♦ Recepción/ 27 junio 2019
♦ Aceptación/ 25 agosto 2019

Secure Data Storage in The Cloud With Enhanced Symmetric Block Cipher Design

Almacenamiento Seguro De Datos En La Nube Con Diseño Mejorado De La Cifra De Bloques Simétricos

Waleed Kareem Awad [a, *],
Omar A. Dawood [a, b],
Mohamed Khalaf [b],
Hussein K. Almulla[c]

[a]College of Computer and Information Technology University of Anbar, Anbar - Iraq,
waleed.kareem@uoanbar.edu.iq,
waleed.yahsat@gmail.com
[b]College of Computer and Information Technology University of Anbar, Anbar - Iraq, the_lionofclub@yahoo.com,
Omar-Abdulrahman@uoanbar.edu.iq

ABSTRACT/ Cloud storage become most widely contemporary storage that used by the big companies through applying their services and their commercial activities. The security threats increased dramatically with the accelerating of increasing the volume of data on remote servers. The encryption-based methods are used to trust the data on remote servers securely with encrypted form. In this paper developed a new modern symmetric cipher under Substitution Permutation Network (SPN) structure with three strong variable ciphering keys of 128,192 and 256 bit of changeable rounds. The proposed algorithm involves a new algebraic theories and concrete mathematical principles that completely depend on Galois Field GF(2^8). The present cipher works to trust the cloud storage through encrypting the data to ensure the confidentiality. The proposed cipher enhanced the security metric and solve numerous type of internet-based storage problems for cloud services.

Keywords: Block Cipher, Cloud Storage, Galois Field (28), Substitution and Permutation Network (SPN), Advance Encryption Standard (AES), Feistel Structure (FS).

RESUMEN / **El almacenamiento en la nube se convierte en el almacenamiento más ampliamente contemporáneo que utilizan las grandes empresas mediante la aplicación de sus servicios y sus actividades comerciales. Las amenazas de seguridad aumentaron dramáticamente con la aceleración de aumentar el volumen de datos en servidores remotos. Los métodos basados en cifrado se utilizan para confiar en los datos en servidores remotos de forma segura con forma cifrada. En este artículo, se desarrolló un nuevo cifrado simétrico moderno bajo la estructura de la Red de Permutación de Sustitución (SPN) con tres claves de cifrado variables fuertes de 128,192 y 256 bits de rondas cambiables. El algoritmo propuesto involucra nuevas teorías algebraicas y principios matemáticos concretos que dependen completamente de Galois Field GF (28). El presente cifrado funciona para confiar en el almacenamiento en la nube mediante el cifrado de los datos para garantizar la confidencialidad. El cifrado propuesto mejoró la métrica de seguridad y resolvió numerosos tipos de problemas de almacenamiento basados en Internet para servicios en la nube.** **Palabras clave: cifrado de bloque, almacenamiento en la nube, campo de Galois (28), red de sustitución y permutación (SPN), estándar de cifrado avanzado (AES), estructura Feistel (FS).**

I. Introduction

Cloud Computing (CC) is the on-demand delivery of compute power, data storage, applications, and other IT resources with little cost and with little configuration effort over the internet with pay-as-you-go model. CC term is usually used to specify data centers available to many customers and to the owners of organizations over the Internet. It is probable that data owner will charge applications, software, and others as a services. Many data owners will not need to store and operate large amounts of data, where using cloud computing they can store and operate data in the cloud. Cloud service providers can provide unlimited storage and parallel computing resources [1].

Cloud computing has developed from several technologies (such as grid computing autonomic computing, virtualization,) and the convergence of various technologies has emerged to be called cloud computing. By comparing Cloud Computing with traditional models, cloud computing migrates application software and databases to the big data centers, where the data and services will not be fully dependable. therefore, secure storage is very important for it due to it provides virtualized resources on Internet [2]. The data owner wants to share some of his documents that kept in the cloud with other legal users, so he must encode his sensitive data and documents locally before uploading it in the cloud storage to avoid illegal access to his data. Then, the secret key for each document must be sent to all authorized users. A main challenge to creating such encryption systems lies in the effective management and distributing of encryption keys. Distribution of secret keys has been problematic until recently, because it involved face-to-face meeting, use of a trusted courier, or sending the key through an existing encryption channel. [3]. The rapid spread of new technologies on the Internet has made it necessary to find and build modern ways to increase network security, so cloud computing is a modern model that uses the Internet and its main function is to reduce the effort on users and reduce costs and storage management and other sources.

Most data owner consider that the biggest problems in cloud infrastructure are confidentiality, integrity and authentication. We can define a security mechanism as a procedure used to discover, block, or recover from a security attack. so, to achieve security objectives and security mechanisms we can used encryption. While to prevent unauthorized users access to data and software at the network level we can use the network security [4].

Process of storing data online in the cloud called cloud storage. Cloud storage gets suitable storage of data, and in the other hand there is concern about security issues. Data storage security involves authorized access to data stored in the cloud. To achieve data confidentiality of access and sharing authentication data using encryption. The technique used to achieve authentication called digital signature, with a digital signature the origin as well as the integrity of the data can be ensured. The technique that is used to detect the unauthorized alteration on the data is called data integrity, the employment of cryptographic hash functions within the digital signature provides data integrity [5].

II. Literature Survey

While sharing the IT infrastructure in cloud computing is cost-efficient and provides more flexibility for the clients, it introduces security risks organizations have to deal with. This is necessary so that they can isolate their data from other cloud clients and to fulfill confidentiality and integrity demands. Moreover, since the IT infrastructure well be under control of the cloud provider, the customer has not only to trust the security mechanisms and configuration of the cloud provider but also the cloud provider itself. Therefore, in cloud model, data owner must encrypt data and then upload to cloud storage service, if he wants to share data with others users.

In [2] B. Shwetha et al. presented scheme focus on secure data storage in cloud; it is an essential part of quality of service. The authors proposed an efficient and flexible scheme with salient qualities. To guarantee the accuracy of users' data in the cloud. The presented scheme realizes the data storage accuracy, agree to the authenticated user to access the data and data error localization.

In November 2015, B. Kosal et al. proposed a schema for the interference of denial of service (DOS) attacks for clouds known as FAPA (Flooding Attack Interference Architecture). The authors were able to design a dynamic response model so they could stop the flow of attacks through their proposed model depending on the characteristics or features of this attacks [9].

In [10] N. Kaaniche1 et al. they suggested and executed the efficiency and scalability of CloudaSec framework for securely sharing outsourced data via the public cloud. CloudaSec guarantees the privacy of content in the public cloud infrastructures with the possibility of controlling the mechanism of entry of participants in addition to the mechanism of effective and flexible cancellation.

In [11], Sana Belguith,. She proposed new hybrid lightweight encryption technique which combining between asymmetric and symmetric cryptographic algorithm. Where the author used symmetric algorithm to encrypt data and asymmetric algorithm used to distribute keys between cloud provider and authorized, using various input files. Based on the output analysis.

In June 2017, K. M. Akhil et al. the authors focuses in the presented paper on secure data transfer. where, they suggested approach that provided security to transfer data using encrypted technique. the authors also take into consideration the topic worried with third party, where the proposed approach prevent third party from access and manipulation to user data [12].

III.Cloud Computing Architecture

The architecture of cloud computing can be divided into three significant classes as follows:

A. A Layered Model of Cloud Computing

The architecture of a cloud computing divided into 4 layers [6]: which involves:

- The Hardware Layer: the hardware layer implemented in data centers. This layer regroups and managing all the hardware components and the physical resources of the cloud including physical servers, routers and switches.
- The infrastructure layer: The infrastructure layer known as the virtualization layer. This layer allows creating the virtual resource that will be used by the upper layer.
- The platform layer: Platform layer built on top of the infrastructure layer. it is dedicated to the operating system and application frameworks.
- The application layer: This layer is the highest level of the hierarchy. the application layer consists of the actual cloud applications.

B. Cloud Computing Business Models

Hardware and platform-level resources are provided as services on an on-demand basis. Conceptually every layer of the architecture described in the previous section can be implemented as a service to the layer above. Conversely, every layer can be perceived as a customer of the layer below. However, in practice, clouds offer services that can be grouped into three categories: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). These will be described using the XaaS taxonomy, first used by Scott Maxwell in 2006, where "X" is Software, Platform, or Infrastructure, and the final "S" is for Service. It is important to note, as shown in Figure (1), that SaaS is built on PaaS, and the PaaS on IaaS. Each of these service models is described in a following subsection. [7].

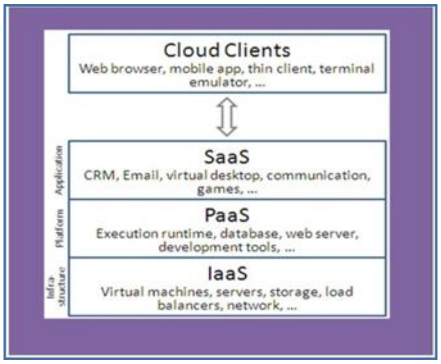

Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
SaaS
CRM, Email, virtual desktop, communication, games, ...
PaaS
Execution runtime, database, web server, development tools, ...
IaaS
Virtual machines, servers, storage, load balancers, network, ...
Application
Platform
Infra-structure

Fig. 1. Cloud Computing Business Models

- IaaS (Infrastructure as a Service): The ability provided directly the IT infrastructure to the customer of IaaS is storage space, computing, or network resources in terms of virtual machines with which the customer can run and execute operating system applications, or any software that they choose.
- PaaS (Platform as a service): Here a layer of software or development environment provided as service. in this layer, the cloud provider not only provides the hardware, but they also provide a toolkit and a number of supported programming languages such as (Java/ Python/ .Net. etc) to build higher level services.
- SaaS (Software as a Service): in this layer applications deliver as a service on demand with little cost and with little configuration effort over the internet with pay-as-you-go concept.

C. Deployment Model in Cloud Computing

There are three types of cloud computing deployment models namely public, private and hybrid cloud computing [8].

- Public Cloud Computing: similar to the internet. It offers a set of resources (h/w and s/w) as a service to general public . where the access is available to public domain. Public clouds are administrated by third parties or vendors over the Internet, and services are offered on pay-per-use basis
- Privet Cloud Computing: private cloud computing resides within the boundaries of an organization (one user) and is execute inside the organization. It is like to that of intranet where the user has more control in the system. This type of cloud computing has more benefits with increased security reliability, and corporate ownership of the cloud.

- Hybrid Cloud Computing: Hybrid cloud computing combines the features of both private and public cloud computing. It appropriates for the business to business environment.

IV. Data Storage in Cloud Computing

Cloud data storage gets suitable storage of data, but in the other hand there are many challenging design issues. Because of the lack of ability to control physical resources in the cloud, many threats and risks are associated with cloud data storage services. As these threats negatively affect the security and integrity of data as well as the performance of cloud systems.[22][23][24]

Cloud storage can be defining as a process for storing user data through cloud service provider (CSP) into set of cloud servers, where digital data is stored in logical groups. Cloud storage suppliers are responsible for maintaining, supporting and accessing available data and protecting and operating the physical environment, that is mean the cloud storage services offer transparency to the customers. Cloud storage services can be accessed through the cloud-based cloud service or applications using the API [3]. in the cloud storage application, the data owner can store and share their data with other users over the cloud with pay-as-you-go model [13].[25][26]

Cloud storage gets suitable storage of data, and in the other hand there is concern about security issues. Data storage security involves authorized access to data stored in the cloud. The ability to share encrypted data with different data owners over public cloud storage can meaningfully decrease security concerns about chance data drip in the cloud. but this way has many limitations due to the difficulty of key management and key distribution [14].

Although Cloud provides resources and applications as demand services at relatively low cost, there is a fundamental problem that the data owner needs to resolve, making the data access control policy flexible and scalable and accessible only to authorized users [15].

Data storage security involves authorized access to data stored in the cloud. Cloud storage has arisen as a hopeful solution to provide universal, convenient, and on-demand access to large volumes of shared data over the Internet. The data owner and commercial customers are involved by cloud storage as of its many benefits, containing low cost, little effort, high speed, and better resource utilization [5].

V. The Proposed Cryptographic Symmetric Cipher

The proposed algorithm designed with a novel symmetric structure that has been adopted a solid algebraic theories and hard mathematical notations over the GF (28). The present cipher represents a series of development steps for several developed algorithms over many years of research. Thus, It has inherited most of the good feature from previous published symmetric ciphers which open the door in front of its design likewise you can see [16], [17], [18]. The proposed structure built to accommodate the future need for the cloud storage requirements with high level of security and maximum performance[27]. It is an iterated block cipher algorithm that works with product structure as a set of layers. The round transformation and the main stages in the algorithm are quite similar to the Advance Encryption Standard (AES) design [19]. But, there are big differences in terms of internal mathematical base and the round transformation layers. The suggested cipher accepts input data of 128-bit that encrypted under 128-bit of secret key repeated up to 10-rounds. The main round operates on state array of 16, 20 and 24 bytes across four basic operations. The four essential operations in the main round transformation include Lookup-S-box Table of Substitution Layer,Pandiagonal-Permutation Layer, Involution Mixing Layer and the Bitwise addition for the cipher key layer which can be stated in Fig 2.

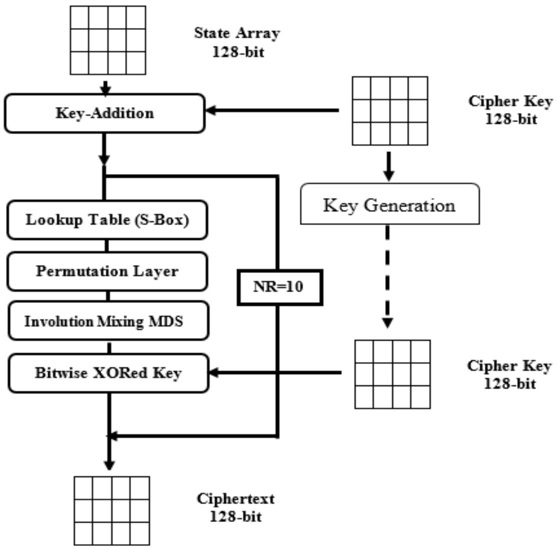


Fig. 2. The Structure of the Proposed Algorithm

A. Proposed Lookup-S-box Table of Substitution Layer

This is the critical part in the cipher which considers the only nonlinear layer that mapping the input vector to the output vector in a nonlinear form. The substitution layer is the main source for the confusion generation. The Look-up table of S-box is built by multiplying the input vector according to the irreducible polynomial of x8 + x5 + x4 + x3 + x2 + x + 1 of order eight. Thereafter, multiplying the resultant by 8*8 Boolean affine matrix as stated in Eq (2). The final step is XORed each vector with a constant hexa-vector of (2B).

$$Y=Ax^{-1}\oplus b \qquad (1)$$

$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 1&0&0&1&1&1&1&0 \\ 0&1&0&0&1&1&1&1 \\ 1&0&1&0&0&1&1&1 \\ 1&1&0&1&0&0&1&1 \\ 1&1&1&0&1&0&0&1 \\ 1&1&1&1&0&1&0&0 \\ 0&1&1&1&1&0&1&0 \\ 0&0&1&1&1&1&0&1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \qquad (2)$$

Table 1. Forward Look-up Table S-Box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	2B	16	3C	CE	29	86	D9	2E	2A	D7	74	55	DB	64	20	41
1	AB	0D	DC	06	84	F7	9D	E0	DA	60	8C	7F	27	FE	1E	90
2	6B	42	38	53	D0	1F	34	69	75	F1	45	ED	70	E9	47	8D
3	5A	E8	07	C7	F8	30	88	8F	2D	9C	48	58	B1	56	F6	6E
4	0B	E6	9F	AD	A2	23	17	FF	D6	7A	31	B9	A4	F4	0A	89
5	04	FC	CF	6A	95	81	C1	B7	0F	46	4A	3D	94	72	78	22
6	1A	D8	CA	0C	B4	03	D4	91	C2	EA	2F	08	73	EE	79	C9
7	A1	B6	F0	F2	13	A5	1B	9B	EF	F5	1C	93	C5	96	00	24
8	B2	D1	CD	57	71	1D	E1	BF	66	BD	A6	9E	BC	43	C8	F9
9	5C	80	83	AE	AF	92	62	67	EC	B5	C4	D2	32	63	F3	51
A	35	50	49	85	59	36	8B	10	FD	B3	7E	A8	5E	7B	65	CC
B	39	8A	14	E2	12	6D	A9	97	7D	87	0E	9A	82	3B	26	A3
C	3A	18	5B	61	52	A7	B8	68	E4	98	3F	09	5D	11	76	DD
D	DF	BB	CB	05	A0	4B	33	6F	8E	FB	40	15	02	54	D3	DE
E	E7	2C	E5	C3	4F	AA	4E	E3	37	3E	6C	01	BA	28	FA	25
F	C0	C6	44	99	B0	EB	77	19	D5	5F	7C	4C	BE	21	AC	4D

B. Proposed Inverse Lookup-S-box

The inverse subbyte process comprises the reverse steps for the mathematical operations of forward S-box multiplying by the inverse coefficients for the affine transform and the constant vector. The constant vector (F6) will increase the complexity for the decryption operation and make the mathematical intractable as stated in Eq (3). The Inverse Look-up S-box table can be shown in Table 2.

$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 0&0&1&1&0&1&0&0 \\ 0&0&0&1&1&0&1&0 \\ 0&0&0&0&1&1&0&1 \\ 1&0&0&0&0&1&1&0 \\ 0&1&0&0&0&0&1&1 \\ 1&0&1&0&0&0&0&1 \\ 1&1&0&1&0&0&0&0 \\ 0&1&1&0&1&0&0&0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \qquad (3)$$

Table 2. Backward Look-up Table S-Box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	7E	EB	DC	65	50	D3	13	32	6B	CB	4E	40	63	11	BA	58
1	A7	CD	B4	74	B2	DB	01	46	C1	F7	60	76	7A	85	1E	25
2	0E	FD	5F	45	7F	EF	BE	1C	ED	04	08	00	E1	38	07	6A
3	35	4A	9C	D6	26	A0	A5	E8	22	B0	BD	BD	02	5B	E9	CA
4	DA	0F	21	8D	F2	2A	59	2E	3A	A2	5A	D5	FB	FF	E6	E4
5	A1	9F	C4	23	DD	0B	3D	83	3B	A4	30	C2	90	CC	AC	F9
6	19	C3	96	9D	0D	AE	88	97	C7	27	53	20	EA	B5	3F	D7
7	2C	84	5D	6C	0A	28	CE	F6	5E	6E	49	AD	FA	B8	AA	1B
8	91	55	BC	92	14	A3	05	B9	36	4F	B1	A6	1A	2F	D8	37
9	1F	67	95	7B	5C	54	7D	B7	C9	F3	BB	77	39	16	8B	42
A	D4	70	44	BF	4C	75	8A	C5	AB	B6	E5	10	FE	43	93	94
B	F4	3C	80	A9	64	99	71	57	C6	4B	EC	D1	8C	89	FC	87
C	F0	56	68	E3	9A	7C	F1	33	8E	6F	62	D2	AF	82	03	52
D	24	81	9B	DE	66	F8	48	09	61	06	18	0C	12	CF	DF	D0
E	17	86	B3	E7	C8	E2	41	E0	31	2D	69	F5	98	2B	6D	78
F	72	29	73	9E	4D	79	3E	15	34	8F	EE	D9	51	A8	1D	47

C. Pandiagonal-Permutation Layer

This layer is basically responsible for generating a diffusion property where it distributes or rearranges the set of value's positions to another different positions. The arrangement process depends mainly on mathematical arrangement formula of perfect magic square. The perfect magic square is quite similar to the regular magic square configuration except the summation of pandiagonal parallel of any extended diagonals and corresponding back diagonals which will be equivalent to the magic constant [20] [21]. The permutation method is not restricted to constructed a perfect magic square mathematically. It just works to map the state array over 4*4 into a perfect magic square arrangement as stated in Fig 3. The perfect magic square gives an optimal diffusion for the round function with maximum immunity against the differential and linear attacks.

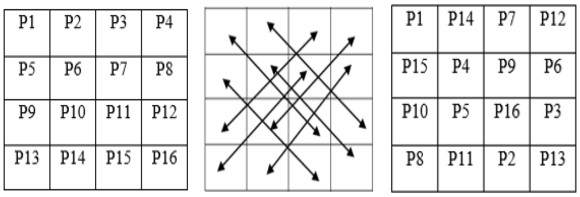


Fig. 3. Pandiagonal-Permutation Layer

D. Involution Mixing Layer

The Involution Mixing layer involve an invertible Maximum Distance Separable (MDS) matrix of a linear equation as stated in Eq(4) [22]. The input state array of 4*4 multiplied by MDS matrix module x4+1 given the mixed vector. This layer is responsible for the confusion and diffusion properties at the same time.

c(x) = 02x3 + 04x2 + 03x + 04   (4)

Thus, the proposed MDS is involuted matrix where the same matrix multiplied in forward and backward operations with self-inverse notation. The following mathematical formula clarifies the encryption plaintext and decryption of cipher text,

Where, C(x) = MDS(x) ⊗ a(x),   (5)

P(x) = MDS(x) ⊗ C(x),   (6)

$$\begin{bmatrix} S_{0c} \\ S_{1c} \\ S_{2c} \\ S_{3c} \end{bmatrix} \otimes \begin{bmatrix} 04 & 02 & 04 & 03 \\ 03 & 04 & 02 & 04 \\ 04 & 03 & 04 & 02 \\ 02 & 04 & 03 & 04 \end{bmatrix} = \begin{bmatrix} S_{0c} \\ S_{1c} \\ S_{2c} \\ S_{3c} \end{bmatrix} \otimes \begin{bmatrix} 04 & 02 & 04 & 03 \\ 03 & 04 & 02 & 04 \\ 04 & 03 & 04 & 02 \\ 02 & 04 & 03 & 04 \end{bmatrix} = \begin{bmatrix} S_{0c} \\ S_{1c} \\ S_{2c} \\ S_{3c} \end{bmatrix}$$

for 0 ≤ M < Nb   where Nb =4 no of bytes in the word

The mixing layer is a pure mathematical stages that deals with involuted of self-inverse linear equation. The main clue for the involuted MDS is to increase the implementation speed and to achieve balance in algebraic computation. This mean the proposed algorithm execute internal encryption and decryption over GF(2^8) equally. So, the multiplication of forward MDS by itself or backward equation give the identity matrix as stated below:

$$M(\,x\,) = n(\,x\,)\ \ mod\ (\ x^4 + 1\ )\ ...(4)$$

$$\begin{bmatrix} 04 & 02 & 04 & 03 \\ 03 & 04 & 02 & 04 \\ 04 & 03 & 04 & 02 \\ 02 & 04 & 03 & 04 \end{bmatrix} \times \begin{bmatrix} 04 & 02 & 04 & 03 \\ 03 & 04 & 02 & 04 \\ 04 & 03 & 04 & 02 \\ 02 & 04 & 03 & 04 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

E. Bitwise -XORed-Key Addition

The key addition process involves bitwise XORed between the ciphering sub-key and the state array of plaintext. It is self-inverse operation that has been adopted at the end of each round over GF(2).

F. Subkeys-Generation Algorithm

The key generation algorithm is a set of procedures that take the responsibility of generating ciphering sub-key for each round. The proposed algorithm takes the initial entry of secret key from the user and then make expansion with several sub-keys that numbered for each encryption round. The key expansion process acts the essence of the algorithm structure which gives the cryptographic strength for the cipher. The proposed generates the ciphering keys by two mathematical sophisticated functions (g & F). Where each generated function consists of three procedures, nonlinear subbyte operaton, complement process, and XORed constant word for (F) function. On other hand, the (F) function includes nonlinear subbyte, right rotate, and XORed with another distinct constant word as shown in Fig 4. The two complicated functions provide a confusion and diffusion property for the whole sub-keys

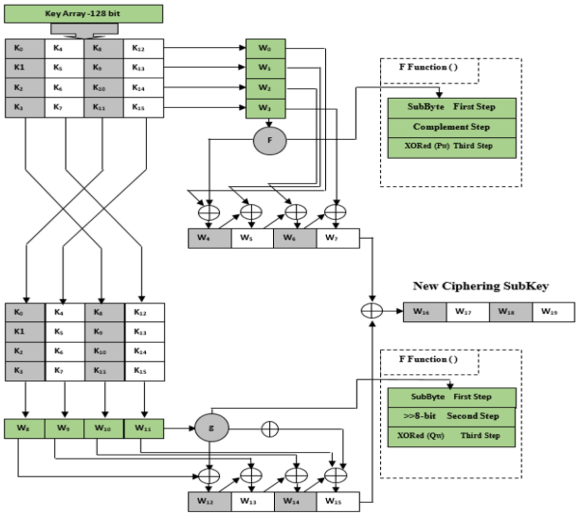
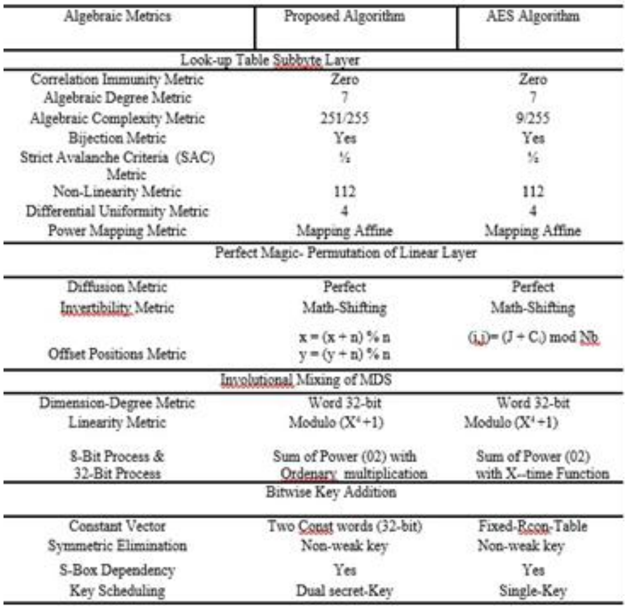


Fig. 4. The Proposed Key Scheduling Strategy

VI. Analysis and Security Evaluation

In this section a deep analysis and security evaluation metrics have been achieved. The design structure is implemented with SPN instead of Feistel structure because the Feistel structure has been criticized by many researchers. The main concerned weak point was the exchanging one part of the structure and keep fixed another part. The symmetry structure for the suggested cipher is developed with symmetric mathematical operations. This strategy has been adopted to face the structural attacks and provides a strength for the cipher parts. The subbyte layer designed to produce a high non-linearity and mathematical computational complexity. The prefect magic square permutation is a critical part that achieves an ideal diffusion for the round function has been adopted as a new optimization. The selected MDS with involution property gave balance structure of the proposed cipher. The main idea behind the involutional property is to reduce the design of integrated circuits on the electronic board as much as possible, Since the involutery feature gives the mathematical function F(x) the same implementation in encryption and decryption processes and to defeat power analysis attack. The last stage for the proposed cipher is the key generation algorithm which responsible for producing the secret ciphering sub-keys strongly. The proposed round-key is characterized by key agility and versatility that enable it to operates on different applications. The key expansion methodology based upon simple operations that include XOR, Rotate, Complement, and bitwise XORed with additional words. These simple operations make the generated key obtained an enormous power is almost to tend to be random as a one-time-pad key. Which when discovering one subkey there is no chance for the attacker to know the other sub-keys of next round. The complementary metric for the security is the efficiency which involves the sufficient amount of resources to implement the encryption and decryption processes efficiently and effectively. During design process the authors take in to account the security and efficiency factors to be compatible cipher for the recent cloud applications. The crucial analysis for the strengths design strategy were to defeats the practical attacks. The round key designed with key dependent S-box to increase the effect of Strict Avalanche Criteria (SAC) and the correlation immunity. The realistic challenge is how to design a robust cipher that should apply an accepted security level with an optimized performance. There is no doubt that all the countermeasures have been taken through designing steps to repel the linear and differential attacks. The designed cipher with multi-layers is to makes the ciphering key more resistant against the related attacks. Several evaluations and tests have been implemented likewise randomness tests, time implementation which produced reasonable results. The assessment with different metrics compared with AES cipher can be shown in Table 3. And the Excel chart clarifies the time implementation according to different length of text can be stated in Fig. 4. The strength of the proposed algorithm can be investigated and evaluated by the specialists and cryptographic designers and we shall be happy and thankful to accept any scientific criticisms may enhance our proposed cipher.

Table 4. Evaluation Comparison between the AES and the proposed Algorithm



Algebraic Metrics	Proposed Algorithm	AES Algorithm
Look-up Table Subbyte Layer		
Correlation Immunity Metric	Zero	Zero
Algebraic Degree Metric	7	7
Algebraic Complexity Metric	251/255	9/255
Bijection Metric	Yes	Yes
Strict Avalanche Criteria (SAC) Metric	½	½
Non-Linearity Metric	112	112
Differential Uniformity Metric	4	4
Power Mapping Metric	Mapping Affine	Mapping Affine
Perfect Magic- Permutation of Linear Layer		
Diffusion Metric	Perfect	Perfect
Invertibility Metric	Math-Shifting	Math-Shifting

Offset Positions Metric	x = (x + n) % n
	y = (y + n) % n
		$(i,j) = (J + C_i)$ mod Nb

Involutional Mixing of MDS		
Dimension-Degree Metric	Word 32-bit	Word 32-bit
Linearity Metric	Modulo (X^4+1)	Modulo (X^4+1)
8-Bit Process & 32-Bit Process	Sum of Power (02) with Ordenary multiplication	Sum of Power (02) with X--time Function
Bitwise Key Addition		
Constant Vector	Two Const words (32-bit)	Fixed-Rcon-Table
Symmetric Elimination	Non-weak key	Non-weak key
S-Box Dependency	Yes	Yes
Key Scheduling	Dual secret-Key	Single-Key

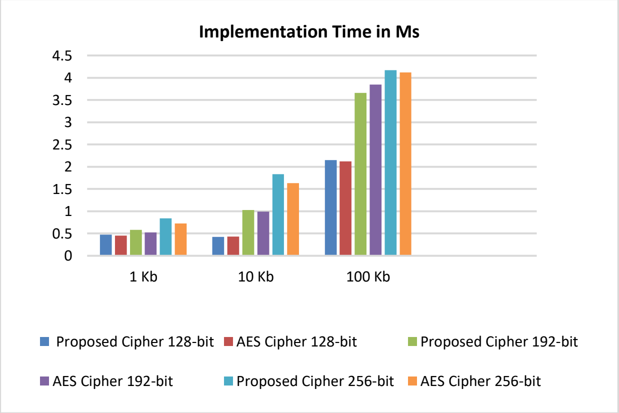


Fig. 5. Time Implementation Chart between the AES and the Proposed Algorithm

VII. Conclusions

The advance technology and information revolution of different trends with multidisciplinary sectors generates a huge amount of simultaneous data. These large volume of data are stored in remote servers on the internet. The stored data need to be encrypted in order to be trusted against the attackers and cryptanalytic attacks. In this paper proposed a new secure symmetric cipher of 128-bit with SPN structure of high level of security margin. The proposed algorithm is dedicated to encrypt the data on cloud storage that stored based on internet. The designed cipher gives an accepted result from several metrics of security, efficiency and the implementation time.

References

[1] Rao, S.,Rao, N. and Kumari, K. (2009).: Cloud computing: An overview". Journal of Theoretical and Applied Information Technology, 9(1): 71-76.

[2] B. Shwetha Bindu1., and B. Yadaiah (2011).: Secure Data Storage In Cloud Computing. International Journal of Research in Computer Science ISSN 2249-8257 Volume 1 Issue 1, pp. 63-73.

[3] Sameeh A. Jassim, Waleed Kareem Awad (2018). SEARCHING OVER ENCRYPTED SHARED DATA VIA CLOUD DATA STORAGE. Journal of Theoretical and Applied Information Technology, 30th June.

[4] Zuriati A., and Roszelinda K. (2014). Quantum Key Distribution Approach for Cloud Authentication: Enhance Tight Finite Key. International conference on Computer Science and Information Systems (ICSIS'2014) Oct 17-18.

[5] Zhangjie Fu et al. (2014). Secure Storage of Data in Cloud Computing, International Conference on Intelligent Information Hiding and Multimedia Signal Processing.

[6] Zhang, Q., Cheng, L., and Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges".Journal of Internet Services and Applications,1: 7–18, The Brazilian Computer Society.

[7] Yang, J. & Chen, Z. (2010). Cloud computing research and security issues. International Conference on Computational Intelligence and Software Engineering (CiSE), Wuhan, China, 1-3.

[8] Taha Chaabouni and Maher Khemakhem. (2012). CLOUD COMPUTING: A NEW VISION OF THE DISTRIBUTED SYSTEM, ICAITA, SAI, SEAS, CDKP, CMCA, CS & IT 08, pp. 245–252, 2012. CS & IT-CSCP.

[9] B.Kosal Kumar and G.Sumalatha (2015). A Model to Prevent Flooding Attacks in Clouds. International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056, Volume: 02 Issue: 08 |Nov-2015.

[10] Nesrine Kaaniche et al. (2014). CloudaSec: A Novel Public-key based Framework to handle Data Sharing Security in Clouds. International Conference on Security and Cryptography.

[11] Sana Belguith. (2015). Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm. Conference: ICAS, The Eleventh International Conference on Autonomic and Autonomous Systems.

[12] K. M. Akhil et al. (2017). Enhanced cloud data security using AES algorithm, International Conference on Intelligent Computing and Control (I2C2). 23-24 June-2017

[13] Cheng-Chi Lee et al. (2013). A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments, International Journal of Network Security, Vol.15, No.4, PP.231-240, July-2013.

[14] Baojiang Cui at le. (2016). Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage, IEEE Transactions on Computers (Volume: 65 , Issue: 8 , Aug. 1-2016)

[15] Nate Lord (2018). Cryptography in the Cloud: Securing Cloud Data with Encryption". Article published in https://digitalguardian.com, on Tuesday September 11, 2018.

[16] O. A. Dawood, A. M. S. Rahma, and A. M. J. Abdul Hossen (2015). The New Block Cipher Design (Tigris Cipher), Int. J. Comput. Netw. Inf. Secur., vol. 7, no. 12, pp. 10–18-2015.

[17] O. A. Dawood, A. M. S. Rahma, and A. M. J. Abdul Hossen. (2017). New Symmetric Cipher Fast Algorithm of Revertible Operations' Queen (FAROQ) Cipher, Int. J. Comput. Netw. Inf. Secur., vol. 9, no. 4, pp. 29–36, Apr-2017.

[18] O. A. Dawood, A. M. S. Rahma, A. Mohssen, and J. A. Hossen. (2015). The Euphrates Cipher," IJCSI Int. J. Comput. Sci. Issues, vol. 12, no. 2, pp. 154–160.

[19] Daemen J, Rijmen V. (2013). The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media; Mar 9-2013.

[20] O. A. Dawood, A. M. S. Rahma, A. Mohssen, and J. A. Hossen. (2016). Generalized Method for Constructing Magic Cube by Folded Magic Squares: International Journal of Intelligent Systems and Applications(IJISA), Vol. 8, No. 1, pp.1-8, Jan. DOI: 10.5815/ijisa.

[21] O. A. Dawood, O. I. Hammadi, and T. K. Asman. (2018). Developing a New

Secret Symmetric Algorithm for Securing Wireless Applications, in 1st Annual International Conference on Information and Sciences (AiCIS), pp. 152–158,

[22] Osamah Ibrahim Khalaf, Ghaida Muttashar Abdulsahib and Muayed Sadik, 2018. A Modified Algorithm for Improving Lifetime WSN. Journal of Engineering and Applied Sciences, 13: 9277-9282

[23] Osamah Ibrahim Khalaf, Bayan Mahdi Sabbar''An overview on wireless sensor networks and finding optimal location of node'',Periodicals of Engineering and Natural Sciences, Vol 7, No 3 (2019)

[24] Ayman Dawood Salman1, Osamah Ibrahim Khalaf and Ghaida Muttashar Abdulsahib, 2019. An adaptive intelligent alarm system for wireless sensor network. Indonesian Journal of Electrical Engineering and Computer Science, Vol. 15, No. 1, July 2019, pp. 142~147

[25] Ogudo, K.A.; Muwawa Jean Nestor, D.; Ibrahim Khalaf, O.; Daei Kasmaei, H. A Device Performance and Data Analytics Concept for Smartphones' IoT Services and Machine-Type Communication in Cellular Networks. *Symmetry* **2019**, *11*, 593.

[26]GHAIDA MUTTASHAR ABDULSAHIB and OSAMAH IBRAHIM KHALAF, 2018. AN IMPROVED ALGORITHM TO FIRE DETECTION IN FOREST BY USING WIRELESS SENSOR NETWORKS.International Journal of Civil Engineering & Technology (IJCIET) - Scopus Indexed. Volume:9, Issue:11, Pages:369-377.

[27]Osamah Ibrahem Khalaf, Ghaidaa Muttasher et al., "Improving video Transmission Over Heterogeneous Network by Using ARQ and FEC Error Correction Algorithm‟, vol. 30, no.8, pp.24-27, Nov 2015