[1]Rakhi V. Gupta

[2] Parminder Singh

[3] Avinash Kaur

Privacy Model for Smart Meter in Multi-Hop Network Environment

Abstract: - The transition from traditional power grids to smart grids represents a significant shift in the way we manage and utilize electrical power. This evolution brings about numerous opportunities and challenges in power system operations. The increased granularity of energy consumption data in smart grids can indeed raise privacy concerns. The smart meter data or high-resolution energy data, provides insight into specific patterns of energy use within a household. These patterns can be analyzed to infer various aspects of a consumer's behavior and lifestyle. The present title discloses the anti-theft model for multi hop smart grid node using embedded system. In the designed system, sensors are used to read the values of current and voltage. These values of voltage and current are converted into watt per minute. The standard AES 128 encryption technique is engaged to perform encryption. For encryption of the readings, "IV Key" and "ENC Keys" are used and the encrypted values are uploaded on to the Fire Base Server. The replica of the keys is updated on to another ESP processor. To access the real values of the node, android application is designed through which user have to enter the correct values of the private key. Once the key is entered through the android application, through the FIRE Base Server, the keys are sent to the ESP node for verification, if the true key is entered, the decrypted values are displayed on the android application and if wrong key is entered then random values are displayed. The system is also implemented with RSA(Rivest-Shamir-Adleman) algorithm on ESP32 Arduino platform. Later the results of both the methods are compared to gain better results. Making use of simple processes and procedures, the proposed model is made suitable for devices with minimal computational resources.

Keywords: ESP328, AES-128, RSA, Anti-Theft Smart Grid, Secured Node, Multi-Hop Network.

I. INTRODUCTION

Smart grid is the smart electricity distribution system in which different smart, top-notched electronic components and systems are engaged to monitor and efficiently manage the electricity from all generation sources to each of the consumption node to intelligently manage the varying electricity demands of the end users. Basically, smart grid is the means to coordinate the needs and capabilities of all of the distinct electricity generation sources, grid operation management, the end users and all components of the sources and nodes in order to function as efficiently as possible with minimal cost and through creating minimal environmental impact with highly optimized, highly reliable, flexible and stable. The different components which are deployed in design, development and management of the smart grid system have already been reached to the highest maturity level and hence highly reliable, flexible, stable and extendable system is designed and operated. Governments of different countries are already taking initiatives aggressively in order to attain more and more development in the energy sector to be smartly managed and attain Net Zero Emission by 2050.

Intelligent management of the smart grid is based on different verticals like collection of consumption data, retention of the data, sharing of the consumption data among the different nodes and reuse of the data for estimation and forecasting based on individual uses, homes and office uses. Either of the individual node, for individual uses, home or office uses, must be register first by sharing the personal information with the service provider. Once the registration is done, then smart grid system initiates multi-dimensional communication between the energy

[1] *School of Computer Science and Engineering, Lovely Professional University, Phagwara,Punjab, rakhig4@gmail.com

[2] School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab,parminder.16479@lpu.co.in

[3]School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab,avinash.14557@lpu.co.in

provider, the end user and any possible third-party service provider company. Operating the existing complex network of energy transportation system addition with the intricated smart grid system poses tremendous challenges. One of the downsides is the privacy of the end user. Some of the privacy related consequences of the smart grid system can be listed as identity theft, personal behaviour patterns, estimation of specific appliances used, real time surveillance of the energy usages, behaviour estimation through the residual data analysis, profiling targeted power controlling and targeted attacks by referring the above information. To attain control over these situations, birth to a new terminology has been given and it is known as privacy protection in smart grid.

Through this research paper, one of the possible methods for privacy protection of the end users of the smart grid systems have been disclosed. The system is fit to deploy in multi-hop communication environments which is basis of implementation of the smart grid system. The system is designed around set of ESP328 processor architecture. One end of the proposed system is equipped with the current sensor and voltage sensor. These two sensors read the current values of the current and the voltage. These sensors data are then converted into wattage per minute consumption. The consumption data is then encrypted using the Advanced Encryption Standard 128 bits (AES-128). The encryption using the AES-128 is performed using the "IV-Key" and the "ENC-Key". The encrypted data is stored at the FIRE Base Server. It is the central location where all the encrypted data is stored for accessing in the future. Another component of the system is again designed using the ESP-328 architecture in which keys are stored physically. This second component of the ESP-328 architecture is stored at the remote secure location. To access the encrypted data, separate android and ios based application, named "Smart Meters" is designed. Users must first sign-ups to the application by entering the personal information. Once signed-up, user must add his meter into the application. As an additional feature, user can add multiple meters one application. Now, once the sign-up process is completed and meter information has been loaded, user must sign-in through the credentials. Through sign-in user have to enter the private key provided. Once the private key is entered by the user, it is sent over to the FIRE Base Server and then to the second end of the system where the key is verified. If the key is verified successfully, then information is displayed on the mobile applications, but in case if the key is wrong then data wrangling is done and wrong data is displayed on the mobile application. Here, since the decryption process which is performed using the ESP-328 at the remote end, it is hardwired implementation which gives additional benefit of security to the credentials of the user and meter readings.

II. MOTIVATION AND CONTRIBUTION

Continuous research and development in privacy-preserving technologies are necessary to discover innovative solutions that are both effective and resource-efficient. This includes exploring lightweight cryptographic protocols and algorithms suitable for resource-constrained devices. Balancing the need for privacy with the practical constraints of cost, energy, and computational resources is a complex task. Addressing these challenges requires a multidisciplinary approach involving cryptography, energy management, and policy considerations to create sustainable and effective privacy-preserving solutions for smart meters and home appliances.

By focusing on privacy protection from the smart meters, the overall goal is to create a robust and secure foundation for the entire system. This approach acknowledges the potential vulnerabilities and privacy risks associated with the transmission of data in smart metering systems and aims to mitigate these risks from the outset.

The study proposes a privacy-preserving system for smart meter. Main contribution of our proposed system is:

- A robust privacy-protection model is designed for communication over untrusted mediums, and a system is implemented to allow data transmission over a mesh network with an untrusted third party being in direct contact with all the end nodes.
- Implemented system ensures the integrity of the data collected from smart meters and identifies any potential malicious activities for multi-hop smart grids.

To check the till date development in the similar domain detailed literature review has been carried out which is disclosed in the subsequent section. Further, implementation and results has been disclosed in the lateral sections.

III. RELATED WORK

M. Akgün et. al. disclosed *"Privacy Preserving Scheme for Smart Grid using Trusted Execution Environment"* [1] to protect the consumer privacy from customer node to the smart appliances to the server and the CSPs, without

disturbing the functionality of the smart grid. Authors make use of the Trusted Execution Environment (TEE) for storing the security keys, allocated while encryption of the data received from the smart appliances, along with the encrypted data. The disclosed system deals with the false data injection attacks by separately executing the fundamental security, privacy expectations and specific expectations. The subsequent Figure 1, discloses the systematic component arrangements for system development.

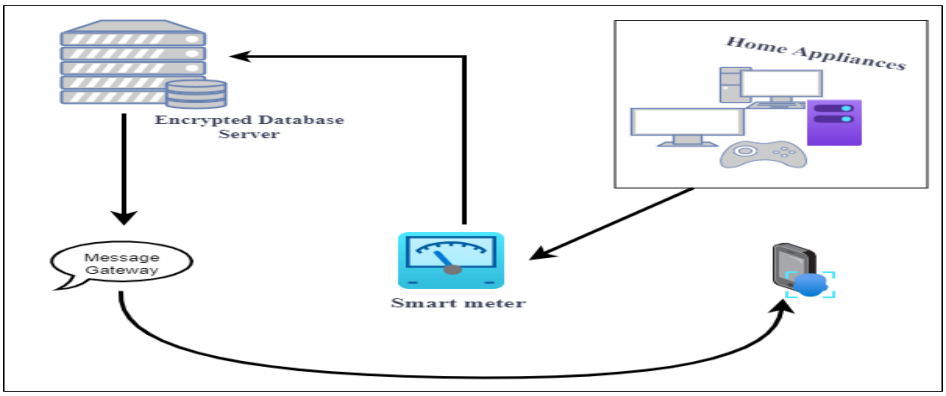

Figure 1. Privacy Preserving Scheme Using Trusted Execution Environment

Authors have carried out the performance analysis of the proposed system by game-based privacy definitions to assess the performance metrics. Authors also have claimed that the proposed system outperforms other reported homomorphic methodologies.

On the other hand, Albert Guan and D. J. Guan have disclosed an efficient and privacy protection scheme for effortless communication in smart grid scheme. The proposed communication scheme is targeted to share the data to the server in a secured and protected way. The communicated data is used for computing the billing information and for power distribution system. The proposed system is claimed to be effective for computing the billing information and to make the effective electric power distribution in the scenario where smart meters failed to communicate each other. [2]

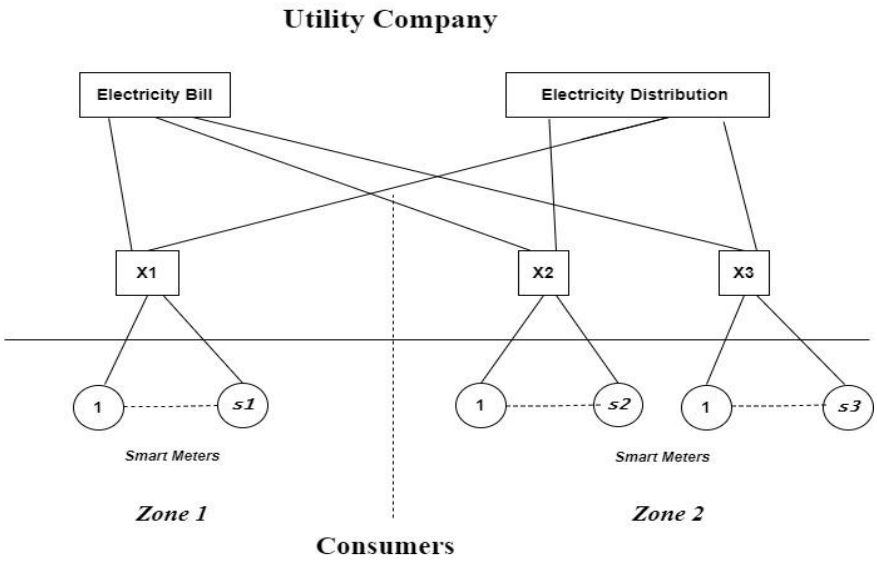

Figure 2. Simplified Smart Grid System Components of the Proposed System

The communication system between the nodes and the server is designed, by the authors, using the secret sharing scheme and differential privacy scheme, which is similar to the one-time pad encryption module. [2]

In the other literature, Xingze He et. Al. have disclosed *"A Distortion Based Approach to Privacy-Preserving Metering in Smart Grids"*, the disclosed system is claimed to be lightweight, efficient and robust and best suitable for metering scheme for smart grid environments. The power consumption data is distorted using the additive noise

before sending it to the other end. The related parties can decode the data for production estimations, dynamic pricing and billing related activities.

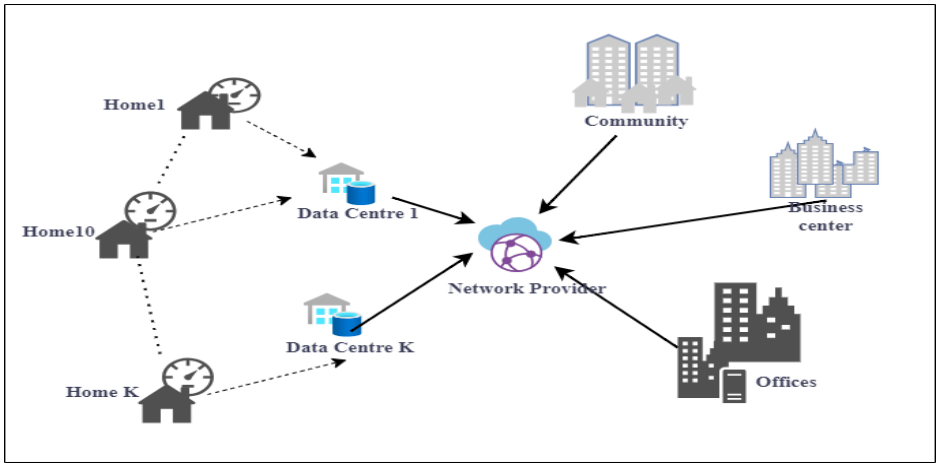

Figure 3. Proposed Model by Authors for Privacy Preserving Metering Scheme

The detailed overview of the modern privacy preserving mechanisms and different policies extended by different agencies are thoroughly disclosed by Anna Triantafyllou et. Al. through their research paper [4]. The authors have discussed about Advanced Metering Infrastructure, Privacy Policies, Privacy Standards, Smart Metering Components, Authentication Policies, Authentication Standards and various other verticals of the smart grids. The referred Advanced Metering Infrastructure is disclosed in the Figure 4.

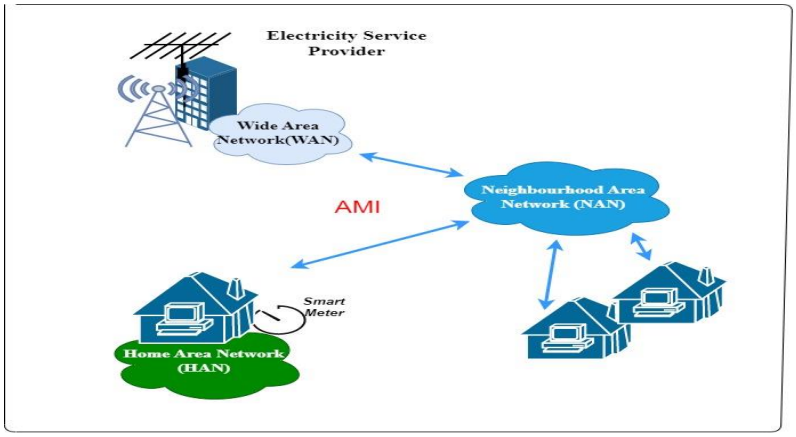

Figure 4. Advanced Metering Infrastructure

Through the other another literature [5], fault-tolerant data aggregation scheme has been proposed which is able to perform linear computation of the multidimensional data without third parties' involvement. Authors preferred Chinese residual theorem for encryption of the multidimensional data and the weight of the individuals. Additionally, Shamir secret sharing and bilinear mapping techniques have been employed to improve the proposed research work by implementing fault tolerance and user data integrity.

S. Chen et. al. [6] have demonstrated application of edge computing for smart grid systems which is designed using the Internet of Things. Through this research work authors have addressed the issues in the IoT based smart grid systems like response time, scheduling, maintenance, responsiveness to the end users and market responses. To address these issues, the novel architecture, has been introduced which merge the edge computing into IoT based smart grids.

In the demonstrated system which is built by considering the three important pillars like power distribution, micro-grid, and metering environments, it is possible to attain high level of privacy protection along with data prediction and grading strategies.

Whereas the possibility of the distributed and spatial aggregation scheme for data aggregation of the smart meter nodes has been disclosed by the Lei Zhang et. al. [7]. Author attempted to collect fine grained utility data of the appliances at each of the smart meter node in the smart grid environment. Furthermore, Panagiotis I. et. al. has disclosed exclusive mechanisms used to prevent the intrusion into the smart grid environment. [8] Application of Blockchain technology is demonstrated for authentication and data collection to provide firm security and privacy in the smart grid domain. Authors [9] integrates the ECC cryptography technique along with the blockchain to enhance the performance of the proposed system.

In another literature, Sarmadullah Khan et. al. [10] have discussed a novel communication scheme using the UPnP to implement auto discovery, plug and play networking interoperability, integration, privacy, and security features. Effectiveness of the scheme has been extended by implementing the communication between the HEG and appliances through UPnP protocol and having ECC based HTTP communication protocol for communication between the HEG and utility. Possibility of the application of tree-based threat model in advanced metering infrastructure in smart grid environment has been discussed by Rong Jiang et. al. [12]

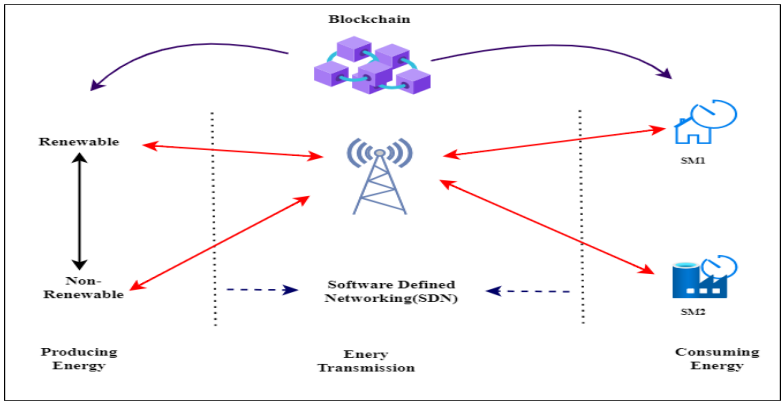

Figure 5. Distributed Energy Trading Model using Blockchain

Jonathan T. Lee et. al. has discussed exhaustive review on data sharing and privacy in electricity access through literature cited as [13]. While Simin Hu et.al have discussed novel energy efficient and privacy preserving scheme for data aggregation [14]. Further, Shen Wang et. al. has disclosed application of transfer learning to implement unified security model through software defined security mechanism [15]. Qian Zhou et. al. has discussed application of Chess-Board Alternations for development of defending mechanism for global attackers [16]. Xin Lu et. al. has discussed distributed energy trading model using Blockchain model [17] as shown in the following figure 7.

IV. PRIVACY AND SECURITY REQUIREMENT

A. Privacy Requuirements

The privacy implications of smart grid systems are valid and have been recognized as important considerations in the deployment of such technologies. Smart grids involve the continuous collection of data related to electricity consumption. This data, if not handled properly, poses a risk to consumer privacy. The detailed consumption data collected by smart grids can be used to create consumer profiles. This profiling can reveal intimate details of individuals lives, including their daily routines, appliance usage patterns, and lifestyles. The misuse of consumers data could have serious consequences, ranging from targeted criminal activities to unwanted surveillance and tracking threats. Utilities need to establish robust security measures for the storage of this sensitive information. While smart grid systems offer significant benefits in terms of energy efficiency and management, addressing privacy concerns is crucial to ensure the responsible and ethical deployment of these technologies. Striking a balance between technological innovation and the protection of individual privacy is key to fostering public trust in smart grid systems.

Summarizing the facts, we can write as:

- Without consumers authenticate identification details, any third party must not be allowed to link the consumed data.

- Consumers living behaviors should not be identifiable from consumed data to any third party.
- Third party should not be able to acquire and disclose the consumed data of the consumer.
- The consumed data must be handled considering the regulation and protection policies for data.

B. Security Requirements

The proposed study is mainly focused on the privacy requirements of the system. But, along with the privacy requirements, security concerns play an equally important role when talking about the sustainability of a system. Two main points when talking about the security requirements to be considered are as mentioned below:

- **Data Integrity:** Protecting data in transit is a critical aspect of ensuring the security of a system. To achieve this, it's important to implement measures that not only encrypt the data to prevent eavesdropping but also provide a mechanism for detecting unauthorized changes.
- **Data Confidentiality:** Given the diverse communication standards across different components in a smart grid, it's important to implement encryption in a way that is tailored to the specific requirements of each communication channel. Additionally, ensuring that consumption data is not disclosed in cleartext to intermediary data concentrators is essential for maintaining privacy.

V. PROPOSED SECURITY MODEL IMPLEMENTATION

Through this research work it is targeted to design a hardwired encrypted model to enhance the existing security model designed to protect the privacy of the individual node engaged in smart grid environments. The targeted system is designed using the ESP328 hardware architecture to provide the hardwired encryption model. Set of ESP processor architectures are engaged to provide encryption and decryption which are connected remotely through the Fire Base Server (FBS). At the user end of the smart grid environment, one of the ESP processors is engaged which takes care of the encrypting the personal and usage data of the consumer. This data is encrypted and sent over to the FBS. The data encryption is performed using the Advanced Encryption Standard (AES) 128-bit. Another ESP processor is placed remotely which is specifically used for decrypting the user information. Access to the database is provided through the Android application. User enters the key upon which the key is sent to the second ESP processor through FBS. At the ESP processor the received key is checked for the authenticity, if approved the correct data after decryption is sent over to the user through android application. In case if the key is mismatched, the data wrangling is performed and sent over to the android application.

In this system since the data encryption is performed using the hardware architecture, it is not possible to break up the encrypted data. Additionally, instead of placing the original data at the FBS, encrypted database is updated which will only be decrypted using ESP architecture if the key is matched, this gives additional security. Further, it is also evident that the data travel through the different nodes hence multi-hop communication environment is also supported. Also, the user gets the freedom to add required number of smart meters in one android application which gives flexibility to the user to alter the node changes at their ease. One more advantage we get through performing the encryption using popular Advanced Encryption Standard (AES). The in-depth implementation of the proposed system is carried out in terms of Encryption Model, Decryption Model and Android Activity. All the models are discussed in the subsequent sections. The systematic block diagram of the proposed system is disclosed through the following figure 6.

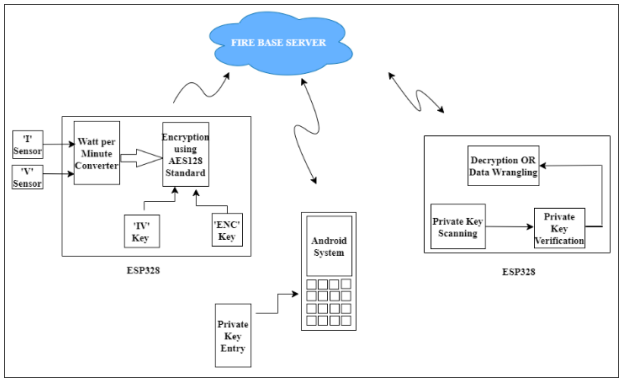

Figure 6. Block Diagram of the Proposed System

*A. **Encyption Model***

In the development of the proposed system, advanced encryption standard encryption algorithm is used to encrypt the data for secure transmission over long range. The AES standard is preferred over other encryption standards because of its diversity in nature like for 128-bit block size of encryption model, flexibly we can use 128-bit, 192-bit or 256-bit key for encryption due to which it is possible to have more secured encryption. While performing the encryption the matrix orientations is mapped column wise. Further, key expansion, GF (28) polynomial, shifting row-wise permutations are some of the exclusive features. Implementation of the encryption module of the proposed system is carried out on ESP-328 processor architecture. The module is described with reference to the following table I, which discloses the statement of the codes used for encryption. The exact process which is followed for implementing the encryption model can be discussed through the flow chart as disclosed through Figure 7.

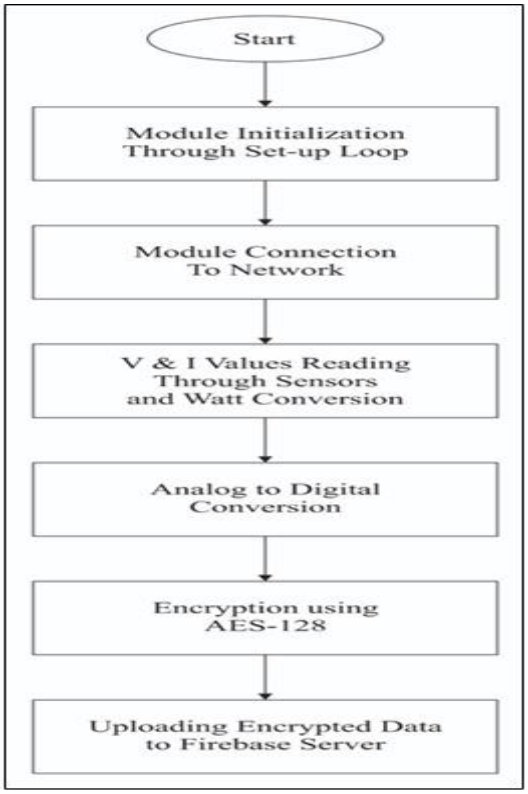

Figure 7. Flowchart of Encryption Model

Once we begin for implementation, the model first of all initiates set-up loop in which requirements from the available resources are reserved for course of execution and further, resources are defined like input ports and output ports. Next step in the implementation process is the module connection to the internet source. Here, the module connects through the wi-fi interface. The system is designed in such a way that it will read the current utilization of the Current (I) and Voltage (V), this is done through the current and voltage sensors which are connected to the ESP328 module. These values are read and converted into its equivalent digital quantity for further course of execution by the processor. Processor reads the utilization data and other personal information of the node and engage the AES-128 encryption protocol for encryption of the data. The encrypted data is then uploaded to the Firebase server. Firebase server is the central location where all encrypted data is stored for further processing. Here, since the encryption is carried out using hardware resources, it is called as hardwired encryption which gives additional security features as compared to soft encryption.

Precise implementation of the module can be discussed through the following lines of codes which begins with the declaration of the required libraries. In the encryption module, different functions which are described in the libraries like EmonLib.h, wifi.h, WifiClient.h, AESLib.h and different other libraries are included this has been discussed through first and second statement of the table-I.

TABLE I. IMPLEMENTATION OF ENCRYPTION MODEL

Sr. No.	Encryption Module Statement
1.	#include "EmonLib.h"
2.	#include <AESLib.h>
3.	#define BAUD 9600
4.	#include <FirebaseESP32.h>
5.	#define vCalibration 83.3
6.	#define currCalibration 0.50
7.	#define API_KEY "AIzaSyAy4YfEpdlAckQ96Q-bLfr3Ae6WXc5IiGU"
8.	
9.	#define DATABASE_URL "smart-metering-system-ac740-default-rtdb.firebaseio.com"
10.	#define USER_EMAIL "aes128@gmail.com"
11.	#define USER_PASSWORD "1234566123"
12.	#define METER_ID "1232"
13.	byte aes_key[] = {"123456789123456"};
14.	void
15.	aes_init(){aesLib.gen_iv(aes_iv);aesLib.setpadding mode ((paddingMode)0);}
16.	void print_key_iv() { }String encrypt(char * msg, byte iv[]) { }
17.	aesLib.encrypt64((byte*)msg, msgLen, encrypted, aes_key, sizeof(aes_key), iv);
	void setup() { Serial.begin(9600); ……}
	kWh = kWh + emon.apparentPower * (millis() - lastmillis) / 3600000000.0;

Further, all the communication is executed in serial transmission mode for which the baud rate has to be declared. In this case the required baud is set to 9600 bits per second, this indicates the number of bits which are transmitted per second from the ESP module. The baud is set by executing the statement number 3 of the module.

The firebase server is used as the central place to store the encrypted database of the client. The firebase server needs to be initialized before utilizing in the module, this is done through execution of the 4th statement of the table-I. In the proposed module, current and voltage parameters of the client node is recorded which is then used for calculating the power utilization. Precision of the module is calibrated by executing the 5th and the 6th statement of the code. Application key is defined in order to identify the targeted application. This key is defined with respect to the fire base server web address on which the encrypted databases are stored. This is done through the statement 7th and 8th one in the table-I. Targeted application is connected using the wi-fi connectivity module. The inbuilt Wi-fi module is connected using the Service Set Identity (SSID).

Unique credentials are created for each of the client nodes considering the email address and password and along with these credentials unique meter id is allocated to the node. This is executed using the statements 9th, 10th and 11th statements. Further, the AES-keys and IV-keys are generated for encryption purpose. This process is carried

out by executing the function described using 13 and 14 statements of the modules. The actual encryption of the collected data is executed using selected AES key. The encrypted data is then transmitted over the channel at 9600 bits per second for serial monitoring. The encryption of the data and serial transmission of the data is executed using the statement 15 and 16 of the table-I. Before transmission of the data the power utilization data is converted into watts per second to make it readable in the research work. This is done through execution of line number 17 of the encryption conde in table.

B. Decryption Model

The second dedicated module in the research work is the decryption module. In this module dedicated process of decryption is carried out. In the research work, the overall process of the cryptography is hardwired which means encryption and decryption is carried out on the hardware and hence the dedicated module is described and developed using another ESP hardware module. The tiny steps which are executed for implementation of the decryption model can be understood through the flowchart given in Fig. 12.

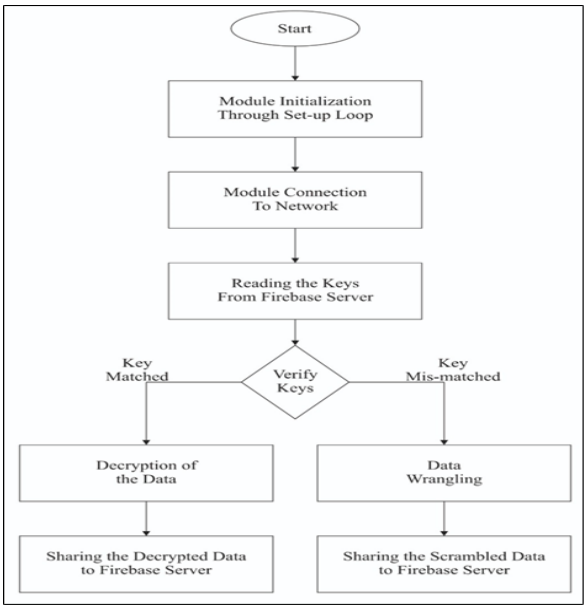

Figure 8. Flowchart of Decryption Model

The software routine which is described for development of the decryption module on ESP is discussed in Table II.

TABLE II. IMPLEMENTATION OF DECRYPTION MODEL

Sr. No.	Decryption Module Statement
1.	#include <AESLib.h>
2.	#include <FirebaseESP8266.h>
3.	#define API_KEY
4.	"AIzaSyAy4YfEpdlAckQ96Q-
5.	bLfr3Ae6WXc5IiGU"
6.	#define DATABASE_URL "smart-metering-system-ac740-default-rtdb.firebaseio.com"
7.	void aes_init() { aesLib.gen_iv(aes_iv);
8.	aesLib.set_ paddingmode ((paddingMode)0); String decode() { char decoded[200]; int b64len = base64_ decode(decoded, message, strlen(message)); return String(decoded); } if (dataRETRIVE121== key121)

	else { Serial.printf("Set string... %s\n", Firebase. setString (fbdo, F("/India_Server/Maharashtra /maharashtra_all/121/flag"),"0") ? "ok" : fbdo. errorReason().c_str());

The development of the process is naturally initiated through the declaration and definitions of the required libraries, packages, and functions. Some of the libraries are listed through line number 1 and 2 of the code as disclosed in the above table-II. Further the Wi-Fi credentials are read, and the module is connected to the internet source. To authenticate the application and to fetch the functions for execution and data communication, the API key in defined along with the database server. Definition of the API key and the database URL is done through the line number 3 and 4 of the code as disclosed above. Local objects are defined for data handling between the database server and the decryption module. To estimate the actual key for accessing the database padding process is perform which can be attain by executing the line number 5 of the code. The process of the decryption is initiated by executing the string decode () function, as disclosed through the line 6 of the code. While decrypting the message the keys are checked for the correctness, if keys are matched then the true values of the database are sent over to the android application, this is done through execution of the 7th statement and part of the subsequent code and if the key mismatch occurs, in that case the garbage values are sent over to the android applications, this is done through executing the line 8 of the code as disclosed in the above table-II.

*C. **Android Model***

Android module is the means through which it is possible to read the database of the node. The android application is designed using the android studio. The application development is done through development of various activities. Once we begin, the very first activity is the sign-up activity through which registration of new user is carried out. Here user must enter the credentials for registration. The second activity is the login activity, in which user must re-enter their credentials for entering to the application. Once the user enters the login credentials, then, user can add multiple meters in the application. This completes the registration process. Now, whenever, user want to access the previous data of utilization, user have to enter the private key, the key is communicated to the decryption module through Firebase server and another process is initiated as discussed in the decryption module.

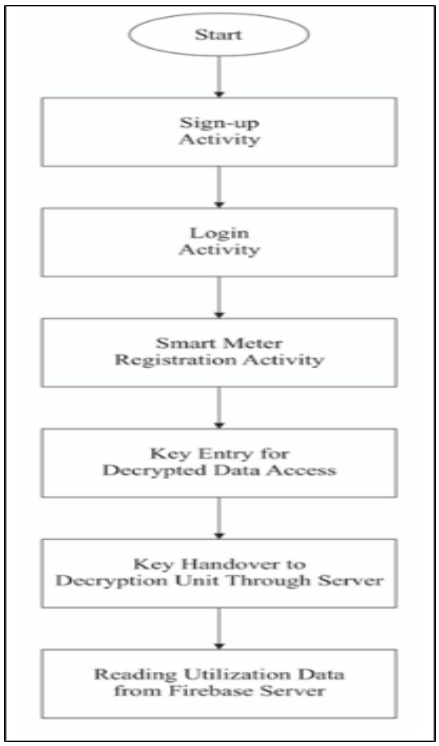

Figure 9. Flowchart of Android Model

The software development of the module is discussed with respect to the following table-III. For implementation of the module, different libraries are declared which are required for implementation of the module for reading the database from the Fire Base Server. This is done through the execution of statement 1, 2, 3 and 4 in the module. Immediately, public class is described using the main activity module. Through this module, different buttons, edit text console, progress bar, fire base server access module and other required modules are described. This execution is the part of the public class main activity as disclosed through statement 5 of the code in table-III.

TABLE III. IMPLEMENTATION OF ANDROID MODEL

Sr. No.	Decryption Module Statement
1.	package com.example.salinemonitaring;
2.	import android.os.Bundle;
3.	import com.google.firebase.auth.FirebaseAuth;
4.	
5.	import androidx.appcompat.app.AppCompatActivity;
6.	public class MainActivity2 extends AppCompatActivity { }
7.	auth = FirebaseAuth.getInstance();
	database=FirebaseDatabase.getInstance();

Subsequently, the firebase authentication is initiated to read the database instance into the local application. This is done by executing the statement 6 and 7 of the above code. Further different statements are executed for providing the sign-up activity, adding the meters of the nodes, adding the meters, inserting the credentials for reading the database and many other required fields. The outcome of the execution of the complete code as disclosed in the table-I, table-II and table-III are disclosed through the subsequent section.

VI. IMPLEMENTATION OF PRIVACY PROTECTION SCHEME USING RSA ALGORITHM

RSA is another algorithm which is used for cryptography purpose. It uses public and private key for encryption and decryption purpose. In spite of having many downsides RSA algorithm is used in many applications. Hence, in this research work, to juxtapose the difference between the AES and RSA algorithm, the research work is implemented using the RSA protocol and outcome is discussed. In order to precisely differentiate between the two algorithms, the discussion is carried out in an abstract way through the following table.

TABLE IV. AES AND RSA ABSTRACT DIFFERENCE

Attributes	AES Standard	RSA Standard
Encryption Type	Symmetrical	Asymmetrical
Key Length for Encryption	128 or 256	1024, 2048, 4096
Speed	Faster	Slower
Complexity	Low	Higher
Applications	Files and Databases	Authentication
Technique	Substitution-Permutation	Modular Exponentiation

Computation Cost	Low	High
Secrecy of Key Distribution	Secure Method	Not needed
Attack Resistance	Compromised if exposed to Brute-Force	Compromised if exposed to factoring techniques
Key Management	Calmer	Composite
Security Level	High	High (Depends on key size)
Hardware Implementation	Better suited for hardware implementation	Challenging
Standardization	NIST standard	Industry standard

The implementation of the RSA algorithm can be best discussed using the following table.

TABLE V. IMPLEMENTATION OF ANDROID MODEL

Sr. No.	**Module Statement**
1.	#include <RSALib.h>
2.	#define BAUD 9600
3.	byte rsa_key[] = { 0x35,0x50,0x70,0x36,0x87,0x54,0x34,0x98,0x21, 0x48,0x54,0x95,0x30,0x20,0x79,0x71 };
4.	byte rsa_iv[16] = { 1, 0, 2, 4, 0, 1, 0, 3, 8, 0, 1, 0,
5.	5, 0, 3, 9 };
6.	void RSA_init() { RSALib.gen_iv(rsa_iv);
7.	RSALib.set_paddingmode((paddingMode)0);
8.	void print_key_iv()
9.	String encrypt (char * msg, byte iv[])
10.	String decrypt (char * msg, byte iv[])
	void log_free_stack(String tag)
	void loop()

As discussed through the previous sections, the required RSA library is imported in the program which load all of the required predefined functions and variables in to the program. Here the library inclusion is done through the statement 1 as discussed in the above table v. Subsequently, the default baud rate is set to 9600 for communication purpose to the serial port. This is done by executing the second line of the code. Then, in the program rsa_key function is executed which assures the rsa_key initialization and generation of the private key for encryption and decryption process. This is done through execution of the line 3 to 5 of the statements on the program. The generated RSA key is communicated over the serial port at 9600 baud rates through execution of the line 6 of the program. Further, the actual encryption of the private message is encrypted by executing the string encrypt function defined in the program. The encoded message is displayed over the serial port. Accordingly, the message is decrypted by

executing the string decrypt function listed at line 8 in the above table. Finally, the log values indicating the time required for encryption and decryption is displayed over the serial port and the process is repeated in the loop for continuous reading of the private message, encryption and decryption process. The above two processes are executed using the line 9 and 10 of the above listed program.

VII. RESULTS AND DISCUSSIONS

In the proposed research work, three modules are designed. Out of which first modules take care of the reading the voltage and current data of the node. This data is converted into power consumption per second. It is encrypted and sent over to the fire base server. The Fire base server is configured to store all the encrypted data received from different nodes. The second module is designed to execute decryption function. Both above modules are designed using ESP processor architecture. The third module of the research work is designed using the android platform. This is the module through which user can access the database of node. Some of the glimpses of the above modules are disclosed through the following pictures.

The subsequent Figure 10 discloses the login console of the module. Once registered, the user has to enter the email and password for login into the system.

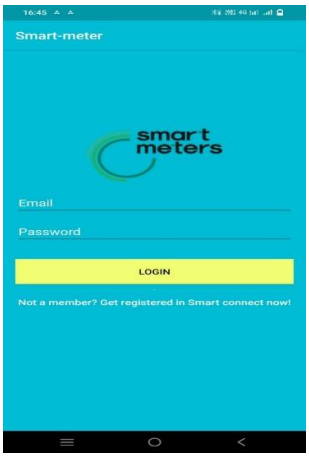

Figure 10. Login Console

Once the user enters the required credentials, new window opens up which shows all of the registered meter by the login user. This window is depicted in the subsequent Figure 11.

Figure 11. Registered Meters by the User

Through this console, user also gets the freedom to add different meters. Each of the meters are assigned with the unique meter id code. Upon selecting the meter, the meter reading can be read by inserting the unique key. The output of the meter readings has been depicted in the subsequent Fig 12.

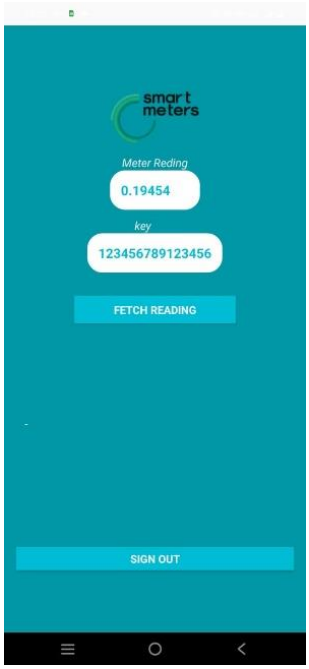

Figure 12. Meter Reading Indicating Power Utilization

Performance analysis of the proposed system with respect to the previously cited technologies, with respect to the different ascendency parameters have been discussed through the following table.

TABLE VI. STATISTICAL ANALYSIS

Sr. No	Scheme	Encryption (ms)	Decryption (ms)	Reference
1.	AES-128	0.77	--	[24]
2.	ECC	3158	--	
3.	AES-256	0.75008	0.12864	[25]
4.	AES (20MB)	1350.5	1844.5	[26]
5.	DES (20MB)	2356.5	2744.2	
6.	RSA (20MB)	6641	4	
7.	Blowfish	1355.2	1025.5	
8.	DES	713.7	126.3	[27]
9.	E-DES	635.8	432.5	
10.	T-DES	447.2	220.3	
11.	RSA	703.85	649.86	
12.	Blowfish	237.1	112.5	
13.	AES	175.4	186.2	
14.	AES	287	293	[28]
15.	Blowfish	293	290	
16.	DES	284	280	
17.	RC4	282	286	
18.	RSA	462	499	
19.	SM2	0.36	1.12	[29]
20.	RSA 512	0.4	8.1	[30]
21.	EC Elgamal	4.9	13.7	

22.	R-LWE (P1)	0.4	0.14	
23.	R-LWE (P2)	0.8	0.3	
24.	AES-128	0.158	0.206	[PROPOSED]
25.	RSA	0.510	0.450	[RECORDED]

Above table discloses the detailed statistical comparative analysis between the different outcomes disclosed by the authors in cited literature and the proposed techniques. Different authors have disclosed the time required for encryption and decryption for different encryption algorithms like AES, DES, Blowfish, RSA, RC4, SM2, EC Elgamal and different other cryptographic algorithms. It is evident that the with the proposed technique it is possible to encrypt the data in least amount of time that is within 0.158 ms duration. While if we consider decryption time, it is comparable with the AES-256 cited as [25]. But, considering the promising time saving in encryption, the addition decryption time of 0.07736 ms as compared to [25] is negligible. Later in the discussion, the implementation is also carried out using the RSA algorithm where, the algorithm took 0.510 milliseconds of time for encryption and 0.450 milliseconds of time for decryption purpose. This time for encryption process is much higher than the time required using the AES standard. It is also comparable to the one which is disclosed in the reference [27].

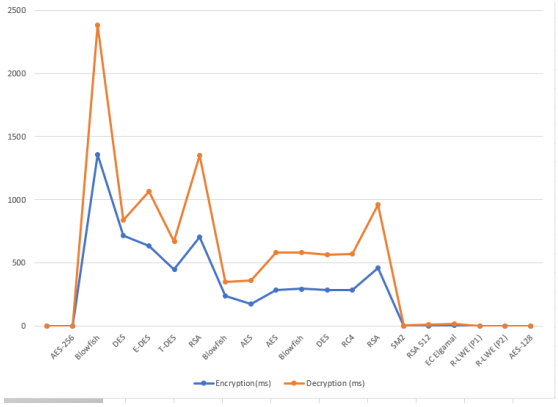

Figure 13. Graphical Representation for Statistical Analysis

Figure 14. Total Execution Time in Different Schemes

TABLE VII. COMPARISON OF AES IN DIFFERENT SCHEMES

Sr. No	Scheme	Encryption(ms)	Decryption(ms)
1.	AES-128 [24]	0.77	
2.	AES-256 [25]	0.75008	0.12864
3.	AES (20MB) [26]	1350.5	1844.5
4.	AES [27]	175.4	186.2
5.	AES [28]	287	293
6.	AES-128 [PROPOSED]	0.158	0.206

VIII. CONCLUSION

An Anti-Theft Model for Smart Grid Node in Multi-Hop Network Environment is designed to read the power utilization data through the current and voltage sensor at the user node. These readings are converted into power consumption per seconds and encrypted using advanced encryption standard and sent over to the server. Reading of the utilization data and the encryption process is carried out using ESP328 processor architecture. The Fire Base Server is used as the secured storage server where all meter's readings are encrypted and stored. Dedicated smart meter android application is designed through which Fire Base Server data can be fetched. A provision is made on this application to enrol new meters into the application after signing into the application. To fetch the meter data,

user have to enter the key into the application. Then, application communicates with the dedicated node designed, using another ESP328 module, for decrypting the utilization data. If the correct key is inserted at the android application, then decrypting unit transfer actual utilization reading to the android application while in case if wrong key is inserted then decrypting unit performs data wrangling and send wrong data to the android application. The complete research work has been disclosed through introduction, exhaustive literature review, implementation of the modules and finally through the results and discussion sections.

REFERENCES

[1] M. Akgün, E. U. Soykan and G. Soykan, "A Privacy-Preserving Scheme for Smart Grid Using Trusted Execution Environment," in IEEE Access, vol. 11, pp. 9182-9196, 2023, doi: 10.1109/ACCESS.2023.3237643.

[2] A. Guan and D. J. Guan, "An Efficient and Privacy Protection Communication Scheme for Smart Grid," in IEEE Access, vol. 8, pp. 179047-179054, 2020, doi: 10.1109/ACCESS.2020.3025788.

[3] X. He, X. Zhang and C. . -C. J. Kuo, "A Distortion-Based Approach to Privacy-Preserving Metering in Smart Grids," in IEEE Access, vol. 1, pp. 67-78, 2013, doi: 10.1109/ACCESS.2013.2260815.

[4] A. Triantafyllou, J. A. P. Jimenez, A. D. R. Torres, T. Lagkas, K. Rantos and P. Sarigiannidis, "The Challenges of Privacy and Access Control as Key Perspectives for the Future Electric Smart Grid," in IEEE Open Journal of the Communications Society, vol. 1, pp. 1934-1960, 2020, doi: 10.1109/OJCOMS.2020.3037517.

[5] Z. Song, T. Zhou, W. Zhong, D. Chen, L. Liu and X. Yang, "Fault-Tolerant Data Aggregation Scheme Supporting Fine-Grained Linear Operation in Smart Grid," in IEEE Access, vol. 11, pp. 68525-68537, 2023, doi: 10.1109/ACCESS.2023.3292586.

[6] S. Chen et al., "Internet of Things Based Smart Grids Supported by Intelligent Edge Computing," in IEEE Access, vol. 7, pp. 74089-74102, 2019, doi: 10.1109/ACCESS.2019.2920488.

[7] L. Zhang, J. Zhang and Y. H. Hu, "A Privacy-Preserving Distributed Smart Metering Temporal and Spatial Aggregation Scheme," in IEEE Access, vol. 7, pp. 28372-28382, 2019, doi: 10.1109/ACCESS.2019.2899961.

[8] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems," in IEEE Access, vol. 7, pp. 46595-46620, 2019, doi: 10.1109/ACCESS.2019.2909807.

[9] C. -D. Lee, J. -H. Li and T. -H. Chen, "A Blockchain-Enabled Authentication and Conserved Data Aggregation Scheme for Secure Smart Grids," in IEEE Access, vol. 11, pp. 85202-85213, 2023, doi: 10.1109/ACCESS.2023.3301570.

[10] S. Khan, R. Khan and A. H. Al-Bayatti, "Secure Communication Architecture for Dynamic Energy Management in Smart Grid," in IEEE Power and Energy Technology Systems Journal, vol. 6, no. 1, pp. 47-58, March 2019, doi: 10.1109/JPETS.2019.2891509.

[11] F. Liang, W. Yu, D. An, Q. Yang, X. Fu and W. Zhao, "A Survey on Big Data Market: Pricing, Trading and Protection," in IEEE Access, vol. 6, pp. 15132-15154, 2018, doi: 10.1109/ACCESS.2018.2806881.

[12] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen and X. Shen, "Energy-theft detection issues for advanced metering infrastructure in smart grid," in Tsinghua Science and Technology, vol. 19, no. 2, pp. 105-120, April 2014, doi: 10.1109/TST.2014.6787363.

[13] J. T. Lee, J. Freitas, I. L. Ferrall, D. M. Kammen, E. Brewer and D. S. Callaway, "Review and Perspectives on Data Sharing and Privacy in Expanding Electricity Access," in Proceedings of the IEEE, vol. 107, no. 9, pp. 1803-1819, Sept. 2019, doi: 10.1109/JPROC.2019.2919306.

[14] S. Hu, L. Liu, L. Fang, F. Zhou and R. Ye, "A Novel Energy-Efficient and Privacy-Preserving Data Aggregation for WSNs," in IEEE Access, vol. 8, pp. 802-813, 2020, doi: 10.1109/ACCESS.2019.2961512.

[15] S. Wang, J. Wu, S. Zhang and K. Wang, "SSDS: A Smart Software-Defined Security Mechanism for Vehicle-to-Grid Using Transfer Learning," in IEEE Access, vol. 6, pp. 63967-63975, 2018, doi: 10.1109/ACCESS.2018.2870955.

[16] Q. Zhou, X. Qin and X. Xie, "Hiding Contextual Information for Defending a Global Attacker," in IEEE Access, vol. 6, pp. 51735-51747, 2018, doi: 10.1109/ACCESS.2018.2869947.

[17] J. Estrada-Jiménez, J. Parra-Arnau, A. Rodríguez-Hoyos, J. Forné and E. Pallarés-Segarra, "A Measurement Study of Online Tracking and Advertising in Ibero-America," in IEEE Access, vol. 9, pp. 80996-81007, 2021, doi: 10.1109/ACCESS.2021.3085024.

[18] S. P. Mohanty, E. Kougianos and P. Guturu, "SBPG: Secure Better Portable Graphics for Trustworthy Media Communications in the IoT," in IEEE Access, vol. 6, pp. 5939-5953, 2018, doi: 10.1109/ACCESS.2018.2795478.

[19] T. S. Ustun and S. M. S. Hussain, "IEC 62351-4 Security Implementations for IEC 61850 MMS Messages," in IEEE Access, vol. 8, pp. 123979-123985, 2020, doi: 10.1109/ACCESS.2020.3001926.

[20] X. Lu et al., "Blockchain-Based Distributed Energy Trading in Energy Internet: An SDN Approach," in IEEE Access, vol. 7, pp. 173817-173826, 2019, doi: 10.1109/ACCESS.2019.2957211.

[21] Y. -J. Lin, Y. -C. Chen, J. -Y. Zheng, D. -W. Shao, D. Chu and H. -T. Yang, "Blockchain-Based Intelligent Charging Station Management System Platform," in IEEE Access, vol. 10, pp. 101936-101956, 2022, doi: 10.1109/ACCESS.2022.3208894.

[22] F. Yu, J. Peng, X. Li, C. Li and B. Qu, "A Copyright-Preserving and Fair Image Trading Scheme Based on Blockchain," in Tsinghua Science and Technology, vol. 28, no. 5, pp. 849-861, October 2023, doi: 10.26599/TST.2022.9010066.

[23] H. Keko, P. Hasse, E. Gabandon, S. Sučić, K. Isakovic and J. Cipriano, "Secure standards-based reference architecture for flexibility activation and democratisation," CIRED 2020 Berlin Workshop (CIRED 2020), Online Conference, 2020, pp. 584-587, doi: 10.1049/oap-cired.2021.0123.

[24] Shijo Mathew T. and Suresh Sankaranarayanan, Performance Analysis of Security Protocols in Smart Energy Meter System, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 19 (2017) pp. 8294-8315.

[25] A.-M. Dariush and N. Morteza, "Design and microcontroller-based hardware performance analysis of a security-enhanced lightweight communication scheme for smart grid", Security Privacy, vol. 1, no. 5, pp. e34, 2018.

[26] Panda, Madhumita. (2016). Performance analysis of encryption algorithms for security. 278-284. 10.1109/SCOPES.2016.7955835.

[27] O. G. Abood, M. A. Elsadd and S. K. Guirguis, "Investigation of cryptography algorithms used for security and privacy protection in smart grid," 2017 Nineteenth International Middle East Power Systems Conference (MEPCON), Cairo, Egypt, 2017, pp. 644-649, doi: 10.1109/MEPCON.2017.8301249.

[28] Hossain, Md. Alam & Hossain, Md & Uddin, Md & Imtiaz, Shariar Md. (2016). Performance Analysis of Different Cryptography Algorithms. International Journal of Advanced Research in Computer Science and Software Engineering.

[29] Kehe Wu, Rui Cheng, Wenchao Cui, Wei Li, A lightweight SM2-based security authentication scheme for smart grids, Alexandria Engineering Journal, Volume 60, Issue 1, 2021, pp. 435-446, ISSN 1110-0168, https://doi.org/10.1016/j.aej.2020.09.008.

[30] Agarkar AA, Agrawal H. LRSPPP: lightweight R-LWE-based secure and privacy-preserving scheme for prosumer side network in smart grid. Heliyon. 2019 Mar 12;5(3):e01321. doi: 10.1016/j.heliyon.2019.e01321. PMID: 30911691; PMCID: PMC6416661.