RSA algorithm using the receiver private key to produce SKD.
6. Using SKD the cipher text (C) is decrypted to plain text MD with ARIA Symmetric algorithm.
7. Using MD, the hash value is re-generated (RH)
8. The re-generated hash value is compared with the original hash to ensure authentication of the message.

Likewise, decryption block diagram for the proposed hybrid security protocol is illustrated in Fig 5.

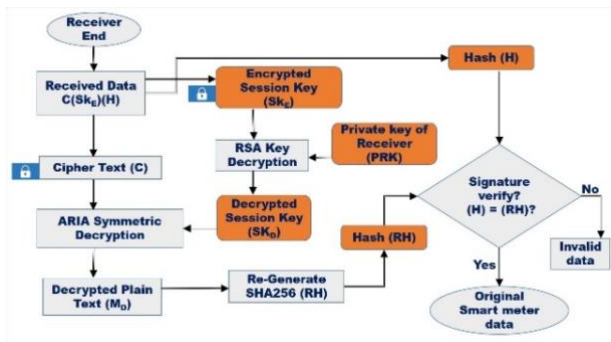


Fig 5. Hybrid security protocol - Decryption

4.2. Proposed Hybrid Algorithm

The processes involved in the encryption are summarized as in Table 4:

Table 4 ARIA encryption with RSA key and SHA256

ARIA encryption algorithm with RSA key and SHA256	
1:	Input: Plain text $M$ in readable format (Example – daily consumption, customer profile, tariff chart)
2:	Initializations: $SK$ – 128 bit key, $SK_L$ (leftmost 128 bits), $SK_R$ (remaining bits) = 0, Assign constants $CK1, CK2, CK3$ – 128-bit values
3:	Compute intermediate round values $W_0, W_1, W_2, W_3$ $W_0 = SK_L$ , $W_1 = F_O(W_0, CK1) \text{ XOR } SK_R$ , $W_2 = F_E(W_1, CK2) \text{ XOR } W_0$ , $W_3 = F_O(W_2, CK3) \text{ XOR } W_1$ $F_O$ - Odd Round Function $F_E$ - Even Round Function $F_E(D, RK) = A(SL_2(D \wedge RK)) - D$ , $RK$ - 128-bit string, $SL_1, SL_2$ - substitution layers with two $8 \times 8$ -bit substitution boxes (S-Boxes), function $A$ - Diffusion layer
4:	Generate encryption round keys $erk_n$ ( $n = 1, 2, 3, \dots, 13$ ), ( $m = 0, 1, 2, 3$ ) $erk_n = W_m \text{ XOR } (W_{m+1} \gg \gg 19)$ where $(n, m) = (1,0), (2,1), (3,2)$ $erk_n = (W_0 \gg \gg 19) \text{ XOR } W_3$ where $n = 4$ $erk_n = W_m \text{ XOR } (W_{m+1} \gg \gg 31)$ where $(n, m) = (5,0), (6,1), (7,2)$ $erk_n = (W_0 \gg \gg 31) \text{ XOR } W_3$ where $n = 8$ $erk_n = W_m \text{ XOR } (W_{m+1} \ll \ll 61)$ where $(n, m) = (9,0), (10,1), (11,2)$ $erk_n = (W_0 \ll \ll 61) \text{ XOR } W_3$ where $n = 12$ $erk_n = W_m \text{ XOR } (W_{m+1} \ll \ll 31)$ where $(n, m) = (13, 0)$ extra key addition layer
5:	Convert 128-bit plain text $M$ to compute cipher text $C$ in 12 rounds $M_n = F_{O/E}(M_{n-1}, erk_n)$ where $n = \{1, 2, 3, \dots, 11\}$ for round $n$ with odd/even functions Ciphertext $C = SL_2(M_{11} \text{ XOR } erk_{12}) \text{ XOR } erk_{13}$
6:	Generate receiver's public key $PK$ using $n = p \cdot q$ where $p, q$ - large prime numbers Totient $\phi(pq) = (p - 1)(q - 1)$ $PK = (n, e)$ where $e$ - relative power
7:	Compute encrypted session key $SK_E$ $SK_E = SK_E \text{ mod } n$
8:	Compute hash value $H$ from plain text $M$ using SHA256 hash function $H_{SHA256}(M, SK_E)$

<b>ARIA encryption algorithm with RSA key and SHA256</b>	
<b>9:</b>	Output: Generate secure output data with cipher text ( $C$ ), cipher key ( $SK_E$ ) and hash value ( $H$ )

Subsequently, the processes involved in the decryption are summarized in the algorithm as in Table 5.

**Table 5** ARIA decryption with RSA key and SHA256

<b>ARIA decryption algorithm with RSA key and SHA256</b>	
<b>1:</b>	Input: Received data - encrypted plain text $C$ , encrypted session key $SK_E$ and the hash value of the plain text $H$
<b>2:</b>	Compute receiver's private key $PRK$ using $(n, d)$ where $d$ is the modular inverse of $e \bmod \phi(n)$
<b>3:</b>	Restore the original session key $SK$ by decrypting $SK_E$ $SK = (SK_E)_d \bmod n$
<b>4:</b>	Generate decryption round keys $drk_n$ ( $n = 1, 2, 3 \dots 13$ ), ( $m = 0, 1, 2 \dots 13$ ) $drk_n = erk_m$ where $(n, m) = (1, 13)$ $drk_n = A(erk_m)$ where $(n, m) = (2, 12), (3, 11), (4, 10), (5, 9), (6, 8), (7, 7), (8, 6), (9, 5), (10, 4), (11, 3), (12, 2)$ function $A$ - Diffusion layer $drk_n = erk_m$ where $(n, m) = (13, 1)$
<b>5:</b>	Convert the cipher text $C$ to original plain text $M_D$ in 12 rounds $C_n = F_{O/E}(C_{n-1}, drk_n)$ where $n = \{1, 2, 3 \dots 11\}$ for round $n$ with odd/even functions decrypted plain text $M_D$ $M_D = SL_2(C_{11} XOR drk_{12}) XOR drk_{13}$ where functions $SL_1, SL_2$ - substitution layers with two $8 \times 8$ -bit substitution boxes (S-Boxes)
<b>6:</b>	Re-generate the hash value $RH$ using the decrypted plain text $M_D$ with SHA256 function $RH_{SHA256}(M_D, SK)$
<b>7:</b>	<b>If</b> ( $H = RH$ ) Output the securely received original plain text $M = M_D$ <b>Else</b> Output error detection message and forward to attack detection module

The no. of rounds change depending on the size of the master key. There are 12, 14 and 16 rounds for the key sizes of 128, 192 and 256 respectively. The master key in ARIA algorithm can be with 128, 192 and 256-bit keys to encrypt 128-bit blocks in 12, 14, and 16 rounds, depending on the key size. Here, in our proposed work, the key size considered is 128 bits with 12 rounds. As the no. of rounds increase which is directly proportional to the master key size, the strength of encryption increases linearly.

**4.3. Algorithm Description**

During the encryption phase of the hybrid algorithm, the master key is generated with 128 bits. Then the intermediate round values are computed using the assigned constants. Encryption round keys are generated in the ARIA algorithm for each round necessary for the encryption operation which enhances the strength and performance of encryption. The number of the rounds depend on the size of the master key. Here, for the 128-bit key, with 12 rounds of odd and even functions, and the XOR functions executed in the substitution layer, the plain text  $M$  is converted to cipher text  $C$  as in the equations (1) and (2):

$$M_n = F_{O/E}(M_{n-1}, erk_n) \tag{1}$$

where  $n = \{1, 2, 3 \dots 11\}$  for round  $n$  with odd/even functions

$$C = SL_2(M_{11} XOR erk_{12}) XOR erk_{13} \tag{2}$$

here, CK1, CK2, and CK3 are 128-bit with values as below, which are obtained from the first 128\*3 bits of the fractional part of  $1/P1$  (P1-circle ration)

$$C1 = 0x517cc1b727220a94fe13abe8fa9a6ee0$$

$$C2 = 0x6db14acc9e21c820ff28b1d5ef5de2b0$$

$$C3 = 0xdb92371d2126e9700324977504e8c90e$$

The number of round keys in this case is 13, as there is an extra key addition layer with 12 rounds. Additionally, in the hybrid protocol, the encryption session key itself is protected by encrypting using the RSA algorithm, where two large prime numbers are generated and the totient function is calculated using the equation (3) as below:

$$\phi(pq) = (p - 1)(q - 1) \tag{3}$$

The co-prime  $e$  is chosen, the public key  $PK$  is generated, and the encryption session key  $SK_E$  is produced using the modulus function as shown in equation (4) and equation (5):

$$PK = (n, e) \tag{4}$$

$$SK_E = SK_E \bmod n \tag{5}$$



Finally in the encryption process, the hash value is generated using the SHA256 function for verifying the digital signature of the sender as in equation (6).

$$H = H_{SHA256}(M, SK_E) \tag{6}$$

Therefore, the encryption output consists of the cipher text, encrypted session key and the hash value. Subsequently, during the decryption phase of the hybrid algorithm, the private key for the RSA decryption is computed and the session key is restored using  $(n, d)$  where  $d$  is the modular inverse of  $e \text{ mod } \phi(n)$  as in equation (7):

$$SK = (SK_E)_d \text{ mod } n \tag{7}$$

Then for the data decryption using ARIA, the reverse rounds are executed using the decryption round keys to retrieve the plain text securely. The decryption round keys are derived from the encryption round keys and the plain text is recovered as in equation (8) and equation (9):

$$C_n = F_{O/E}(C_{n-1}, drk_n) \tag{8}$$

where where  $n = \{1,2,3 \dots 11\}$  for round  $n$  with odd/even functions

$$M_D = SL_2(C_{11} \text{ XOR } drk_{12}) \text{ XOR } drk_{13} \tag{9}$$

The SHA function is chosen over the most common MD5 function because this overcomes the collision possibilities and is more secure. Lastly, the hash value is regenerated using the decrypted plain text and the SHA256 function as in equation (10) and compared with the original hash value.

$$RH = RH_{SHA256}(M_D, SK) \tag{10}$$

If  $H = RH$ , the digital signature of the sender is verified and the original data is recovered in the receiver's end securely and satisfying authentication.

## 5. Results and Discussion

### 5.1. Results

The proposed hybrid security algorithm is executed in Python environment with the execution carried out using Python 3.6 working in Spyder code interface. The output obtained on executing the algorithm of the hybrid security protocol consisting of ARIA encryption/decryption, RSA key

encryption and SHA256 hash value function is shown in figures, Fig 6 and Fig 7.

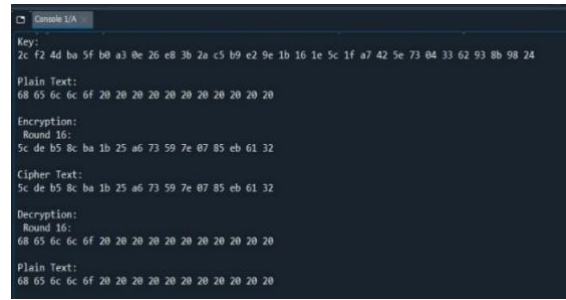


Fig 6. Intermediate results of the hybrid algorithm



Fig 7. Output of the hybrid algorithm

### 5.2. Comparative Analysis

The performance of the ARIA encryption algorithm in terms of speed is comparable and almost equivalent to AES algorithm. However, in place of one S-Box in AES algorithm, the use of two  $8 \times 8$ -bit S-boxes and their inverses for each of the alternate rounds in the ARIA algorithm provides improved security. The performance comparison of the hybrid protocols of ARIA algorithm with RSA and AES algorithm with RSA is shown in Table 6 in terms of various cryptographic performance parameters.

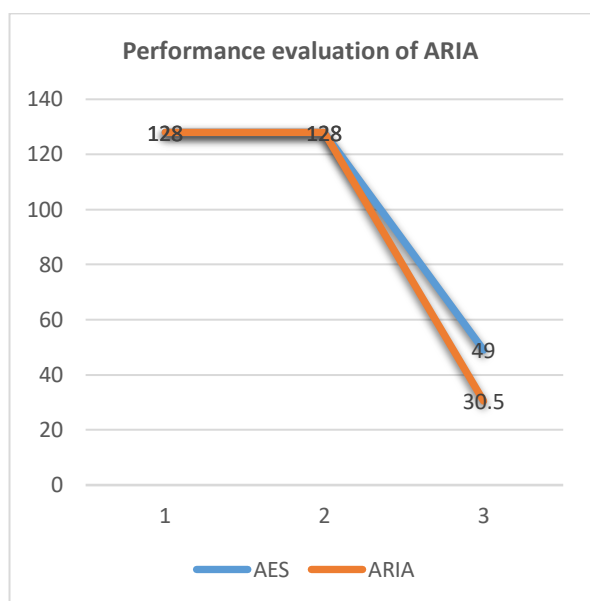
Table 6. Performance comparison of AES and ARIA encryption algorithms

	AES	ARIA
Structure of algorithm	Substitution permutation network	Involution substitution permutation network

	AES	ARIA
<b>Algorithm for key encryption</b>	RSA	RSA
<b>Hash Value generation</b>	MD5	SHA256
<b>CPU Cycles /byte for execution</b>	49	30.5
<b>Memory for implementation</b>	Low to medium level	Low-level
<b>Cryptanalysis attacks</b>	Side channel attacks	Meet-in-the-middle attacks

	AES	ARIA	Serpent	Camellia	Blowfish
<b>Block size</b>	128 bits	128 bits	128 bits	128 bits	64 bits
<b>Key size</b>	128,192, 256 bit	128,192, 256 bit	128,192, 256 bit	128,192, 256 bit	32–48 bits
<b>No. of rounds</b>	10,12, 14	12,14,16	32	18, 24, 24	16

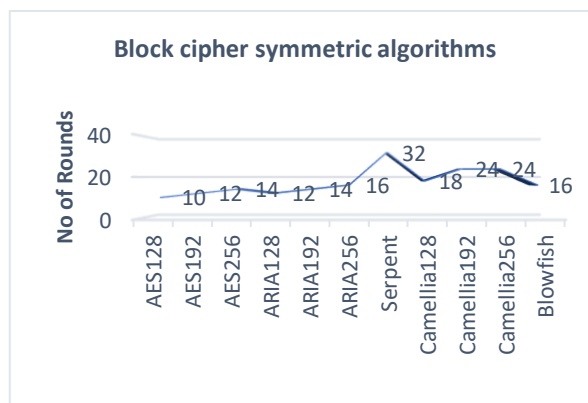
The graphical illustration of the performance comparison for ARIA and AES algorithms is presented in the chart as below in Fig 8.



**Fig 8.** Performance evaluation of 128-bit ARIA algorithm

The number of rounds executed in the Block cipher symmetric cryptographic algorithms also play a major role in deciding the suitable encryption for every application. In particular, for the metering data transmission of SG networks, the security is an important performance metric. The comparison of the computational complexities in terms of the no. of rounds executed is listed in Table 5 and is graphically illustrated in Fig 9.

**Table 5.** No. of rounds executed in Block cipher symmetric algorithms



**Fig 9.** No. of rounds in block cipher symmetric algorithms

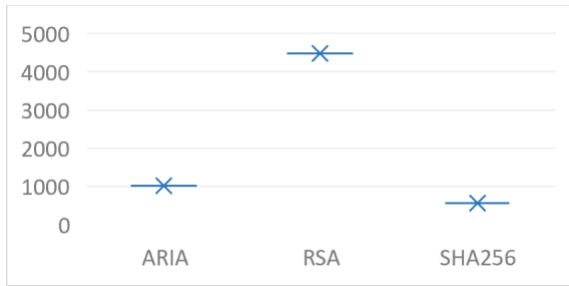
Further analysis and investigation of the results show various comparisons of the conventional symmetric encryption and hybrid encryption algorithm. The performance metrics measured are based on the encryption strength according to key length, memory usage of the CPU and the execution time. The performance metrics of memory usage, execution speed and security strength are crucial in smart meters, hence these measures are reviewed in this work. The individual performance measures of the algorithms used are presented in Table 7.

**Table 7.** Performance measures of individual algorithms

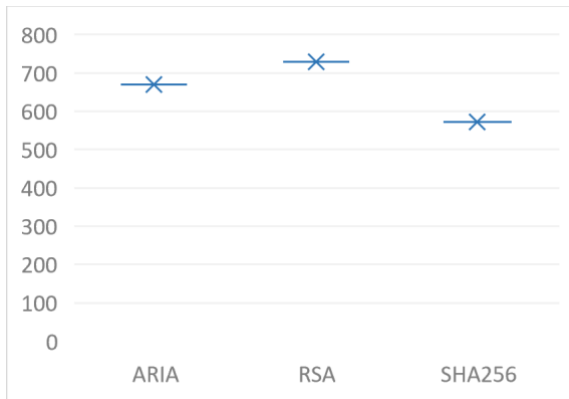
	<b>Encryption strength based on key length bits</b>	<b>Execution time parameters in milliseconds (ms)</b>	<b>CPU memory usage in Mebibyte (MiB)</b>
<b>ARIA</b>	1024	669.62	97.7
<b>RSA</b>	4480	728.9	98.2

SHA256	560	572.77	84.5
--------	-----	--------	------

The individual performance measures are graphically represented as below in Fig 10, Fig 11 and Fig 12.



**Fig 10.** Comparison of encryption strength based on key length bits



**Fig 11.** Comparison of execution time



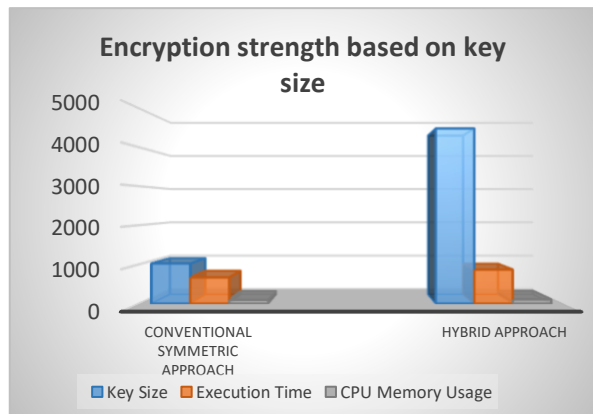
**Fig 12.** Comparison of CPU memory usage

Likewise, the performance metrics are collectively evaluated for the conventional symmetric encryption and the hybrid algorithm. The comparative values are summarized in Table 8.

**Table 8.** Performance comparison of conventional and hybrid algorithms

	Encryption strength based on Key Size	Execution Time	CPU Memory Usage
<b>Conventional symmetric approach</b>	1024	669.62	97.7
<b>Hybrid approach</b>	4480	869.59	108.6

The comparative values of the conventional symmetric algorithm and the hybrid algorithm is graphically represented as in Fig. 13



**Fig 13.** Performance comparison of the conventional and hybrid algorithms

### 5.3. Discussion

Encryption round keys are generated in the ARIA algorithm for each round necessary for the encryption operation which enhances the strength and performance of encryption. Despite the similarity of the AES and ARIA algorithms, the ARIA encryption algorithm has the added security feature of two 8x8-bit S-boxes and their inverses for each of the alternate rounds. Hence, the hybrid protocol of combining the ARIA algorithm with other asymmetric algorithms can be more suitable for secure transmission of data. The two types of S-boxes S1, S2 and their inverses S1-1, S2-1 used in its substitution layers in alternate rounds as shown in figures, Fig 14 and Fig 15, contribute to the improved security of ARIA encryption algorithm.

S-box $S_1$																S-box $S_1^{-1}$																	
0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f		
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76	0	52	09	6a	d5	30	36	a5	38	ff	40	a3	9e	81	f3	d7	fb
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	04	81	4f	dc	22	2a	90	98	4e	ee	b8	14	de	5e	0b	db	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	e1	f8	18	11	69	d9	9e	94	9b	1e	87	e9	ce	55	28	df	e	a0	e0	1b	3d	ad	ae	2a	f5	b0	c8	bd	3c	83	53	99	61
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Fig 14. S-Box  $S_1$  and its inverse

S-box $S_2$																S-box $S_2^{-1}$																	
0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f		
0	e2	4e	54	fc	94	c2	4a	cc	62	04	6a	46	3c	4d	8b	d1	0	30	68	99	1b	87	b9	21	78	50	39	db	e1	72	9	62	3c
1	5e	fa	64	cb	b4	97	be	2b	bc	77	2e	03	d3	19	59	c1	1	3e	7e	5e	8e	f1	a0	cc	a3	2a	1d	fb	b6	d6	20	c4	8d
2	1d	06	41	6b	55	f0	99	69	ea	9c	18	ae	63	df	e7	bb	2	81	65	f5	89	cb	9d	77	c6	57	43	56	17	d4	40	1a	4d
3	00	73	66	fb	96	4c	85	e4	3a	09	45	aa	0f	ee	10	eb	3	c0	63	6c	e3	b7	c8	64	6a	53	aa	38	98	0c	f4	9b	ed
4	2d	f4	14	29	ac	cf	ad	91	8d	78	c8	95	f9	2f	ce	cd	4	4f	22	76	af	dd	3a	0b	58	67	88	06	c3	50	0d	01	8b
5	08	7a	88	38	5c	83	2a	28	47	db	b8	c7	93	a4	12	53	5	8c	c2	e6	5f	02	24	75	93	66	1e	e5	e2	54	d8	10	ce
6	ff	87	0e	31	36	21	58	48	01	8e	37	74	32	ca	e9	b1	6	7a	e8	8	2c	12	97	32	ab	b4	27	0a	23	df	ef	ca	d9
7	b7	ab	0c	d7	c4	56	42	26	07	98	60	a9	b6	b9	11	40	7	b8	fa	dc	31	6d	1d	ad	19	49	bd	51	96	ee	e4	a8	41
8	ec	20	8c	bd	a0	c9	84	4	49	23	f1	4f	50	1f	13	dc	8	da	ff	cd	55	86	36	be	61	52	fb	0e	82	48	69	9a	9a
9	d8	c0	9e	57	e3	c3	7b	65	3b	02	8f	3e	e8	25	92	e5	9	e0	47	9e	5c	04	4b	34	15	79	26	a7	de	29	ae	92	47
a	15	dd	fd	17	af	bf	44	9a	7e	c5	39	67	fe	76	9d	43	a	84	e9	d2	ba	5d	f3	c5	b0	bf	a4	3b	71	44	46	2b	fc
b	a7	e1	d0	f5	68	f2	1b	34	70	05	a3	8a	d5	79	86	a8	b	eb	6f	d5	f6	14	fe	7c	70	5a	7d	fd	2f	18	83	16	a5
c	30	c6	51	4b	1e	a6	27	f6	35	d2	6e	24	16	82	5f	da	c	91	1f	05	95	74	a9	c1	5b	4a	85	6d	13	07	4f	4e	45
d	e6	75	a2	ef	2c	b2	1c	9f	5d	6f	80	0a	72	44	9b	6c	d	b2	0f	c9	1c	a6	bc	ec	73	90	7b	cf	59	8f	a1	f9	2d
e	90	b	5b	33	7d	5a	52	f3	61	af	f7	b0	d6	3f	7c	6d	e	f2	b1	00	94	37	9f	d0	2e	9c	6e	28	3f	80	f0	3d	63
f	ed	14	e0	a5	3d	22	b3	f8	89	de	71	1a	af	ba	b5	81	f	25	8a	b5	e7	42	b3	c7	ea	f7	4c	11	33	03	a2	ac	60

Fig 15. S-Box  $S_2$  and its inverse

From the results, the observation shows the performance measures of Execution time and CPU memory usage of the hybrid algorithm are marginally higher than the conventional symmetric algorithm and may be traded off to attain significantly improved encryption strength. There is an increase by 2% in the execution time and by 1% in the CPU memory usage for the hybrid security algorithm as illustrated in Fig.16

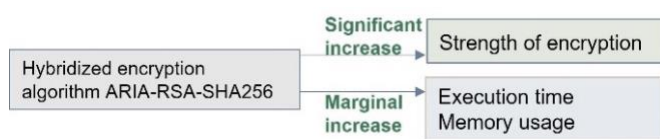


Fig 16 Effectiveness of hybridized encryption

Therefore, the improved encryption strength resulting from the complex key combinations can be a driving force for implementing the proposed hybrid protocol for the metering data transmission of SG networks. The use of ARIA encryption in the hybrid protocol provides efficient security from the known attacks on block ciphers and prevents the easy guessing of single S-box usage as in AES, which make the proposed hybrid algorithm suitable for secure transmission. Some of the available lightweight algorithm designs in symmetric cryptography are the bit sliced-S-Box-based designs, ARX-based and simple key schedules. The state of the art techniques like ultra-lightweight cryptography for narrow constraints and ubiquitous cryptography with versatile algorithms are developed for resource-constraint smart devices [41]. Accordingly, the usage of ARIA symmetric

algorithm is more suitable for low-end devices like smart meters. The implementation using the counter (CTR) mode is suggested in [42] which shows a considerable improvement in CPU clock cycles per byte. Moreover, in the key encryption part of the protocol, the RSA encryption algorithm is used with enhanced functionality. While choosing the large prime numbers for the RSA encryption, there is considerable improvement in execution time when the primality tests are in combination. As suggested by our enhanced method of RSA encryption, a low primality test is used in combination with a high level primality test [43]. A combination of low-level and high-level primality tests is used which includes a low-level primality test with first few hundred primes. Subsequently, the overall key encryption using the RSA algorithm will have a positive impact on the time complexities thus improving speed. The digital signature using verification of SHA256 hash values ensures data integrity and authenticity.

Thus, the implementation of this hybrid model of combining the ARIA symmetric encryption with the RSA public cryptography algorithm with digital signature for the metering infrastructure of SG would result in efficient and secure transmission of data to the utility centres.

## 6. Conclusion

The transmission of data between the AMI system and the utility centres demands utmost security measures to be in place to ensure perfect energy demand- supply balance. Any compromise would lead to data leakage or false data inclusions, which may result in incorrect data analysis results. Hence, along with the encryption of smart meter data through symmetric encryption techniques, the cryptographic key encryption plays a major role. Therefore, in this paper, we have proposed a hybrid security protocol by combining the ARIA encryption algorithm for message encryption and RSA public key encryption for the key encryption. Along with that, SHA256 generated hash value for the digital signature for the secure transmission of energy consumption data from residential smart meters to the utility centres is applied. According to the study and analysis of the hybrid protocol execution, the observation is that the ARIA algorithm provides a secure encryption of the original consumption data with operations of multiple rounds of XOR and S-box substitutions and provides improved security when combined with RSA algorithm and SHA256 hash digital signature. This research topic can further be expanded to other adaptations of the ARIA and RSA algorithm in the context of electricity smart meters. This research idea of hybrid security protocols has the scope for further investigations of the strength of encryption in various cryptanalysis attack scenarios. ARIA encryption can be efficient in 8-bit architectures like smart meters, especially in hardware implementation. As ARIA encryption algorithm is suitable for low-end devices, this can be used individually or in combination with other algorithms for many IoT applications involving low-computational devices [44]. In addition, the study on the hardware implementation modes of the encryption algorithms may lead

to arrive at the suitable smart meter specifications. ARIA encryption algorithm has been successfully applied as efficient security methods of cloud computing applications as explained in [45].

## References

- [1] A. Bani-Ahmed, A. Nasiri, and I. Stamenkovic, "Foundational Support Systems of the Smart Grid: State of the Art and Future Trends," 2018.
- [2] H. Abouelgheit, "Information and Communication Technologies in Modern Electrical Networks: A Brief Review," 2022.
- [3] A. Shobol, M. H. Ali, M. Wadi, and M. R. Tur, "Overview of big data in smart grid," in *8th International Conference on Renewable Energy Research and Applications, ICRERA 2019*, Institute of Electrical and Electronics Engineers Inc., Nov. 2019, pp. 1022–1025. doi: 10.1109/ICRERA47325.2019.8996527.
- [4] U.S. Department of Energy, "Advanced Metering Infrastructure and Customer Systems - Results from the smart grid investment grant program," *Office of Electricity Delivery and Energy Reliability*, pp. 1–98, 2016.
- [5] A. Al-Abri, W. Al Khalil, and K. E. Okedu, "Electricity Sector of Oman and Prospects of Advanced Metering Infrastructures," 2022.
- [6] F. S. Alsharbaty and Q. I. Ali, "A Cybersecurity Model for the Enhancement of WiMAX-based Wireless Communications Infrastructure to Serve Smart Grid Applications," 2023.
- [7] S. Sagiroglu, Y. Canbay, İlhami Colak, and C. Author, "Solutions and Suggestions for Smart Grid Threats and Vulnerabilities," 2019.
- [8] D. M. Menon and N. Radhika, "Design of a Secure Architecture for Last Mile Communication in Smart Grid Systems," *Procedia Technology*, vol. 21, pp. 125–131, 2015, doi: 10.1016/j.protcy.2015.10.019.
- [9] S. Khasawneh and M. Kadoch, "Hybrid Cryptography Algorithm with Precomputation for Advanced Metering Infrastructure Networks," *Mobile Networks and Applications*, vol. 23, no. 4, pp. 982–993, 2018, doi: 10.1007/s11036-017-0956-0.
- [10] S. Grids and H. Cryptosystem, "Australian Journal of Basic and Applied Sciences Hybrid Security Approach for Smart Grid Infrastructure," vol. 9, no. 16, pp. 91–96, 2015.
- [11] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. S. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans Smart Grid*, vol. 2, no. 4, pp. 675–685, 2011, doi: 10.1109/TSG.2011.2160661.
- [12] S. Khasawneh and M. Kadoch, "A Hybrid Encryption Scheme for Advanced Metering Infrastructure Networks," no. May, 2017, doi: 10.4108/eai.7-8-2017.152990.
- [13] A. K. Asundi, P. B. Jyoti, M. S. Nagaraj, and S. S. Sultan, "An efficient cryptography key management for secure communications in smart metering," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 10, pp. 2908–2916, 2019, doi: 10.35940/ijitee.I7846.0881019.
- [14] K. Mahmood, S. Ashraf Chaudhry, H. Naqvi, T. Shon, and H. Farooq Ahmad, "A lightweight message authentication scheme for Smart Grid communications in power sector," *Computers and Electrical Engineering*, vol. 52, pp. 114–124, 2016, doi: 10.1016/j.compeleceng.2016.02.017.
- [15] I. Parvez, M. Aghili, and A. Sarwat, "Key Management and Learning based Two Level Data Security for Metering Infrastructure of Smart Grid," pp. 1–8, 2017.
- [16] D. Abbasinezhad-Mood and M. Nikooghadam, "Design of an enhanced message authentication scheme for smart grid and its performance analysis on an ARM Cortex-M3 microcontroller," *Journal of Information Security and Applications*, vol. 40, pp. 9–19, 2018, doi: 10.1016/j.jisa.2018.02.007.
- [17] K. Alharbi and X. Lin, "Efficient and privacy-preserving smart grid downlink communication using identity based signcryption," *2016 IEEE Global Communications Conference, GLOBECOM 2016 - Proceedings*, 2016, doi: 10.1109/GLOCOM.2016.7841770.
- [18] N. George, S. Nithin, and S. K. Kottayil, "Hybrid Key Management Scheme for Secure AMI Communications," *Procedia Computer Science*, vol. 93, pp. 862–869, 2016. doi: 10.1016/j.procs.2016.07.260.
- [19] T. Rizzetti, B. Menezes da Silva, A. Silva Rodrigues, R. Gressler Milbradt, and L. Neves Canha, "A secure and lightweight multicast communication system for Smart Grids," *ICST Transactions on Security and Safety*, vol. 5, no. 16, p. 156004, 2018, doi: 10.4108/eai.13-7-2018.156004.
- [20] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication," *Future Generation Computer Systems*, vol. 81, pp. 557–565, 2018, doi: 10.1016/j.future.2017.05.002.
- [21] N. N. Mohamed, Y. M. Yussoff, M. A. Saleh, and H. Hashim, "Hybrid cryptographic approach for internet of things applications: A review," *Journal of Information and Communication Technology*, vol. 19, no. 3, pp. 279–319, 2020, doi: 10.32890/jict2020.19.3.1.
- [22] B. K. Alese, E. D. Philemon, and S. O. Falaki, "Comparative analysis of public-key encryption schemes," *International Journal of Engineering and Technology*, vol. 2, no. 9, pp. 1152–1568, 2012.

- [23] F. Wang, Z. Wang, and Y. Zhu, "Adaptive RSA Encryption Algorithm for Smart Grid," *J Phys Conf Ser*, vol. 1302, no. 2, 2019, doi: 10.1088/1742-6596/1302/2/022097.
- [24] G. M. S. G. C. Deka and K. G. S. L. M. Patnaik, *CYBER - PHYSICAL SYSTEMS A Computational Perspective*. 2016.
- [25] L. Wei, L. P. Rondon, A. Moghadasi, and A. I. Sarwat, "Review of cyber-physical attacks and counter defense mechanisms for advanced metering infrastructure in smart grid," *ArXiv*, 2018.
- [26] S. Demirci and S. Sagiroglu, "Software-Defined Networking for Improving Security in Smart Grid Systems."
- [27] "Threat Modeling: 12 Available Methods." Accessed: Jul. 12, 2021. [Online]. Available: <https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/>
- [28] J. Ekanayake, K. Liyanage, J. Wu, A. Yokoyama, and N. Jenkins, *Smart Grid: Technology and Applications*. 2012. doi: 10.1002/9781119968696.
- [29] R. Manjupriya, "A Study on Symmetric and Asymmetric Key Encryption Algorithms," *International Research Journal of Engineering and Technology*, vol. 3, no. 4, pp. 27–31, 2016.
- [30] "Symmetric Algorithms | Types of Symmetric Algorithms." Accessed: Jul. 07, 2021. [Online]. Available: <https://www.educba.com/symmetric-algorithms/?source=leftnav>
- [31] J. Henkel, *Cyber-Physical Systems Security and Privacy*, vol. 34, no. 4. 2017. doi: 10.1109/MDAT.2017.2713356.
- [32] "Public Key Encryption and Digital Signatures." Accessed: Aug. 22, 2021. [Online]. Available: <http://guides.brucejmack.net/SOA-Patterns/WSSP/13.1PublicKeyEncryptDigSigDoc.htm>
- [33] NIST, "Annex A: Security Requirements for Cryptographic Modules," pp. 2–9, 2019.
- [34] T. Caddy, "Fips 140-2," *Encyclopedia of Cryptography and Security*, pp. 468–471, 2011, doi: 10.1007/978-1-4419-5906-5\_205.
- [35] "Popular Symmetric Algorithms - Practical Cryptography for Developers." Accessed: Jul. 22, 2021. [Online]. Available: <https://cryptobook.nakov.com/symmetric-key-ciphers/popular-symmetric-algorithms>
- [36] K. Standard and B. Cipher, "Block Cipher Algorithm ARIA," pp. 1–2, 2021.
- [37] "An Overview of Cryptography." Accessed: Jul. 23, 2021. [Online]. Available: <https://www.garykessler.net/library/crypto.html>
- [38] C. D. C. J. L. B. P. S. B. Ö. A. Biryukov, "Security and Performance Analysis of ARIA," vol. 2, no. 1, pp. 27–33, 2004.
- [39] A. Abdelkhalek, M. Tolba, and A. M. Youssef, "Improved linear cryptanalysis of round-reduced ARIA," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9866 LNCS, pp. 18–34, 2016, doi: 10.1007/978-3-319-45871-7\_2.
- [40] A. Al Khas, I. Cicek, O. Mahalleli, and O. Bulvarı, "SHA-512 Based Wireless Authentication Scheme for Smart Grid Battery Management Systems," 2020.
- [41] H. Brekke, "State of the Art in Lightweight Symmetric Cryptography," *Iahr 2012*, no. Lofgren 2015, pp. 1–11, 2012.
- [42] H. Seo, H. Kwon, H. Kim, and J. Park, "Ace: Aria-ctr encryption for low-end embedded processors," *Sensors (Switzerland)*, vol. 20, no. 13, pp. 1–15, 2020, doi: 10.3390/s20133788.
- [43] A. Philips, J. Jayaraj, J. F.T, and V. P, "Enhanced RSA key encryption application for metering data in smart grid," *International Journal of Pervasive Computing and Communications*, vol. 17, no. 5, pp. 596–610, 2021, doi: 10.1108/IJPC-07-2021-0172.
- [44] T. D. Le, A. Anwar, R. Beuran, and S. W. Loke, "Smart Grid Co-Simulation Tools: Review and Cybersecurity Case Study."
- [45] N. Kaur and H. Wadhwa, "Security Enhancement in Cloud Storage using ARIA and Elgamal Algorithms," *Int J Comput Appl*, vol. 171, no. 9, pp. 19–23, 2017, doi: 10.5120/ijca2017915116.