Proposed Architecture Diagrams for developing an electronic system based on block chain technology to secure confidential data in university

Samia Ahmed Elsayed abou Elwafa[1], Elsaeed Elsaeed Mohamed Abd El-razk[1], Samir Aboul Fotouh Saleh[2], Safaa M. Elatawy[1]

[1]Faculty of Specific Education, Damietta University, Egypt

[2] Professor of Accounting and Information Systems, Mansoura University College of Business

Emails: samiaahmed1123456@gmail.com; Dr_elsaeed2004@hotmail.com; Prof_samir@hotmail.com; zizoabdo1210@gmail.com

Abstract

The current system inside Egyptian universities s relies on the minimum and traditional methods of securing data that do not keep pace with the current digital development. Therefore, the education sector needs to take advantage of the advantages of block chain technology in securing and encrypting data from the risks of hacking and leakage of records. Through the above, an electronic system for generating a data encryption key based on block chain technology and the AES algorithm has been proposed.

Keywords: Blockchain technology; Encryption Algorithm; (AES) algorithm

1. Introduction

Databases are of great importance to the advancement of any society that plans to build its future on sound scientific and technical frameworks, especially as we live in an era in which many variables are controlled and based on important data, whether economic, social or other.

Speaking of digital systems that universities rely on, they are still relying on traditional methods since the emergence of the computer (the name of the user - the password). The current insurance does not keep pace with the BIG DATA technology and does not keep pace with the large capabilities of some users because they have a high ability to penetrate the security mechanism for this data.

Hence, educational institutions lack a security system based on reliable electronic applications to suit users' needs in securing and encrypting their information in a safe way to face any attempts to penetrate it.[1]

DOI: https://doi.org/10.54216/IJAIET.010103
Received: February 20, 2022 Accepted: May 20, 2022

Therefore, attention began to shift towards block chain technology as it is an emerging event in the databases in which the strength of the reliable system is concentrated in the degree of encryption and not centralized, as well as it is characterized by transparency and stability and is characterized by independence and safety due to the impossibility of penetrating its records as it abolishes the role of mediator between the student and the service and the digital system .to support the system The current AES algorithm was used to create a key for securing and encrypting confidential university data such as graduation certificates and electronic exams .

Education sector is starting to implement this technology in different possible areas. The strengths of the different applications of block chain in education will mainly provide greater transparency and also enhances the security. Moreover, it improves traceability, increased efficiency, reduced costs and improves processing speed Characteristics of block chain. Block chain has the following key characteristics. [2]

1- Decentralization. It can be classified into three forms architectural, political and logical decentralization.

2-Persistency. All records in the whole network cannot be tampered and any falsification can be detected easily.

3-Anonymity. A user could generate many addresses to avoid identity exposure. It preserves the privacy on the transactions.

4-Auditability. It improves the traceability and the transparency of the data stored in the block chain.

The block chain technology help students and universities by providing a more focused and specific understanding of how students are interacting with the university. [3]

In this paper, Key Block Chaining (KBC) has been proposed to generate multiple keys; it is inspired by CBC and acts as a KDF. The generated key(s), the generated keys are derived in the form of blocks of fixed-size. The concepts of Advanced Encryption Standard (AES) [4] have also been included to provide randomness in the keys to be generated; AES is a symmetric block cipher algorithm and has been accepted worldwide with its design criteria specifications, making it adaptable for numerous applications [5,6]In order to frustrate an attacker, on the condition that the initial (seed) key is unknown, an attacker cannot extract information about the past keys as well as the future keys from the knowledge of an intermediate key. Hence, our approach can be applied for satisfying backward as well as forward unpredictability properties based on the generated keys, provided an assumption that AES pseudorandom .

2. Related Work

According to Chen, L., Le et al**.. Block chain based searchable encryption for electronic health record sharing**. In this paper, a block chain based searchable encryption scheme for EHRs is proposed. The index for EHRs is constructed through complex logic expressions and stored in the block chain, so that a data user can utilize the expressions to search the index. As only the index is migrated to the block chain to facilitate. [7]

A study by Li, H., Tian, H., Zhang, F et al. **Block chain-based searchable symmetric encryption scheme.**

The mechanism for traditional searchable symmetric encryption (SSE) is pay-then-use. so we combined block chain with SSE, and proposed a fair SSE scheme based on block chain. Our scheme can guarantee fairness for both parties. That is, if the user is not honest, he cannot get right results from the server, and at the same time the server cannot get any information related to the plaintexts during this search process .[8]

A study by Khan, P. W et al. **A Block chain-Based Secure Image Encryption Scheme for the Industrial Internet of Things.** , In this paper, we propose a permissioned private block chain-based solution to secure the image while encrypting it. In this scheme, the cryptographic pixel values of an image are stored on the block chain, ensuring the privacy and security of the image data. Based on the number of pixels change rate (NPCR),

DOI: https://doi.org/10.54216/IJAIET.010103

Received: February 20, 2022 Accepted: May 20, 2022

the unified averaged changed intensity (UACI), and information entropy analysis, we evaluate the strength of proposed image encryption algorithm ciphers with respect to differential attacks. We obtained entropy values near to an ideal value of 8, which is considered to be safe from brute force attack. Encrypted results show that the proposed scheme is highly effective for data leakage prevention and security [9]

2. Blockchain

2.1 Definition

A block chain is a digital record of transactions. The name comes from its structure, in which individual records, called blocks, are linked together in single list, called a chain. Block chains are used for recording transactions made with cryptocurrencies, such as Bitcoin, and have many other applications .[10]

A block chain is, in the simplest of terms, a time-stamped series of immutable records of data that is managed by a cluster of computers not owned by any single entity. Each of these blocks of data (i.e. block) is secured and bound to each other using cryptographic principles (i.e. chain) [11]

Block chain is not just the kind of internet support based on distributed statements, except with a different supply from the equipment connection system. Generally, block chain is a dispersed system of machines (blocks) managed to keep the origin of knowledge distribution. Every block keeps some safety and precision from the data by containing a full collection of records of earlier activities. While a new node is acting as designed through a worker that is the primary unit proving every activity in the node plus completing a numerical query and producing a digital stamp for the nodes, which join a pre-defined operation that applies the hash function. The newly generated block directions are transmitted over all of the block chain channels, enabling each block to similarly control the full record [12].

2.2 The basic elements of the block chain systems' business architecture

Block chain technology enables a different way of creating and storing data that differs from the traditional database (Figure1) as it is done in a decentralized manner and distributed to all the devices connected in the network (Nodes), which all verify the Data validity and consistency (Validation) based on defined collective consensus rules (Consensus), and data is saved in A unified transaction log as mirrored copies on all devices and not as a single copy in a specific central device, and it includes the record A continuous list of parameters called blocks that are linked based on a Hash-value and encoded Cryptography (to protect confidentiality and ensure the correctness of its data by using algorithms, including rules of collective concord) Such as (Proof of Work), (Proof of Stake), (Proof of Concept), (Proof of Ownership), Digital Signature, Public / Private Key Infrastructure encryption and other types[13]

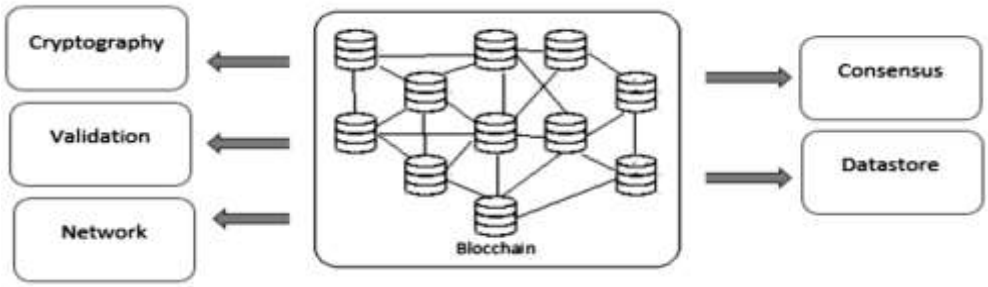


Figure1: the basic elements of a block chain architecture

The decentralization feature of block chain technology allows any type of value to be exchanged between any two parties without the need for a central entity to take over.

DOI: https://doi.org/10.54216/IJAIET.010103
Received: February 20, 2022 Accepted: May 20, 2022

Specific to manage the transactional system as a financial institution (bank, financial company, or other), as its work is based on a "peer-to-peer network". To - peer (peer-to-peer network), which allows all parties and related parties to access the system at any time and document The origin and origin of each transaction, its data recorded and connected to a state of collective consensus, and the confirmation of all parties on it and documented a process It is called (Mining), and as soon as all parties agree on the transaction, a block consisting of Header and Body is created.(Figure 2) and then appending it to the rest of the blocks in the network [14]

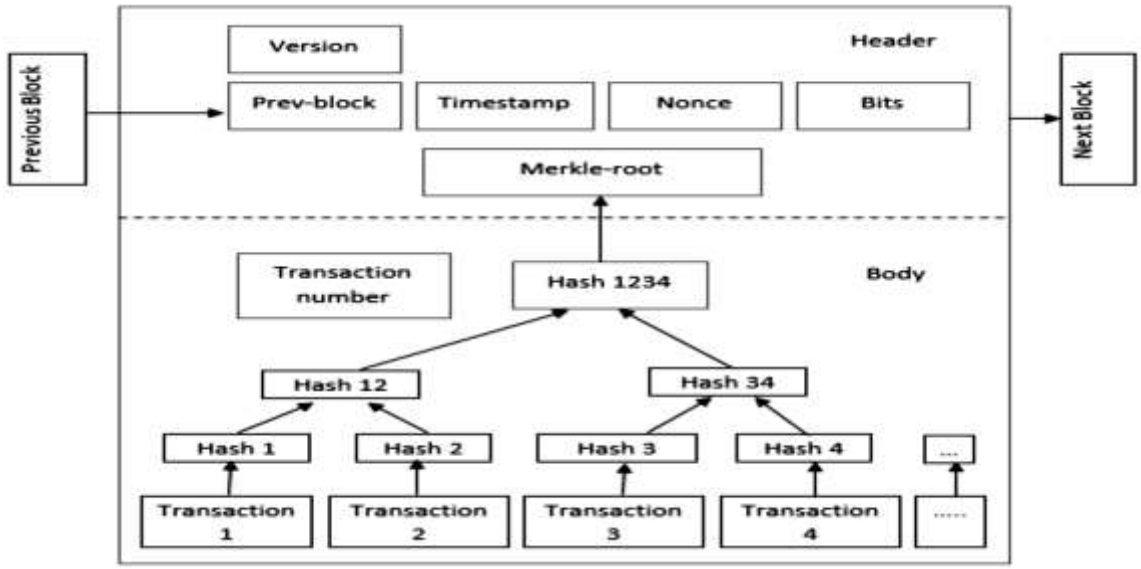


Figure 2: Auxiliary block components of the block chain

2.2.1 Encryption Algorithm

Encryption is one of the advantages of block chain, so we find that there are two types of encryption:

Hash:

The hash function encodes inputs of different length and converts them into outputs of fixed length, expressed in symbols Unique and fixed length As in Figure (3), not all data in a block is displayed, but the block is encrypted And issuing a unique token for each block, this block code and each block is created a cipher token based on a token [15]

With the exception of the first block, it differs from the rest of the blocks, as it is not coded in the previous block (Wang et al., 2019) SHA- As in Figure (4), there are multiple types of the hash function, 256 of which are Bruyn (Bruyn, there is a previous encoding code) (2017). That was used in Bitcoin, and if someone wanted to change the data in a block, then all the cryptographic symbols for the blocks And when the encoding code is generated for the block, a timestamp will be added to it and set a time (Kalis, 2018) And the time of its creation.

DOI: https://doi.org/10.54216/IJAIET.010103
Received: February 20, 2022 Accepted: May 20, 2022

Encryption codes Transaction
data

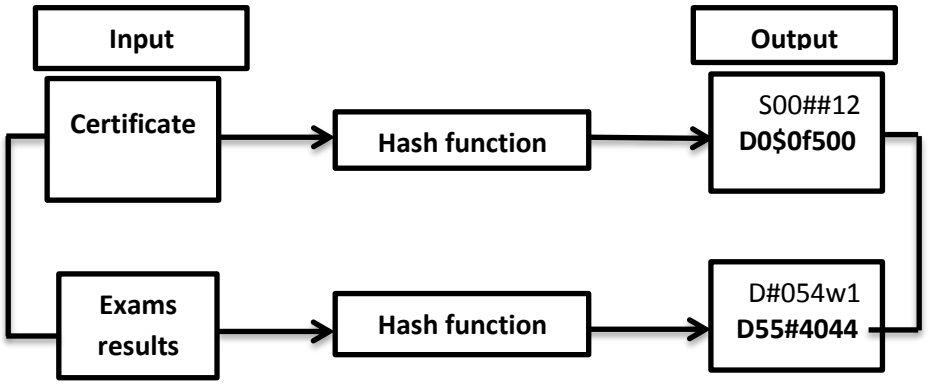


Figure 3: How the hash function works

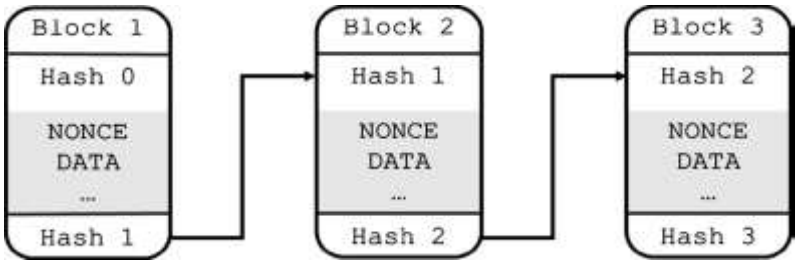


Figure 4: The block is encrypted in the block chain using the hash function

Key encryption:
Key cipher is known as symmetric, analog, or analog encryption, and it has many forms Files using keys and the idea of this encryption can be illustrated in general in Figure (5)

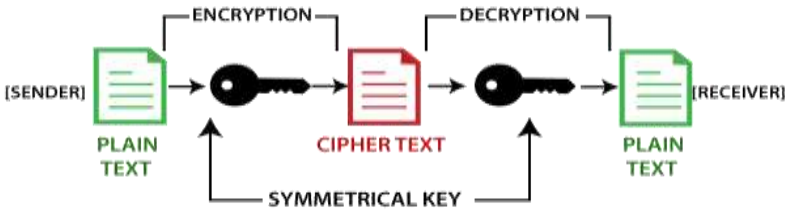


Figure 5: Common key encryption

DOI: https://doi.org/10.54216/IJAIET.010103
Received: February 20, 2022 Accepted: May 20, 2022

Public key: A key consisting numbers and letters, and is used to identify the user's identity in an operation

Transmission and reception, which is visible to everyone
The private key: It is a type of password that is considered personal and confidential. It also consists of numbers and letters which is longer than the public key, and this is one of the differences between them and is used for digital signature (Huhmo , 2018) [16]

3- Advanced Encryption Standard (AES)

AES [4] is a symmetric block encryption standard with 128-bit plaintext blocks and, commonly implemented, 128-bit key, however, 192 or 256 bits key can also be used. It was designed to provide resistance against all known attacks, speed and code compactness on a wide range of platforms, and design simplicity. In AES, a 128-bit block is depicted as a square matrix of bytes by FIPS PUB 197, i.e., a [23], which is then copied into a single, commonly 128-bit block, i.e., the State array which would be modified at each stage of encryption or decryption. Four different stages, one for permutation and three for substitution are used in AES: Substitute Bytes (Sub Bytes), Shift Rows, Mix Columns, Add Round Key. Here, the ordering of input bytes within a matrix is by column, i.e., the first four bytes of input occupy the first column, second four bytes occupy the second column and so on for the given input[17]

3.1. Shift Rows
The first line of the status remains unchanged. The second line turns left with one byte, the third line turns left with two bytes, and the fourth line turns left with three bytes. Receives the transfer state in the state it hosts. For example, the second row rotates one to the right, and the other rows are the same
can be seen in Figure (6).

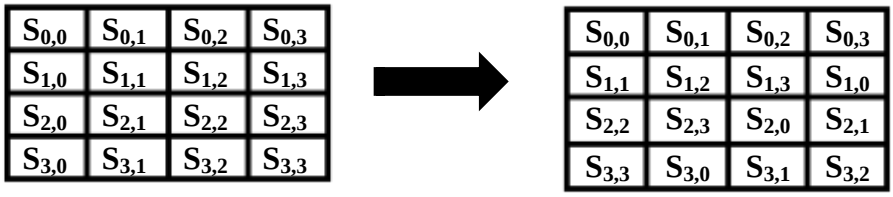


Figure 6: Shift Rows

3. 2. Substitute Bytes

In a sub-step, every byte in the array is transformed through an 8-bit S-box. This provides linear transformation and encryption method. (2 ^ 8) and reverse, and vice versa, and vice versa, and vice versa. Preventing algebraic creation, the S-box suite is used in combining inverse multiplication elements and an invertible quadrant transformation matrix. In addition, when constructing an S square, avoid the growth site, fixed point and anti-stationary point

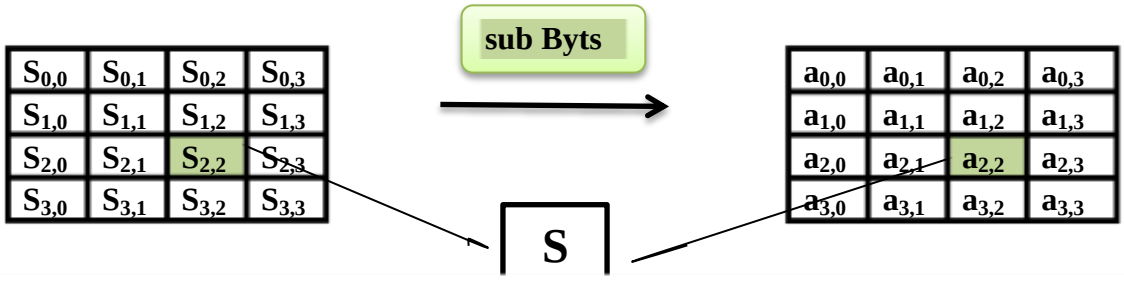


Figure 7: Substitute Bytes

DOI: https://doi.org/10.54216/IJAIET.010103
Received: February 20, 2022 Accepted: May 20, 2022

3.3. Shift Columns

This forward transformation, Shift Columns, is similar to that of the Shift Rows of AES. Here, the first column of the State is not altered. For the second column, a 1-byte circular bottom shift is performed. For the third column, a 2-byte circular bottom shift is performed. For the fourth column, a 3-byte circular bottom shift is performed. This transformation ensures that the four bytes of one row are spread out to four different rows. An inverse transformation of this operation can be performed similarly, if required[18]

4. Architecture

The current system is based on securing and encrypting confidential data within the university through block chain technology, with the ability to generate a key through the algorithm (AES), which is a safe method of encryption due to the length of the encryption key. One of the most important data that must be encrypted is the issuance of
Certificates and their validation.

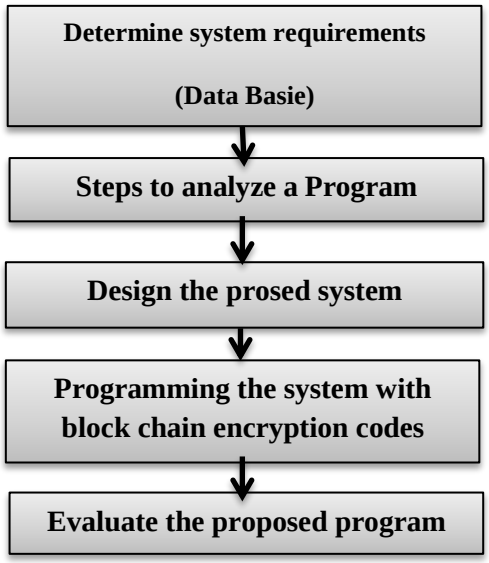


Figure 8: Steps for program design

4.1.proposed architecture Diagrams

DOI: https://doi.org/10.54216/IJAIET.010103
Received: February 20, 2022 Accepted: May 20, 2022

4.1.1The database that relies on Normal methods of insurance : the analysis stage

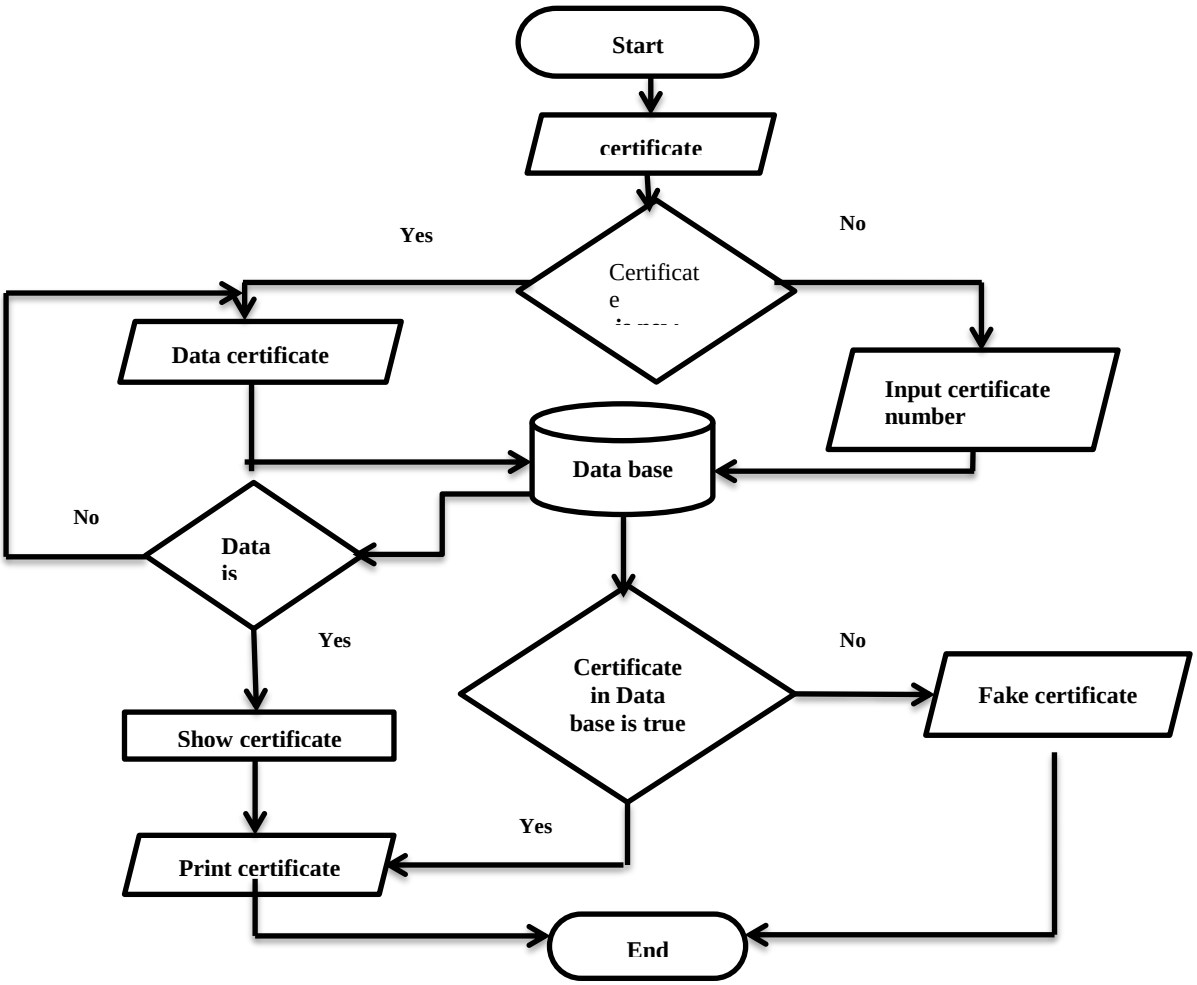


Figure 9: Normal certificate system

4.1.1.1 Algorithm

Input ID certificate
Process check ID certificate in Data base
Output fake certificate
Or print certificate

DOI: https://doi.org/10.54216/IJAIET.010103
Received: February 20, 2022 Accepted: May 20, 2022

4.1.2 Data encryption using block chain Technology : the design stage

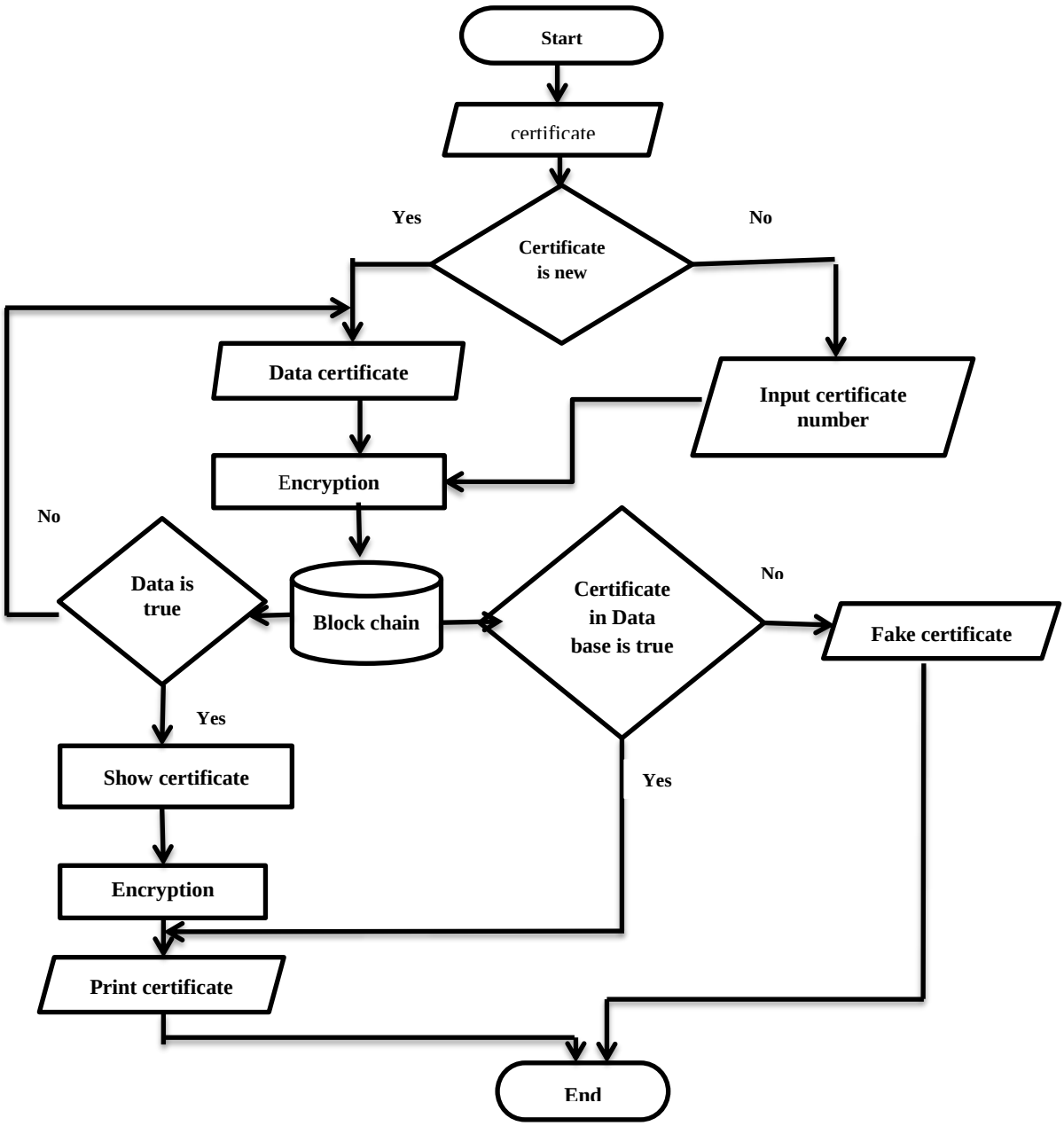


Figure 10: Block chain certificate system

4.1.2.1Algorithm

Input ID certificate
Process check ID certificate in Block chain with encryption hash
Convert to ASE encryption (Raise the degree of safety)
Output fake certificate
Or print certificate

DOI: https://doi.org/10.54216/IJAIET.010103
Received: February 20, 2022 Accepted: May 20, 2022

4.1.3

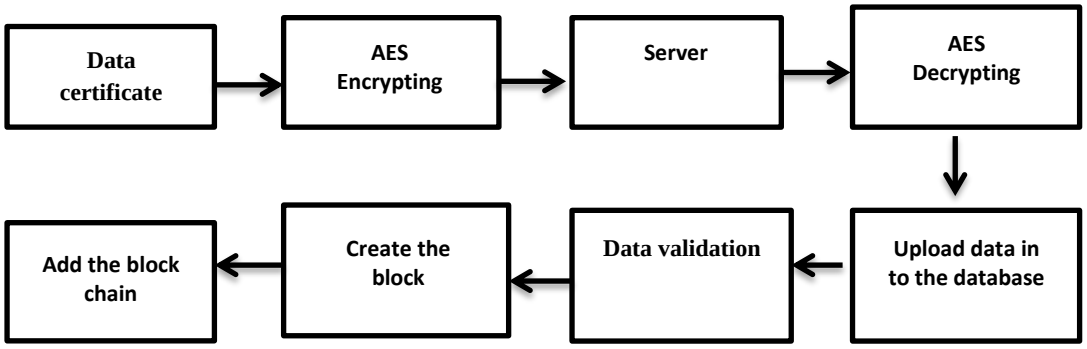


Figure 11: Encryption (AES) algorithm

4.1.4

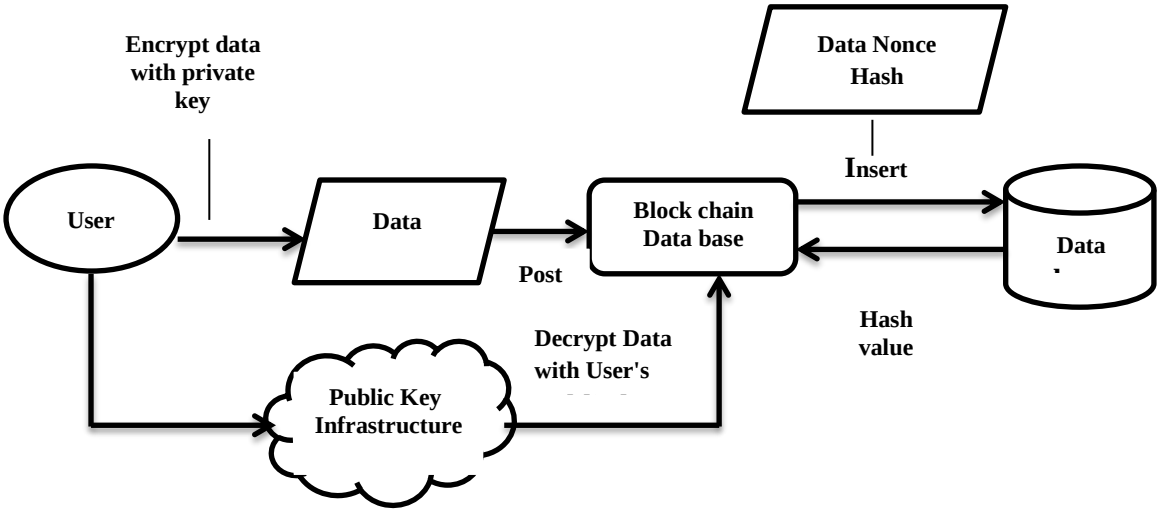
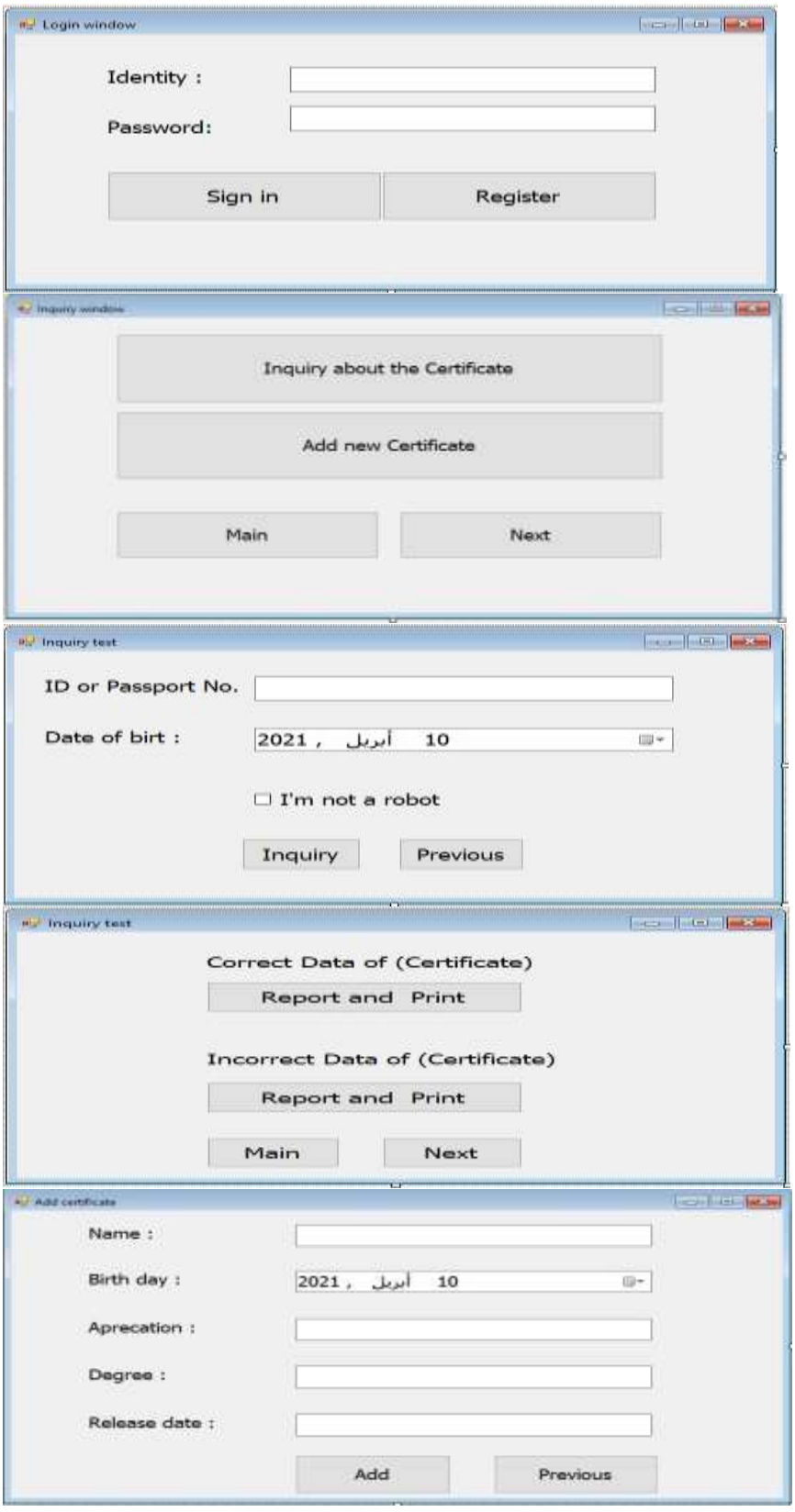


Figure 12: Data based on Block chain's data Architecture

DOI: https://doi.org/10.54216/IJAIET.010103
Received: February 20, 2022 Accepted: May 20, 2022

5. Program interface design:



DOI: https://doi.org/10.54216/IJAIET.010103
Received: February 20, 2022 Accepted: May 20, 2022

7. Evaluate proposed schemes:

No	Evaluation criteria	Degree of availability of the standard		
		Greatly convenient	**Medium suitable**	**inappropriate**
	The main Diagram			
1	Explains program design steps			
2	The layout design steps are consistent with the program			
3	The layout is clear and easy to understand			
4	The planner achieves the goal set for it			
	Analysis Diagram			
5	There is a high degree of safety in obtaining certificates			
6	Its steps are characterized by ease and simplicity			
7	Feedback loop available			
8	The diagram shows the steps for obtaining the certificate			
	Design Diagram			
9	The scheme achieves its main objective of securing and encrypting certificates			
10	The diagram illustrates the block chain steps for the proposed system			
11	The plan shows the possibility of issuing safe, easy and documented certificates			
12	It provides an iterative loop to get feedback			
13	Allows the privacy of dealing with the program			
14	It has a high degree of encryption to secure the data			
	Algorithm Diagram			
15	The diagram shows a method of coding using encryption algorithm (ASE)			
16	It achieves a high degree of safety and privacy of using(ASE)			
	Block chain diagram			
17	The diagram illustrates the block chain architecture			
18	It demonstrates the possibility of encrypting data in more than one way within the block chain			
	The program interface			
19	It is characterized by ease of use			
20	The interface of the software is visually appealing and comfortable			

System application results:

DOI: https://doi.org/10.54216/IJAIET.010103
Received: February 20, 2022 Accepted: May 20, 2022

The scale was applied by a group of experts and arbitrators in the field (n=11) to learn their opinions about the proposed system .Their response was determined on a scale (efficiency of the proposed system) according to the triple estimate (Greatly convenient- Medium suitable- Inappropriate) a continuous scale (3, 2, 1).

x^2 was used and tables from () to () x^2 values for repeats of the response of experts and specialists to the scale items for evaluating the proposed system were clarified.

Table (1) Results of the proposed system arbitration in accordance with (The main Diagram), n= (11).

Evaluation criteria	Degree of availability of the standard						x^2
	Greatly convenient		Medium suitable		Inappropriate		
	#	%	#	%	#	%	
Explains program design steps	10	90.9	1	9.1	0	0	16.545
The layout design steps are consistent with the program	6	54.5	5	45.5	0	0	5.636
The layout is clear and easy to understand	11	100	0	0	0	0	22
The planner achieves the goal set for it	11	100	0	0	0	0	22
d.f = 2							

From the previous table, it is clear that there are statistically significant differences between choices (Greatly convenient- Medium suitable- Inappropriate) to formulate axis sentences (Main Diagram) in favour of selection (Greatly convenient) in all sentences. This demonstrates the extent to which experts and arbitrators have agreed on the efficiency of the (Main Diagram).

Table (2) Results of the proposed system arbitration in accordance with (Analysis Diagram), n= (11).

Evaluation criteria	Degree of availability of the standard						X^2
	Greatly convenient		Medium suitable		inappropriate		
	#	%	#	%	#	%	
There is a high degree of safety in obtaining certificates	8	72.7	3	27.3	0	0	8.909
Its steps are characterized by ease and simplicity	11	100	0	0	0	0	22
Feedback loop available	9	81.8	2	18.2	0	0	12.182
The diagram shows the steps for obtaining the certificate	9	81.8	2	18.2	0	0	12.182
d.f = 2							

From the previous table, it is clear that there are statistically significant differences between choices (Greatly convenient- Medium suitable- Inappropriate) to formulate axis sentences (Analysis Diagram) in favour of selection (Greatly convenient) in all sentences. This demonstrates the extent to which experts and arbitrators have agreed on the efficiency of the (Analysis Diagram).

Table (3) Results of the proposed system arbitration in accordance with (Design Diagram), n= (11).

DOI: https://doi.org/10.54216/IJAIET.010103

Received: February 20, 2022 Accepted: May 20, 2022

Evaluation criteria	Degree of availability of the standard						X^2
	Greatly convenient		Medium suitable		inappropriate		
	#	%	#	%	#	%	
The scheme achieves its main objective of securing and encrypting certificates	9	81.8	2	18.2	0	0	12.182
The diagram illustrates the block chain steps for the proposed system	8	72.7	3	27.3	0	0	8.909
The plan shows the possibility of issuing safe, easy and documented certificates	11	100	0	0	0	0	22
It provides an iterative loop to get feedback	9	81.8	2	18.2	0	0	12.182
Allows the privacy of dealing with the program	7	63.6	4	36.4	0	0	6.727
It has a high degree of encryption to secure the data	10	90.9	1	9.1	0	0	16.545
d.f = 2							

From the previous table, it is clear that there are statistically significant differences between choices (Greatly convenient- Medium suitable- Inappropriate) to formulate axis sentences (Design Diagram) in favour of selection (Greatly convenient) in all sentences. This demonstrates the extent to which experts and arbitrators have agreed on the efficiency of the (Design Diagram).

Table (4) Results of the proposed system arbitration in accordance with (Algorithm Diagram), n= (11).

Evaluation criteria	Degree of availability of the standard						X^2
	Greatly convenient		Medium suitable		inappropriate		
	#	%	#	%	#	%	
The diagram shows a method of coding using encryption algorithm (ASE)	10	90.9	1	9.1	0	0	16.545
It achieves a high degree of safety and privacy of using (ASE)	9	81.8	2	18.2	0	0	12.182
d.f = 2							

From the previous table, it is clear that there are statistically significant differences between choices (Greatly convenient- Medium suitable- Inappropriate) to formulate axis sentences (Algorithm Diagram) in favour of selection (Greatly convenient) in all sentences. This demonstrates the extent to which experts and arbitrators have agreed on the efficiency of the (Algorithm Diagram).

Table (5) Results of the proposed system arbitration in accordance with (Block chain diagram), n= (11).

Evaluation criteria	Degree of availability of the standard						X^2
	Greatly convenient		Medium suitable		inappropriate		
	#	%	#	%	#	%	
The diagram illustrates the block chain architecture	10	90.9	1	9.1	0	0	16.545
It demonstrates the possibility of encrypting data in more than one way within the block chain	8	72.7	3	27.3	0	0	8.909
d.f = 2							

From the previous table, it is clear that there are statistically significant differences between choices (Greatly convenient- Medium suitable- Inappropriate) to formulate axis sentences (Block chain diagram) in favour of selection (Greatly convenient) in all sentences. This demonstrates the extent to which experts and arbitrators have agreed on the efficiency of the (Block chain diagram).

DOI: https://doi.org/10.54216/IJAIET.010103

Received: February 20, 2022 Accepted: May 20, 2022

Table (6) Results of the proposed system arbitration in accordance with (The program interface), n= (11).

Evaluation criteria	Degree of availability of the standard						X^2
	Greatly convenient		Medium suitable		inappropriate		
	#	%	#	%	#	%	
It is characterized by ease of use	9	81.8	2	18.2	0	0	12.182
The interface of the software is visually appealing and comfortable	9	81.8	2	18.2	0	0	12.182
d.f = 2							

From the previous table, it is clear that there are statistically significant differences between choices (Greatly convenient- Medium suitable- Inappropriate) to formulate axis sentences (The program interface) in favour of selection (Greatly convenient) in all sentences. This demonstrates the extent to which experts and arbitrators have agreed on the efficiency of the (The program interface).

First: the veracity of the scale

The current research in verifying the validity of the scales depended on the method of content validity, where the scale was presented in its initial form to a number of arbitrator professors, in order to get to know their views on the scale in terms of the accuracy of the linguistic formulation of the scale's vocabulary, the integrity of the content, and the affiliation of the phrases included in each axis. And the sufficiency of the phrases contained in each axis to achieve the goal for which it was set. The aforementioned modifications have been made to the wording of some phrases, and some phrases have been deleted, thus being subject to the validity of the content.

Second: Scale stability

The stability coefficients of the scale were calculated using the Alpha Cronbach and split-half method, and the following tables illustrate this

Table (7) Stability coefficient for scale n = (9)

Number of phrases	Alpha coefficient	Split half	
		Cyberman	Getman
20	0.877	0.802	0.801

It is clear from the previous table that the values of stability coefficients (alpha - half-hinged, which include Saberman's coefficient, and Guttman's coefficient) are high, which confirms the scale's stability and validity for application in the current research.

References

[1] https://www.nap.edu/read/9601/chapter/7

[2] Columbus L. Gartner hype cycle for emerging technologies, 2016 Adds blockchain & machine learning for firsttime[OL]. <http: // www. forbes. com/ sites /louiscolumbus /2016/08/21/ gartner- hype- cycle-foremerging- technologies-2016-adds-blockchain

[3] T.J. Gopane, "Blockchain Technology and Smart Universities," Proceedings of 4th International Conference on the Internet Cyber Security and Information Systems

[4]DaemenJ,RijmenV.ThedesignofRijndael:AEStheadvancedencryptionstandard.SpringerScience&BusinessMedia;2013

DOI: https://doi.org/10.54216/IJAIET.010103
Received: February 20, 2022 Accepted: May 20, 2022

[5]BouillaguetC,DerbezP,FouquePA.Automaticsearchofattacksonround reducedAESandapplications.In:AnnualCryptologyConference.Springer;2011.p.169–187.

[6]FazackerleyS,McAvoySM,LawrenceR.GPUacceleratedAES CBCfordatabaseapplications.In:Proceedingsofthe27thAnnualACMSymposiumonAppliedComputing.ACM;2012. p.873–878
.

[7] Chen, L., Lee, W. K., Chang, C. C., Choo, K. K. R., & Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. Future Generation Computer Systems, 95, 420-429.

[8] Li, H., Tian, H., Zhang, F., & He, J. (2019). Blockchain-based searchable symmetric encryption scheme. Computers & Electrical Engineering, 73, 32-45.

[9] Khan, P. W., & Byun, Y. (2020). A Blockchain-Based Secure Image Encryption Scheme for the Industrial Internet of Things. Entropy, 22(2), 175.

[10] (https://techterms.com/definition/blockchain)

[11] (https://blockgeeks.com/guides/what-is-blockchain-technology)

[12] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey onDecentralized Digital Currencies," IEEE
18, No. 3, 2016, pp. 2084-2123

[13.14) (J-Chen, S., Wang, H. & Zhang,).2018

[15] https://www.conicryptocash .com

[16]. Alrahili & Aldahawi, Journal of Information Studies & Technology, Vol. 2020(1). Art 5

[17]. Nechvatal, J., Barker, E., Bassham, L., Burr, W., Dworkin, M., Foti, J., & Roback, E. (2001). Report on the development of the Advanced Encryption Standard (AES). Journal of Research of the National Institute of Standards and Technology, 106(3), 511.

[18] . Alex Biryukov; Orr Dunkelman; Nathan Keller; Dmitry Khovratovich; Adi Shamir (2009-08-19).

DOI: https://doi.org/10.54216/IJAIET.010103
Received: February 20, 2022 Accepted: May 20, 2022