ISSN No:-2456-2165

Secure Data transmission trading protocol for networked DC Smart Micro-grids Based on hybrid cryptography and Multi-Agent-Based Controlling

[1]Mouachi Raja
LAMIGEP, EMSI
Marrakesh, Morocco

[2]Remmach Hassnae
LAMIGEP, EMSI
Marrakesh, Morocco

[3]Fatima Gharnati
I2SP Team, FSSM, Cadi Ayyad University
Marrakesh, Morocco

[4]Mustapha Raoufi
LMEE Laboratory, FSSM, Cadi Ayyad University
Marrakesh, Morocco

Abstract:- The DC Smart micro-grid (DC-SM) communication network with proper connectivity among DC-SM resources is play important role to maintain a stability and reliability of the DC-SM. Application of suitable communication network and protocol and highlighted the best security measurement is one of the elements to achieve those broad objectives. To secure the communication network and protocol, many security approaches is proposed. In this paper, a review of DC-SM communication and its security is shown and future direction of communication network and protocol with its security also provided. Many cryptographic algorithms have been developed to maintain the security and integrity of the data of DC-SM. This paper proposes a secure and optimized scheme for sharing data while maintaining data security and integrity over the S-MG. The improved hybrid cryptography technique is ideal for secure S-MGs communication due to the speed of operation and higher degree of security that it offers. The objective of this paper is to develop an enhanced technique That mainly functions by combining the Menzes-Vanstone Elliptic Curve Cryptosystem (MV-ECC) and the 128-bit Advanced Encryption Standard (AES) method to ensure authentication and data integrity. This new technique exploits the advantages of the symmetric and asymmetric cryptographic techniques. Moreover, we have modelled the proposed approach by using the multi-agent system (M-A-S), to manage the complexity of different process. The present work proposed a hybrid algorithm for DC-SM architecture. The MV-ECC-AES algorithm improves the performance of the encryption algorithms, since it encrypts the data in a minimum time and in a secure way. The proposed algorithm is much secured than 128-AES for DC-SM and less resource and time consuming than MV-ECC.

Keywords:- *DC Smart Microgrid; Security, Cryptography; Advanced Encryption Standard (AES); Menzes-Vanstone Elliptic Curve Cryptosystem (MV-ECC); Multi-Agent System (M-A-S).*

I. INTRODUCTION

A increases in energy use necessitates safer and more effective energy production and transmission. Information and communications technology assist in supplying efficient, dependable, and sustainable energy in AC power system operations [1].

A key target of cyber assaults is the smart grid because of its greater network connection.

Due to on-site generation, distribution weaknesses in micro-grids are considerably reduced.

Local or on-site power generation is defined by the US Energy Information Administration as electricity that is self-generated, produced by the same entity that consumes the power or an affiliate, used in the direct support of a service or industrial process located within the same facility or group of facilities that house the generating equipment, and self-produced. A DC smart micro-grid (DC-SM) example is shown on Figure 1.

These microgrids may function with the AC utility grid in a connected or island mode. When there are disruptions on the utility side, the microgrid will cut itself off from the utility grid. The data exchange system in microgrids is anticipated to deliver performance benefits by utilizing network segmentation.

ISSN No:-2456-2165

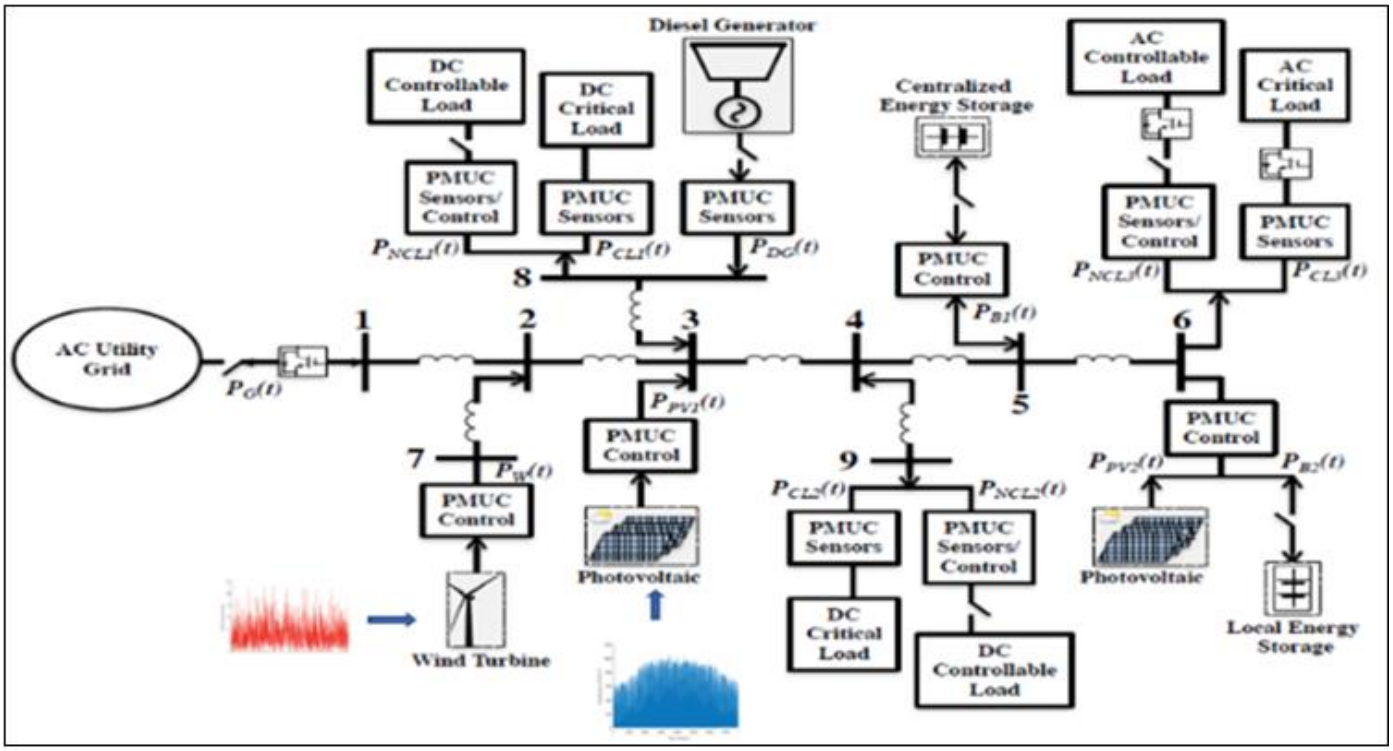

Fig 1 An example of a network of DC-SM with Power Management Unit Controllers (PMUCs).

DC-SMs might also remove the energy waste connected with the conversion of AC to DC and the majority of transmission and distribution losses [2].

A DC-SM control system has to be designed with more resilience.

Microgrids are susceptible to cyberattacks despite the fact that some security issues have been substantially resolved [3].

This article discusses critical microgrid cyber security challenges and suggests research to identify potential solutions.

II. ISSUES WITH CYBER SECURITY

A. DC-SM Subchannel Analysis

This section analyzes cyberattacks and the threat they pose to the DC-SM.

Background attak: Continuous power availability for customers and situational understanding of microgrid circumstances need real-time monitoring. At the DC-SM nodes, including renewable energy sites (sources) and DC loads, equipment like DC smart meters, Power Management Unit Controllers (PMUCs), and generators are utilized to monitor DC power and energy.

Researchers created DEMS in [4] to execute intelligent energy dispatch in real-time dynamic optimization of energy generated in a DC-SM. Based on current data from sensors and energy meters, the system modified the energy dispatch.

Power and energy meter communication side channel timing attack: Side-channels analysis extracts information by looking at implementation artifacts. For instance, the system password for SSH has been extracted from interactive sessions and the protocols employed in the encrypted interactions have been identified [12].

Due to its reliance on real-time measurement data, the DC-SM is susceptible to DoS/DDoS attacks.

B. Distributed Denial of Service (DDoS) attaks

The Distributed Denial of Service (DDoS) attacks exhaust system resources by sending flood request to prevent legitimate user from accessing the system. The effects of DDoS attacks on DC-SM could be catastrophic. DDoS attacks exploit flaws in network protocols so that a victim system have to spend more time and resource to process attackers bad request.

C. Meter Privacy Leakage

Wireless technology is used by Advanced Metering Infrastructure to gather information about power use remotely. Electricity use patterns, which reflect client habits and lifestyles, may be easily extrapolated from the collected data as it becomes more and more exact. The data may subsequently be utilized to identify vacant homes, develop targeted marketing campaigns, or even conduct crimes [5]. Studies reveal that Advanced Metering Infrastructure meters utilize a fundamental frequency hopping method.

According to studies, Automatic Meter Reading meters are simple targets for eavesdropping and spoofing attacks since they broadcast readings in plain text every 30 seconds using a simple frequency hopping wireless communication protocol [6].

ISSN No:-2456-2165

D. Software bugs and malware

Malware poses a serious danger to today's electrical systems, even if there haven't been any notable power outages or system breakdowns that can be directly attributed to it.

The most well-known malware instance is the computer worm Stuxnet, which was found in June 2010. Nearly one-fifth of Iran's nuclear centrifuges are said to have been destroyed [7].

According to reports, Stuxnet infiltrated Iranian PLCs, gathered data from industrial systems, and caused the fast-spinning centrifuges to self-destruct. It is the first malware to be identified that monitors and compromises industrial systems [8] and the first to have a rootkit for Programmable Logic Controllers (PLCs) [9], [10].

III. DC SMART MICRO-GRID CYBERSECURITY OBJECTIVES

A scale system known as a DC smart microgrid connects each power-consuming gadget to a power producing plant [11]. The potential for remote control of the power management and distribution system has increased due to this scale nature. An DC-SM must have the highest level of security against theft, misuse, and malicious activities because energy is a valuable resource. The issues of guaranteeing cybersecurity in an DC-SM are distinct in nature due to the variety of components and circumstances in which DC-SM are used. Due to sophisticated cyberattacks that might not be noticed, implementing an DC-SM without strong and strict security measures can jeopardize the entire system [12]. Inadequate security measures can potentially compromise the DC-SM network's stability [13].

Three cybersecurity goals must be guaranteed [12] in order to guarantee the cybersecurity of DC-SMs:

- Integrity: Defense against unauthorized alteration of DC-SM data. Unauthorized information alteration results in poor management or the abuse of authority.
- Protection of information and privacy through authorized access and disclosure limits is known as confidentiality.
- Accessibility: Make information and services dependable and timely. In DC-SMs, availability can be jeopardized by preventing access to information, which can halt the flow of power.

For our study we will focus on cryptographic algorithms in order to ensure the objective of confidentiality and to remedy the attacks mentioned previously.

IV. METHODOLOGY

The highest emphasis is data security. Transferring data must be done securely and safely. Numerous cryptographic techniques have been proposed and put into use to provide such services. The two primary categories of cryptography algorithms are the symmetric technique and the asymmetric approach:

A symmetric technique is one in which the encryption and decryption keys are the same single key. It is characterized by speed due to its relatively simple implementation, but it is less secure because the key is needed for both encryption and decryption during transmission. Based on the amount of data handled, block chipper and stream chipper are two groups of symmetric algorithms [11].

The encryption key and the decryption key are not the same when employing an asymmetric algorithm. In this procedure, two keys—the public key and the private key—were used. It stands out for its excellent security but is sluggish owing to the numerous computations required [14].

Our strategy involves combining the symmetric and asymmetric approaches to establish a highly secure environment for data transit. Through, we have developed a hybrid algorithm that is both user-friendly and sufficiently safe to provide adequate data protection. We use the Menzes-Vanstone Elliptic Curve Cryptosystem (MV-ECC).

A. AES Algorithm Overview

AES is a symmetric encryption technique. The approach has a constant block size of 128 bits and requires a cryptographic key length of 128, 192, or 256 bits [14], [11]. The flowchart for the 128-AES encryption procedure is shown in Figure 2.

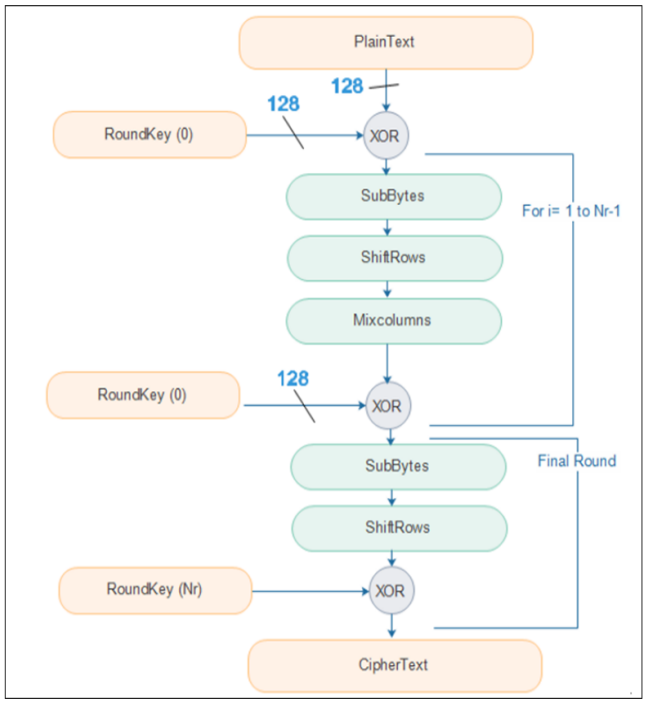

Fig 2 Process of 128-AES Encryption Flowchart.

B. Overview of the Elliptic Curve Cryptosystem

Miller and Thomas Watson separately devised the elliptic curve cryptosystem (ECC), an asymmetric cryptography method, in 1980 [15], [16]. The elliptic curve scalar multipli-cation (ECSM), which causes confusion in all ECC protocols, including encryption, decryption processing, key generation, and key exchange, is the core function of the elliptic curve cryptosystem.

An elliptic curve's (EC) equation over a field of prime numbers Fp is given by:

$y^2 \equiv (x^3 + ax + b)(mod\ p)$, Where a,b ϵ Fp , p ≠ 2,3, and satisfy the condition $(4a^3 + 27b^2)$ is not 0 [16].

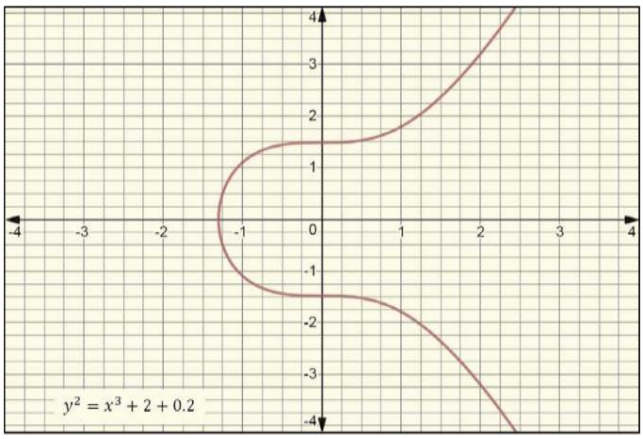

Fig 3 Elliptic curve cryptosystem.

Suppose that $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$, $P \neq Q$ are two points that lie on an EC, respectively. The third point R, which likewise sits on EC, is produced by adding P and Q. P and Q should be included. The study's case studies are listed below [17]:

If $P \neq Q \neq 0$ with $x_P \neq x_Q$, then sum of P and Q in this case is defined by:

$$P + Q = R = (x_R, y_R) \quad (1)$$

Where,

$$\lambda = \frac{(y_Q - y_P)}{(x_Q - x_P)} \quad (2)$$

$$x_R \equiv (\lambda^2 - x_P - x_Q)\ (mod\ p) \quad (3)$$

$$y_R \equiv \lambda(x_P - x_R) - y_P)\ (mod\ p) \quad (4)$$

If $x_P = x_Q$ but $y_P \neq y_Q$ then $P + Q = 0$.

$P = (x_P, y_P)$ is a point that sits on the EC. The phrase doubling P and Q on an EC refers to adding the point P to itself [17]. Specifically

$$P + P = 2P = R = (x_R, y_R) \quad (5)$$

$$\lambda = \frac{3\,x_P^2 + a}{2y_P} \quad (6)$$

$$x_R \equiv (\lambda^2 - 2x_P)(mod\ p) \quad (7)$$

$$y_R \equiv (\lambda(x_P - x_R) - y_P)(mod\ p) \quad (8)$$

Assume that $\boldsymbol{P} = (\boldsymbol{x_P}, \boldsymbol{y_P})$ is a point that lies on EC and that K is an integer. The following characteristics of scalar multiplication:

$$kP = \underbrace{P + P + \cdots + P}_{k-times} \quad (9)$$

C. Menezes-Vanstone Elliptic Curve Cryptosystem (MV-ECC) Overview

The Menezes-Vanstone ECC cryptographic algorithm. There is no counterpart for discrete logarithm issues in this strategy. Therefore, the DC-SM sender just has to disguise the message rather than embed it on the EC [18].

The EC and base point G must first be decided upon by the $DC-SM_1$ and $DC-SM_2$ before the $DC-SM_1$ may send a message to the $DC-SM_2$ with the format Message=(m_A, m_B). Each party chooses a private key at random from the range [1,n]; d for $DC-SM_1$ and e for $DC-SM_2$, and then multiplies that private key by the base point (P_1=n_1.G and P_2=n_2.G) to get their respective public keys. $DC-SM_1$ multiplies his private key by $DC-SM_2$public key to create the secret key K:

$$K = n_1.P_1 = n_1.P_2 = n_2.n_1.G = (k_A, k_B) \quad (10)$$

The message is then ciphered using calculations:

$$c_A = m_1 * k_A\ mod\ p$$

$$c_B = m_2 * k_B\ mod\ p$$

D. Data Encryption Standard (DES) Overview

The Federal Information Processing Standard (FIPS) was created in 1977 using the early symmetric encryption technique known as DES, which was developed by IBM in 1972. Electronic data is encrypted using the symmetric key encryption method known as DES. Block cipher DES has a 64-bit key, however only 56 bits of the key are useful; the remaining bits are utilized for parity. There are two initial and final permutations, as well as 16 circular permutations [20]. The 56-bit key size, which generates 7.2*1016 possible keys, powers DES [17] in normal threat settings, as illustrated in Figure 4.

E. 3 Data Encryption Standard (3DES) Overview

The initial concept was called "Triple Data Encryption Standard (3DES)" and was standardized in ANSI X9.17 and ISO 8732. It was initially expected by IBM in 1998. The Feistel architecture's three key choices form the foundation of this algorithm. The key is 48 bits long and may be divided into 16 subkeys with 8 s blocks. It employs the exact decryption technique seen in Figure 4 [20] [17].

ISSN No:-2456-2165

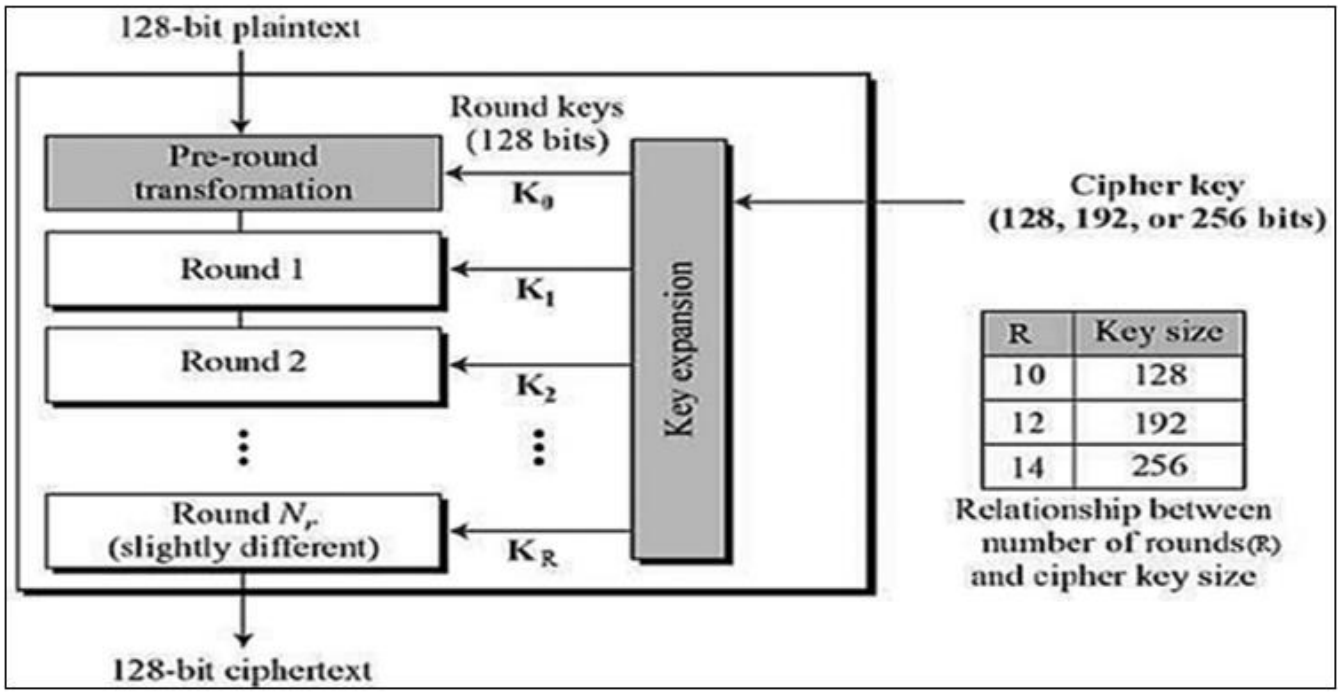

Fig 4 (A) DES Encryption Algorithm. (B) 3DES Encryption Algorithm.

F. Blowfishes Overview

Blowfishe is a symmetric cipher that depends on a Feistel structure and has a changeable key length. It has a key that is between 32 and 448 bits long and a block size of 64 bits. It has a broad box that depends on the key and consumes 16 rounds. The Blowfish algorithm uses the same process for decryption in reverse, and it has four S boxes [19]. as seen in Figure 5 The primary size of blowfish is what provides a great level of protection. The master key has been used in several rounds, making multiple key attacks improbable because the master key is immune to them.

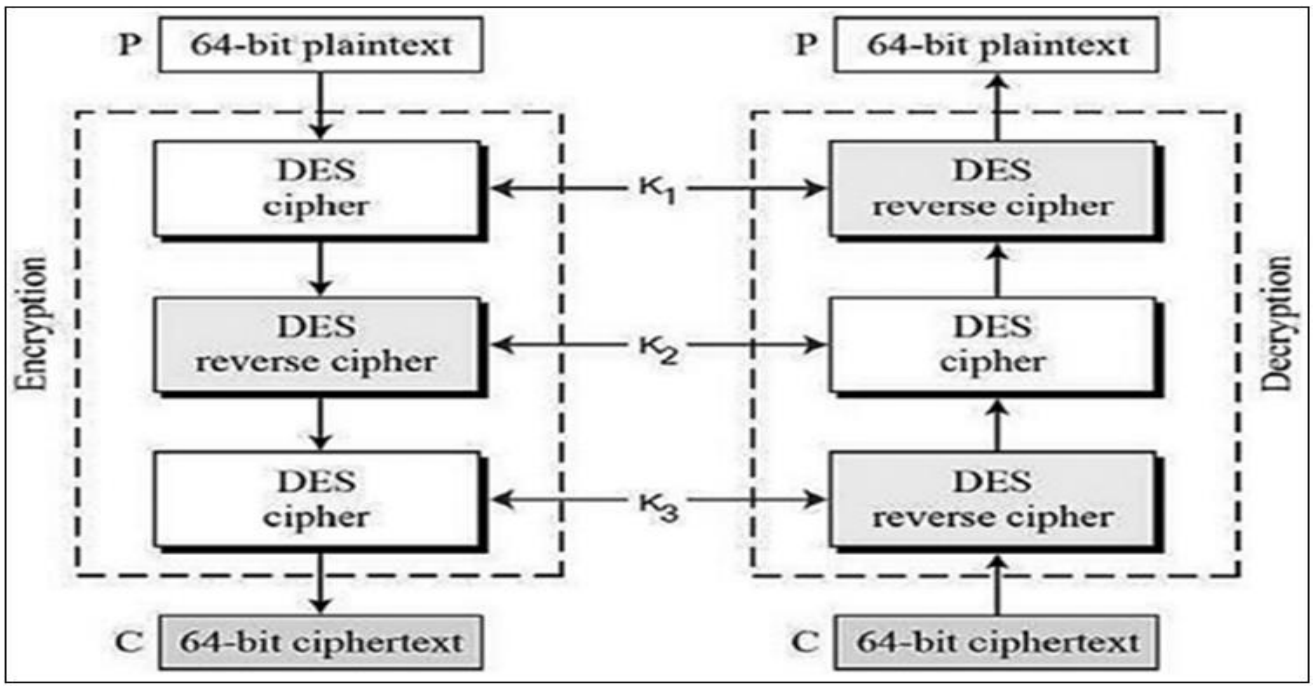

Fig 5 Blowfish Encryption Algorithm.

V. PROPOSED STRATEGY

We described our hybrid MV-ECC-AES method for securing DC-SM in this part (Figure 6). The four phases of this novel technique for encrypting and decrypting data in DC-SM are as follows:

- *Step I: Pre-treatment*

Before sending any Message, this stage involves initializing the resources. The following pre-treatment phase will occur:

ISSN No:-2456-2165

All DC-SM nodes will first get the general point and the common EC that is situated on it.

This action must be established over a secure channel by all S-MG nodes.

The only operation that has to be done on a secure channel is this one. It will only be executed once while the S-MG node is operational.

➢ *Step II: Key creation*

To address the issue with the 128-AES technique, the key will be generated using MV-ECC.

The following actions are necessary for this step's key generation:

A random number will be selected by the DC-SM sender and recipient, n_1 [1, p-1].

Its private key will be referred to as this random number.

The DC-SM sender will now calculate its P_1 public key by dividing its n_1 private key by the shared common point $P_1 = n_1.G$ that was used during setup.

All other DC-SM nodes will get a broadcast of this P_1 public key.

The key used in the preceding data encryption will be the G general.

➢ *Step III: encryption*

These actions are necessary for this step:

Before transferring data, the first round will be separated into blocks of 128 bits.

The key obtained in the previous step will be used to apply the second round, once divided, of 10 rounds of 128-AES to this data.

The key will be appended to the data in each round and have a constant length of 128 bits.

The recipient DC-SM node will receive the encrypted data over the unprotected channel.

➢ *Step IV: decryption*

Receivers will employ MV-ECC keys to unlock the original data using 128-AES decryption.

A DC-SM node will create its private key at random and obtain its public key by multiplying its private key by the general point in the graph that serves as the key for the most recent transmission.

Each time data is sent, a new encryption and decryption key is generated. We encrypt and decode data using 128-AES, and we generate keys using the MV-ECC technique.

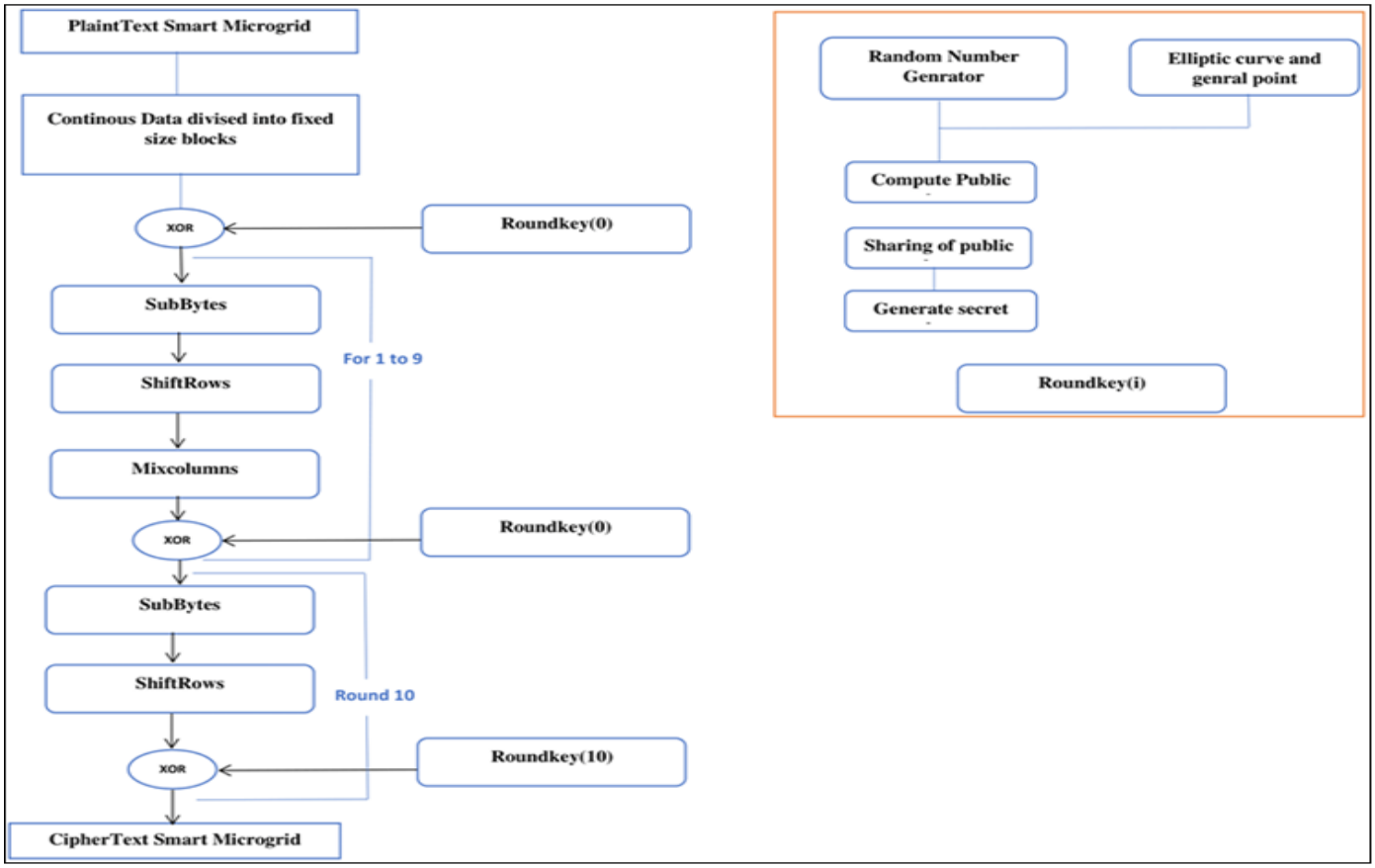

Fig 6 Flowchart of MV-ECC-AES Algorithm.

ISSN No:-2456-2165

In this work, a hybrid cryptography method is introduced. The MV-ECC algorithm's simplicity of key distribution and the 128-AES method's speedy calculation capabilities are combined in the MV-ECC-AES algorithm that is being suggested. With such, DC-SM communication can be secured rapidly and effectively. Figure 6 shows the block diagram for MV-ECC-AES.

VI. RESULTS AND DISCUSSION

We carried out comprehensive experiments to examine the efficacy of our algorithm. The encryption time for various was the criterion we settled on. The length of time required to encrypt data using the various symmetric techniques and the suggested hybrid approach is shown in Figure 7.

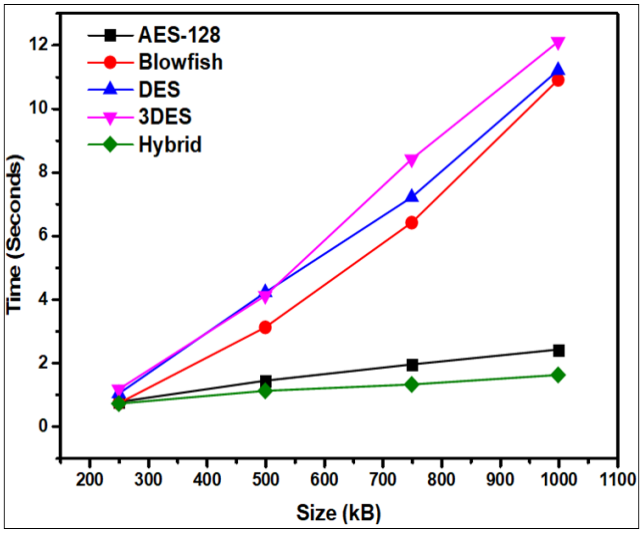

Fig 7 The Time Consumed in Encrypting Data using Each Algorithm.

The findings in Figure 7 demonstrate that, in comparison to the other methods examined, our MV-ECC-AES approach takes less simulation time.

In contrast to our approach, which encrypts the same information in 1.2 seconds, the 128-AES algorithm takes 1.43 seconds to simulate a file of 500 kB in size.

We also assessed the algorithms based on throughput, which was determined by dividing the file size in bytes by the amount of time spent, expressed in seconds, as stated in the equation below:

$$\text{Th} = \frac{\text{F}}{T_E} \qquad (11)$$

Where,

Th : throughput;

F : File size;

TE : Encryption time.

The throughput utilizing the various symmetric methods and the suggested hybrid approach is shown in Figure 8.

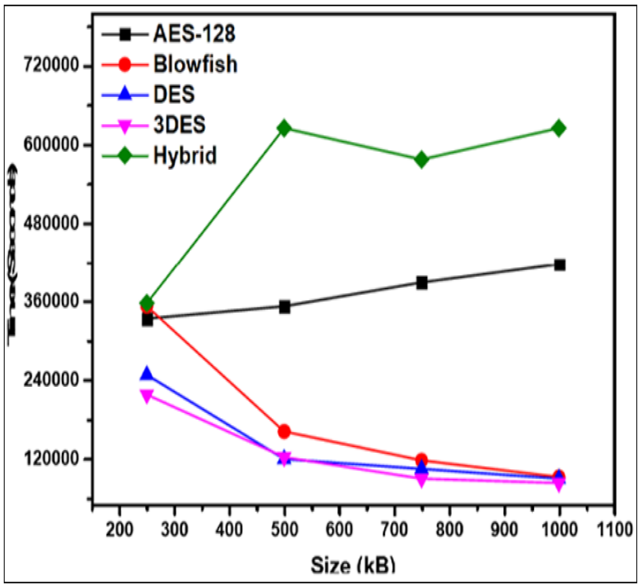

Fig 8 The Throughput using Each Algorithm.

Figure 7 displays the findings of how much time each technique required to encrypt data. And the throughput data are shown in Figure 8.

The suggested hybrid algorithm turned out to be the most effective way to communicate in the DC-SM while still being safe, genuine, and adaptable. Additionally, several comparison findings demonstrated that the hybrid algorithm worked well across the board.

VII. MULTI-AGENT BASED MODELING

Currently, multi-agent systems (M-A-S) are a novel technology for the design and management of DC-SM. This system typically has many key characteristics, including parallelism, resilience, and scalability. It is made up of autonomous software and hardware units known as agents.

Given the ongoing research in S-MGs, this area is becoming more and more complex. To address this issue, we have proposed an approach that consists of six M-A-S: user interface agent, control agent, resource agent, key generation agent, and data encryption agent. These M-A-S work together to accomplish the task of secure communications in DC-SM. Our suggested M-A-S is illustrated in Figure 9.

ISSN No:-2456-2165

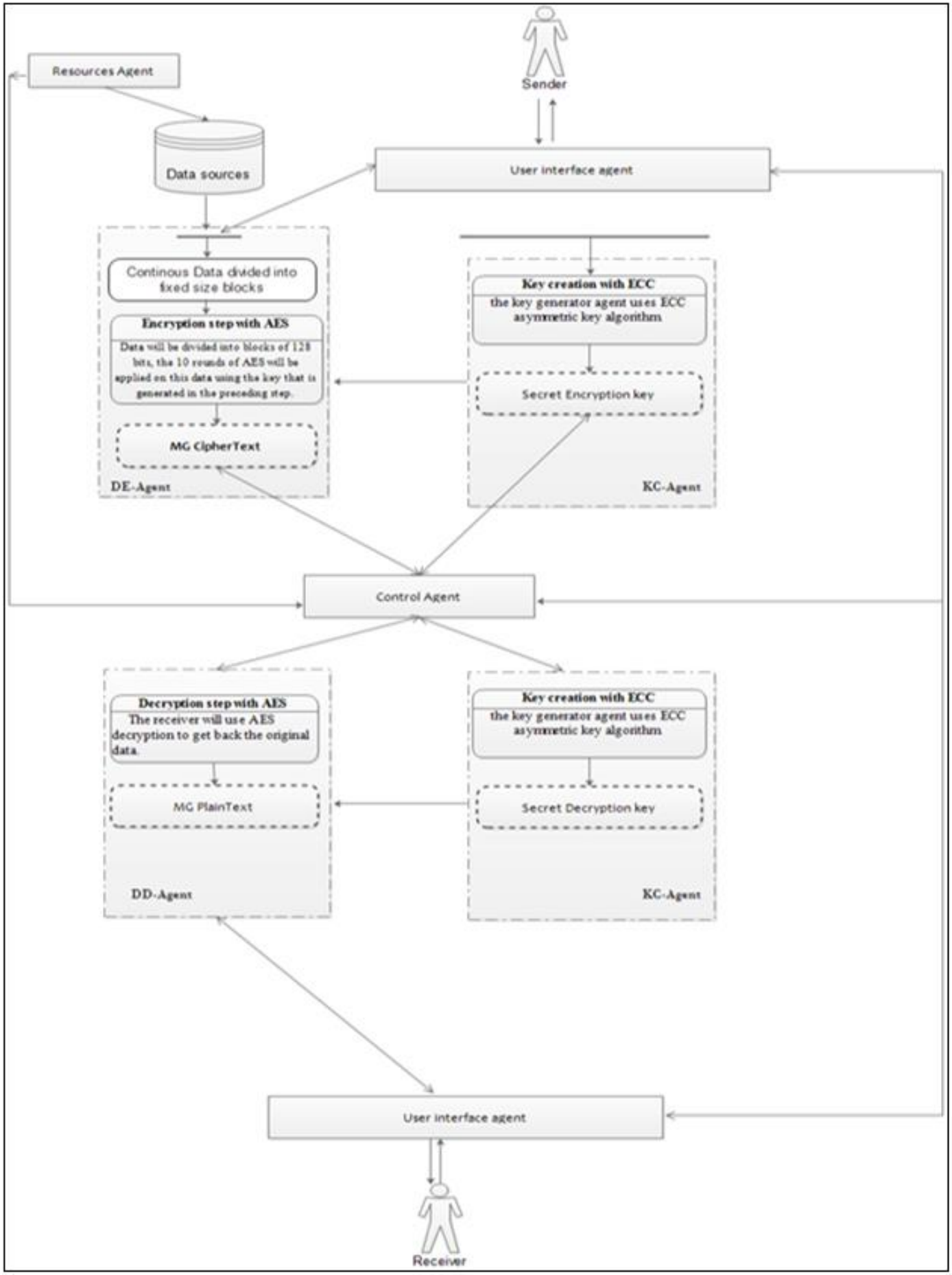

Fig 9 The proposed M-A-S architecture for MV-ECC-AES.

A negotiation is carried out between the control agent, the MR agents, and the user interface agents in order to secure the communication in the DC-SM. To accomplish the necessary objectives, each of these agents cooperates [20]. The main agent uses the information that the control agent gives to it to carry out the various security measures for the S-MG. The group of these agents must regularly communicate in order to exchange knowledge and carry out the following duties in order to increase the security of DC-SM's.

Resources-Agent: This agent is the first to respond when nodes are established but before any data is sent.

User-Interface-Agent: This component interacts with users to gather data about the processed dataset, including the number of characteristics, the algorithms employed, and other details. This agent is also in charge of gathering all environmental requirements and sending them to the control agent for usage by other agent.

- *User-Interface-Agent:*

This component interacts with users to gather data about the processed dataset, including the number of characteristics, the algorithms employed, and other details. This agent is also in charge of gathering all environmental requirements and sending them to the control agent for usage by other agents.

- *Key-Creation-Agent:*

For efficient key sharing, this agent relies on MV-ECC.

- *Data-Encryption-Agent*:

This agent is in charge of assuring 128-AES based data encryption.

- *Data-Decryption-Agent:*

The recipient will utilize MV-ECC and 128-AES decryption to recover the original data.

VIII. CONCLUSION AND FUTURE WORK

In this research, a hybrid method for DC-SM architecture that supports the microgrid communication environment without interfering with its operation is developed. It is less computationally costly. To profit from the advantages of symmetric and asymmetric algorithms, the work that follows is based on the combination of two algorithms, 128-AES and ECC. Additionally, the M-A-S was utilized to manage the complexity of the suggested strategy and represent various processes.

Additionally, because our MV-ECC-AES method encrypts data quickly and securely, it enhances the performance of encryption techniques. The suggested technique requires less time and resources than ECC and is significantly more secure than 128-AES for DC-MG. In the future, DC-MG will be used in a new technique that combines this strategy with other technologies, such blockchain.

REFERENCES

[1]. Ma, S., Zhang, H., & Xing, X. (2018). Scalability for smart infrastructure system in smart grid: a survey. Wireless Personal Communications, 99, 161-184.
[2]. R. Singh and K. Shenai, “Dc microgrids and the virtues of local electricity,”http://spectrum.ieee.org/green-tech/buildings/dc microgridsand-the-virtues-of-local-electricity.
[3]. C. K. Veitch, J. M. Henry, B. T. Richardson, and D. H. Hart, “Microgrid cyber security reference architecture.” Sandia National Laboratories (SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2013.
[4]. ALRASHED, Saleh. Key performance indicators for Smart Campus and Microgrid. Sustainable cities and society, 2020, vol. 60, p. 102264.
[5]. S. Goel, “Anonymity vs. security: The right balance for the smart grid,” Communications of the Association for Information Systems, vol. 36, no. 1, p. 2, 2015.
[6]. Mouachi, R., Ait-Mlouk, A., Gharnati, F., & Raoufi, M. (2017). A Choice of Symmetric Cryptographic Algorithms based on Multi-Criteria Analysis Approach for Securing Smart Grid. Indian Journal of Science and Technology, 10, 39.