Data Encryption BasedBlock chain and IoT

Shaymaa Kaseb Layus [1]
[1] Department of Computer Science, College of Education for Pure Sciences, University of Thi Qar, Iraq.
Shaymaa-kaseb@utq.edu.iq

Baida Abdulredha Hamdan [2]
[2] Department of Computer Science, College of Education for Pure Sciences, University of Thi Qar, Iraq.
baida.alkinza66@utq.edu.iq

Mohammad Kaisb Layous Alhasnawi [3]
[3] Faculty of Administration and Economics, University of Sumer, Thi Qar , Iraq
mohammad.kasib@uos.edu.iq

ABSTRACT

Over the decades, several studies have been conducted on the art of cryptography which is the process of transforming secret data into an unreadable or scrambled form. More specifically, it is a technique to achieve the message secretly. however, the techniques that achieve the cipher data depending on many algorithms which make data unreadable to the human eye unless decrypted by the same algorithm that is predefined by the sender. Thus, in assessing the legitimacy of a traded information, hubs should arrive at an agreement to play out an uncommon activity, where case the chance to enter and record exchanges and problematic cooperation with the framework is fundamentally decreased. As of late, to share and access the executives of IoT devices data with disseminated demeanor another confirmation convention dependent on block-chain is proposed and it is guaranteed that this convention fulfills client protection, saving and security.

Keywords:

Introduction:

In simple terms, cryptography is the journey of converting information or messages form their plain text form into a scrambled unreadable form called the “cipher text”. Cryptography involves two phases: the encryption phase and the decryption phases. Encryption is the method by which the cipher code is generated with the help of a “key” or a rule that allows the scrambling of data, whereas decryption is the effort of generating the original message by deciphering the key by which it was scrambled.

In the very recent years, the term “Blockchain” resurfaced due to the emergence of the new digital currency “Bitcoin” and its popularity. The idea of Blockchain technology actually dates back to the 1990, but nowadays a lot of researchers, big companies, and financial institutions are investing their time and financial resources to develop a new range for their business by involving blockchain technology [1]. Blockchain allows the machine-to-machine transactions of digital currencies with the help of IoT by sending private data to blockchain networks over the internet. Other good applications are also linked with IoT such as cloud storage, digital ID, etc [2].

This paper consists of a background discussing blockchains history, architecture, its importance for encryption, and the blockchain model. Furthermore, a literature review will be conducted before drawing a conclusion to this study.

Background

Figure 1 shows the interesting growth timeline of blockchain technology. Blockchain technology was developed in the early 1990s, but in the past years it caused a revolution after the invention of Bitcoin using this innovative technology [3]. Blockchain became the digital record for the digital currency transactions. it name implies its structure, where the individual records or "blocks" are joined together in one list referred to as "chain". Transactions that are added to the blockchain must be validated by several computers [4,7,8].

Blockchain is a digital technology based on a huge cloud database, through which people can complete transactions or transfer money through a network of decentralized computers scattered around the world. Blockchain is likened to general ledger in accounting science because it is a public database in which digital information is stored for exchanges. Every cluster of nodes in the Blockchain functions on a peer-to-peer (P2P) network system. There are 4 different types of blockchains, two primary types (Private and Public) and other types such as Consortium and Hybrid blockchains [1,7,8].

1. Public: it is a large network for basic use and anyone can join the network of nodes for mining and exchanging cryptocurrencies (such as Bitcoin).
2. Private: it is a small and limited network. Its user needs permission to access the blockchain and can operate only in a locked network. Unlike public network, it does not require a third party for execution.
3. Consortium: it is a kind of semi-decentralized blockchain where several organizations manage the network (such as R3).
4. Hybrid: it is a more flexible system which uses the features of both the private and public blockchain types.

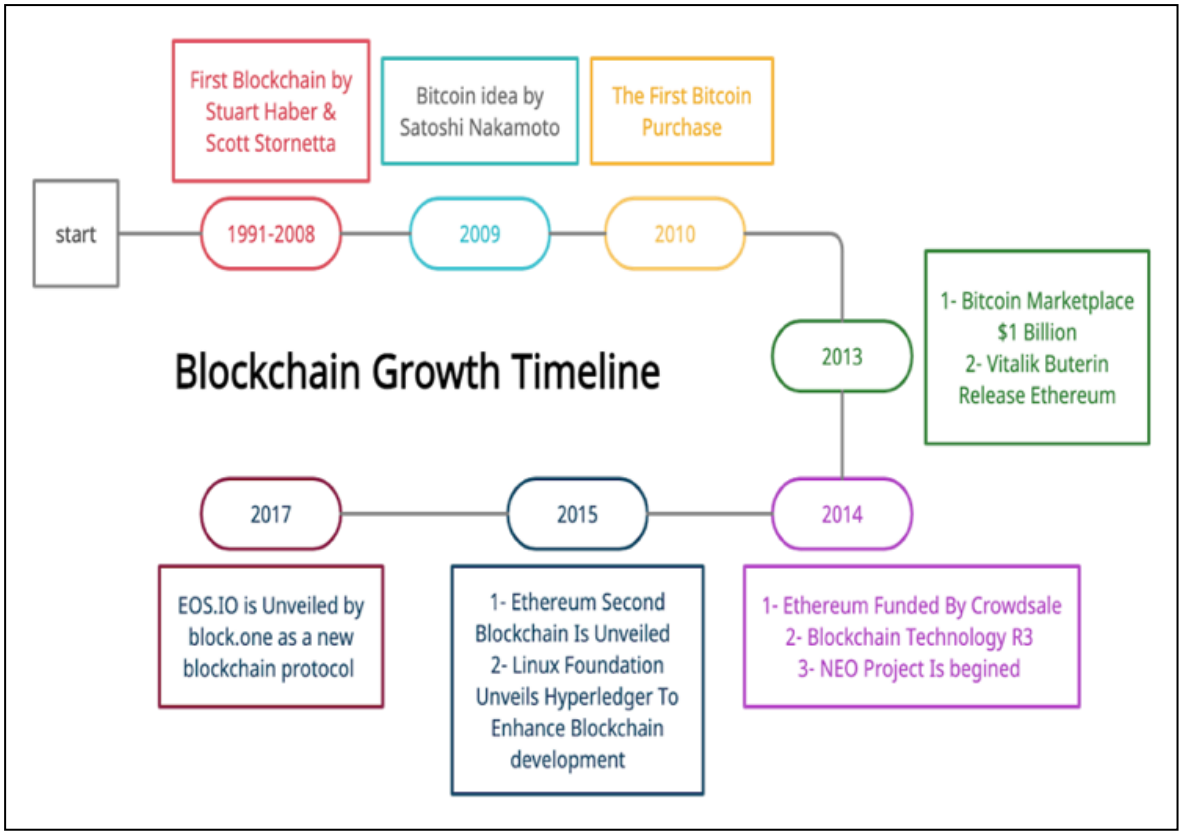


Figure 1: summary of the blockchain Growth [3].

Blockchain features:

In general, blockchain has many features such as:

1- Transparency: this means that the information stored in it can be viewed anywhere and at any time, unlike the normal encryption methods that completely block the information.

2- Privacy: the sender of the information can conceal his identity to protect himself from anyone who wants to track his transactions.

3- Distributed Technology: unlike traditional databases that store data on one or several servers, making the data penetrate, this technology depends on storing data by distribution. This means that the data is stored in multiple devices on a distributed network by nodes. Each node creates a copy of the data, so if the connection is interrupted, the database failure will not occur.

Therefore, blockchain is not intermediary and provides a much safer and immune space.

Blockchain-based architecture

Studies consider the architecture of blockchain as an IT architecture that have 3 layers as shown in Figure 2. [1, 8]

1- Top layer (Application): It is the final service for the company developed by blockchain. It provides the various interfaces for the users to visualize the data.

2- Middle layer (service): it is where blockchain is built by the distributed ledger and it has all significant modules that are regulated by the common services needed to apply all features. This layer is split into lightweight nodes and private blockchain [8] [11].

Lightweight nodes, also known as the tight nodes or thin nodes, have the same objective as the full nodes but instead of keeping a full history of a blockchain, it keeps block header that requires support and inquiry about the validity of the prior transactions. Header of the block carries a detailed summary about a specific block and contains information about the previous block linked to it [7]. The lightweight nodes are not used to store the main data, but to rise the speed of implementation of the asymmetric cryptographic algorithms. There are a lot of new processors but the best choice is ARM Cortex-M series [8] [11].

3- Physical layer (Bottom): it is made up of sensors, microcomputers and actuators. Here the network is represented by nodes that use the power to compute the consensus mechanism, or to store, refuse, and confirm the new transactions.

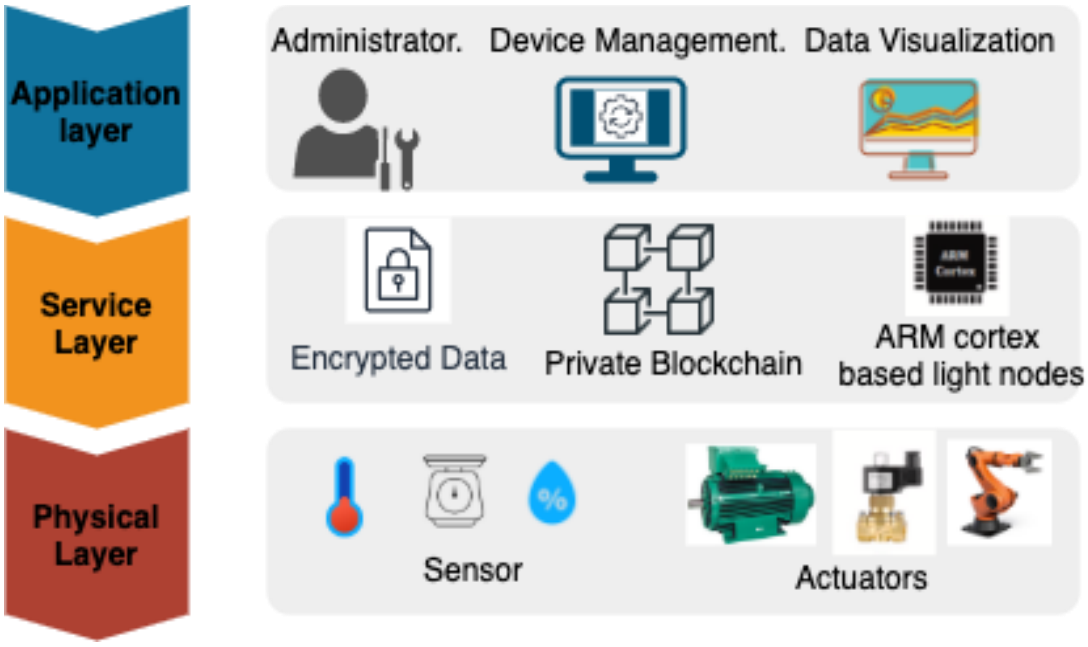


Figure 2: Architecture of the Blockchain [8].

Literature review

1. **A decentralized lightweight blockchain-based authentication; the mechanism for IoT systems:**

The Internet of Things (IoT) describes a system of smart heterogeneous objects that are connected over the internet and generate a huge amount of security-sensitive data. Thus, it is important to keep this data secure. This model is proposed based on authentication using decentralized lightweight blockchain.

The implementation for this study is divided into 3 stages. The first stage is the initialization which produces new systems to register with the network each having a unique identity. The second stage is the device registration that allows devices to get registered on the network. The last stage involves the use of the blockchain in the device authentication and provides a certificate to a device that is allowed to become part of the network. This model has many features to improve the security of data controlled by IoT since it produces secure communication between devices and allows the exchange of time-sensitive data [7]. This model also has cryptographic properties which are very important to protect data from outside attack. However, using the Ethereum blockchain adds additional time to complete a transaction which is a drawback for this model based on figure [3].

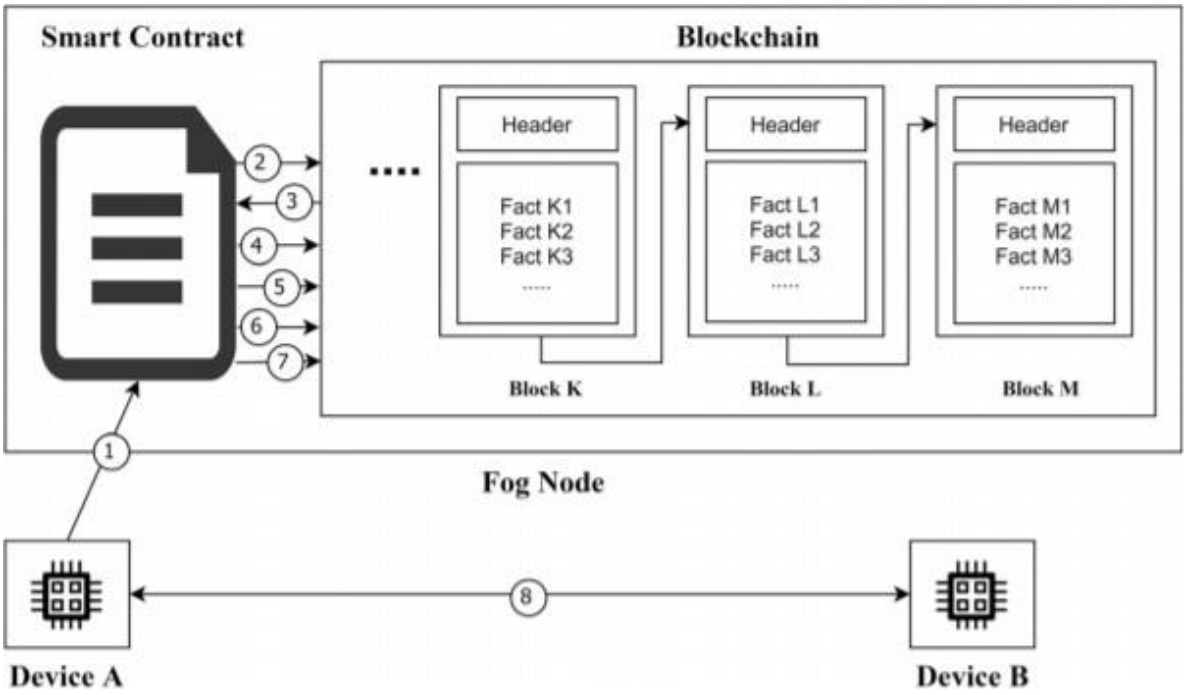


Fig. 3 Communication between IoT devices

2. **Multi-Layer Blockchain-Based Security Architecture for IoT:**

Blockchain technology is being further developed by researchers to address the privacy and security challenges in the IoT.

The proposed solution for the security challenges in the IoT is by using the architecture based on a multi-layer blockchain that depends on the concept of K-unknown clusters within IoT network through many algorithms, like the clustering algorithm. This enhances the coverage while minimizing the network load and energy. In addition, the open-source Hyperledger Fabric Blockchain framework findings of this model used to communicate with one another safely and the base stations use a global blockchain solution in order.

Furthermore, this proposed model is a good option for supporting ultra-reliable low latency massive Machine Type Communication while

using the capabilities and effectiveness of the cellular system under 5G networks.

Moreover, the implementation of this model shows many advantages like using the algorithms (K-unknown clusters within IoT network and open-source Hyperledger Fabric) which improve the efficiency of communications through the peer-to-peer nature of blockchain communication and maps it with enhanced integrity and protection.

In the security domain, this model is the best solution for framework confidentiality, authentication, heterogenicity, and availability, as well as network scalability. Unfortunately, this study has a drawback as it is affected by blockchain configuration like the number of users, endorsing nodes, the number of channels, and block size.

In conclusion, finding a solution for latency that is affected by blockchain configuration will help improve this proposed model [10].

3. A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things:

The aim of this study is how to use blockchain with IoT to improve the security of the overall system, especially in modern industry. In this architecture, the focus will be on how to access the valuable sensor and actuator data, as well as the private and lightweight blockchain.

The body of the system using blockchain draws on the performance of ARM Cortex-M processors for asymmetric cryptography. All network devices are allowed to create blocks in PoAh, but only trusted nodes can authenticate them.

Findings from a study of blockchain with IoT technology used user clients and associated IoT devices that are registered in the blockchain network during the initialization process in order to show that the cumulative results of service execution time suggest that the proposed blockchain platform performs satisfactorily for each activity. The advantages of this system are the easy and stable implementation of IoT blockchain. In addition, the blockchain mechanism allows the users that have access to a private network since not any unknown party is allowed to alter the blockchain. Implementing ECDSA on ARM Cortex-M processors is cost-effective as well. On the other hand, we have one disadvantage to the mechanism since it uses resources that impose some expense.

Finally, the proposed system is an ideal blockchain platform for a smart industrial environment because it is stable, secure, quick, and energy-efficient based on figure below that explain how the model process operate actuators [11]

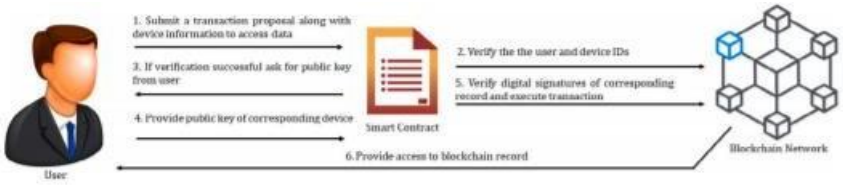


Fig. 7. Data acquisition process.

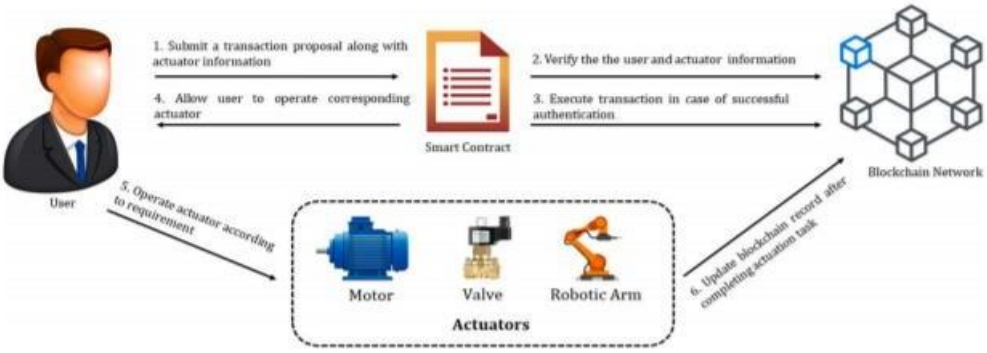


Fig. 4. The process to operate actuators.

Experimental Results and Discussion:

My proposed Encryption Algorithms are two:

The first one is describing the steps that help the image to secure it. So, we start with the initialization of the web service for the blockchain and nodes of the network because we have many image capturing devices which are acts as a node. After that, the node captures the image and sends it for processing by the chain. We summarize this algorithm that performs initial checks, verifies the time which is current time is less than the message distribution phase.

The CA mapped the node that has a cryptographically validated digital certificate and it assigns a digital identity to every node of the network. When the initial checks, it will start the encryption process for the image

Algorithm 1 The blockchain-based image encryption process.

Require: *BlockchainWebService*

Ensure: *genesisblock*

```
while T has not expired do
  if node N_i is authenticated == true then
    if request Ri matched == true then
      if Ri is identified as processed request == false then
        process for the response to C_i
        Hash(image)
        Update chain
      else
        Response to N_i that the Ri is not valid
      end if
    else
      Deny the Request
    end if
    Validate and Add block into chain
  end if
end while
```

The Second algorithm is encryption of the image that uses the image as a message digest.

First of all, prepossessing in which a padded message of the same size (parsed into blocks of 512 bits) as the image is created. So, the output gives a 32-byte or 256-bit string of ASCII characters. In addition, it is impossible to break because the use of the hashed key of the blockchain is so secure. After that, the image will be encrypted into a secure string then sent to the chain where all nodes will verify it. In the last step after verification, the block will be added to the chain which any computing device can obtain this image using the public key of the block

Algorithm 2 Image encryption

Require: $genesisblock(Gb)$

Ensure: $Image(P)$

Get m x n from P

initialize $y = uint8(zeros(mxn))$

initialize K=1

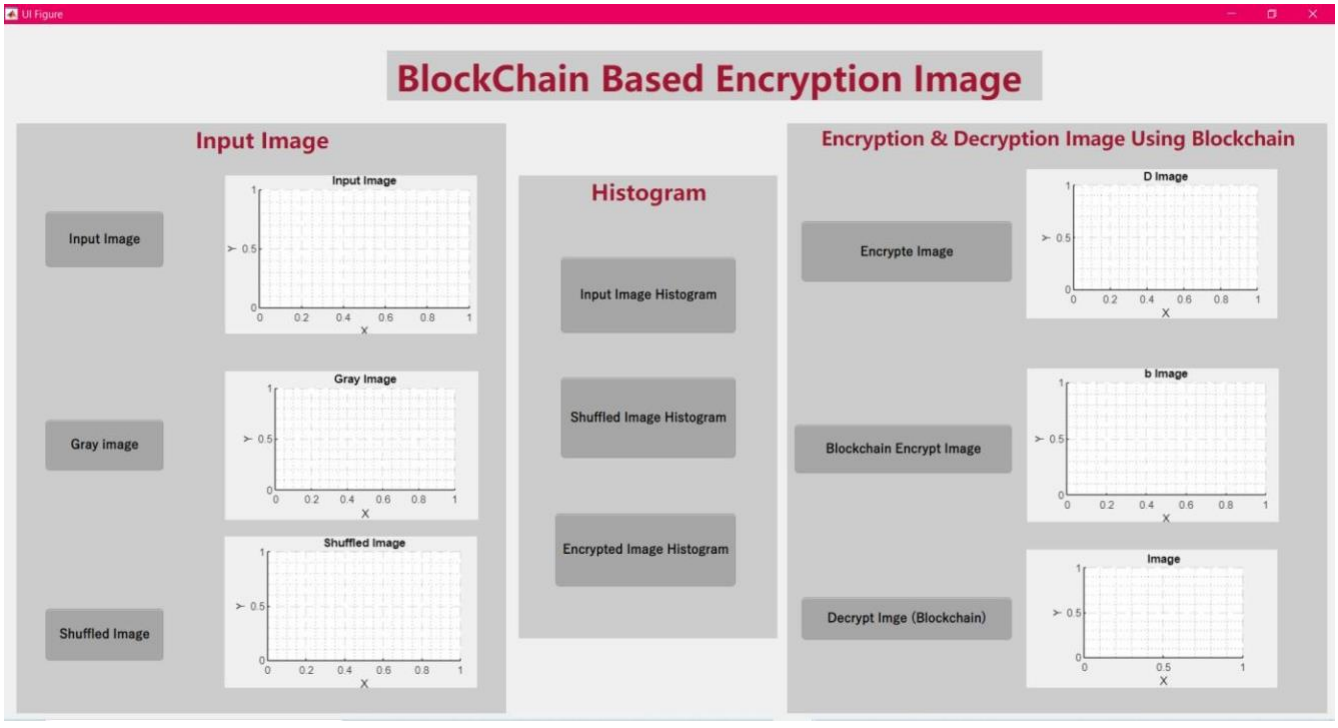
$sh = rand(1, 512 \times 512)$

$[t, Ind] = sort(sh);$

while i $\leq$ m **do**
  while i $\leq$ n **do**
    $temp = x(i, j : j + 31);$
    $y(i, j : j + 31) = (Gb(k, :) \oplus p(i, j : j + 31));$
    $Gb(k + 1, :) = uint8(sha256hasher.ComputeHash(y(i, j : j + 31)));$
    increment k by 1
  end while
end while

We used MATLAB2020 (App Design) for the simulation of the proposed scheme, that the 2 algorithms are merged in 1 GUI for ease of use. The proposed system obtains fine results.

Before we start to explain step by step how the system is working exactly, we need to list all the graphics and buttons first



Starting with the Input Image panel:

- It is composed of 3 grid spaces labeled as “Input Image”, “Gray Image” and "Shuffled Image"
- The Input image must be loaded by the user whereas the Gray image will be retrieved when clicking on the button "Gray Image"
- There are 3 buttons in the Histogram panel:

1. Input Image Histogram button
2. Shuffled Image Histogram button

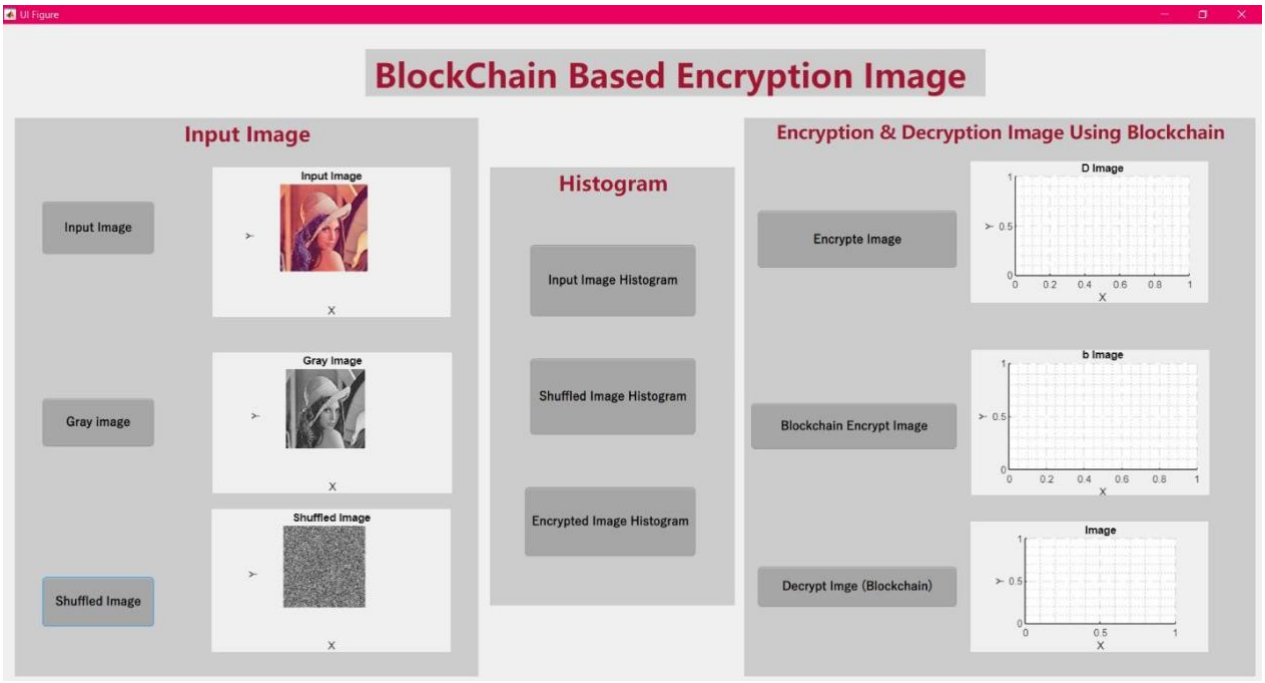
3. Encrypted Image Histogram button

The function of each button will be described later on.

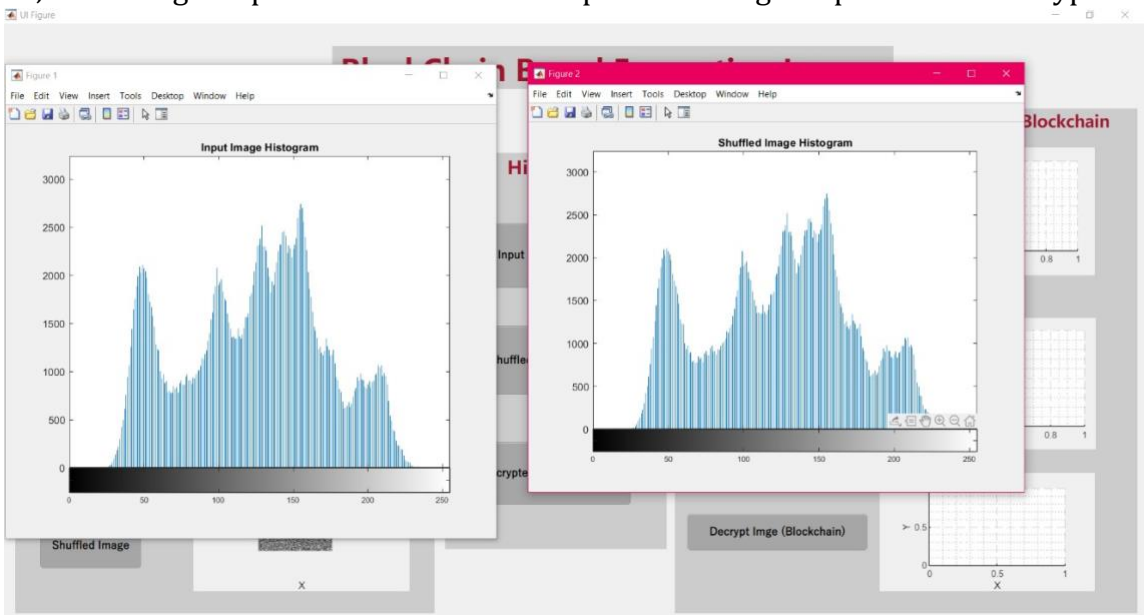
As for the Encryption & Decryption Image Using Blockchain panel:

- It consists of 3 grid boxes allocated for images, and labeled as “Encrypted Image”, “Blockchain Encrypt Image" and "Decrypt Image (Blockchain)"
- 3 buttons are assigned for these 3 grid boxes “Encrypted Image”, “Blockchain Encrypt Image" and "Decrypt Image (Blockchain)"

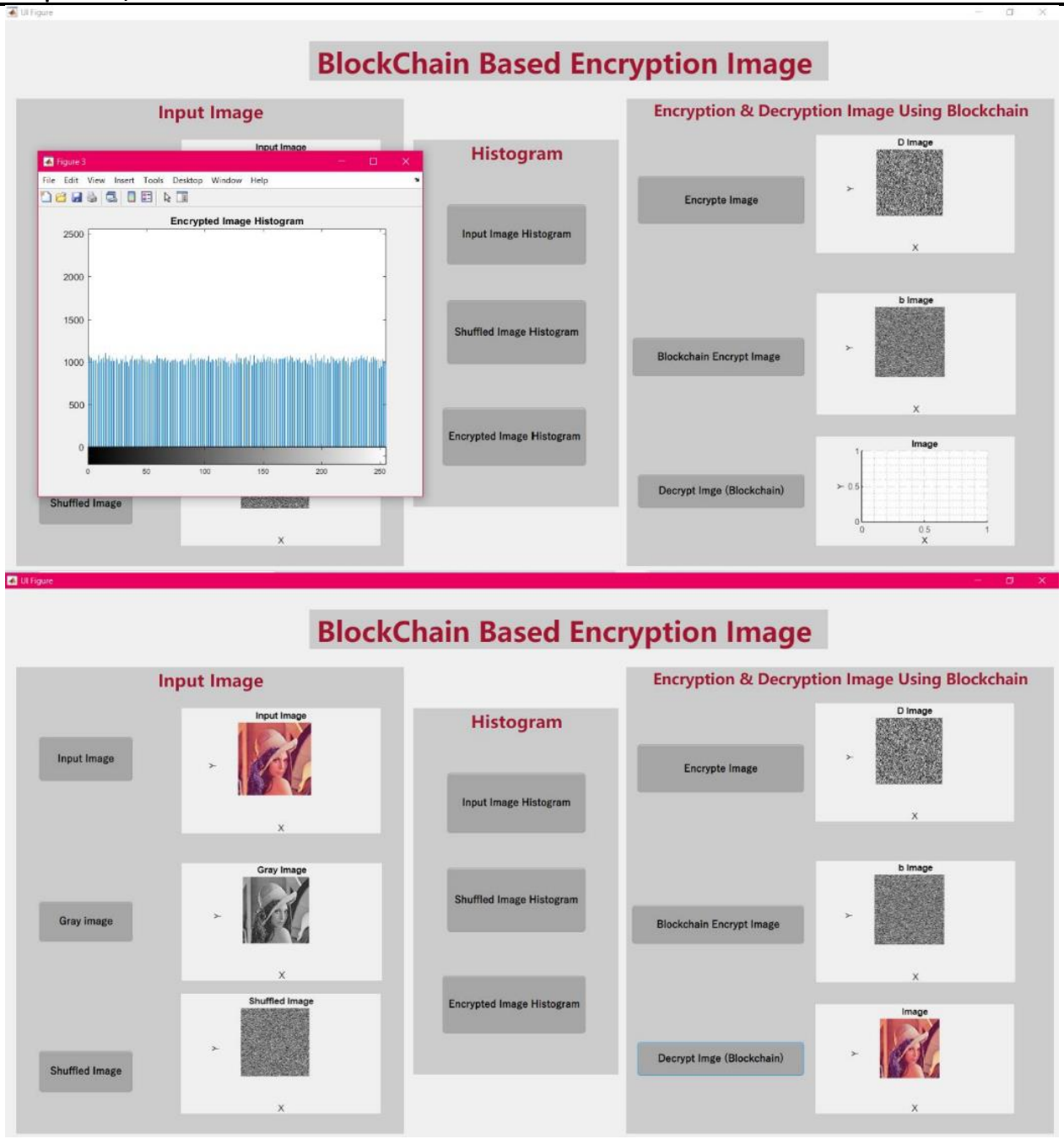
For experimental purposes, first of all, as we show in the figure below for the first panel which is Input Image. We selected a test image (Input Image), shown in Figure below. After that, we used grayscale images, so they range between 0 and 255. The y-axis represents the number of pixels containing those intensity values



Second, the Histogram panel that shows the respective histogram plots of the encrypted image



Third, the Encryption & Decryption Image Using Blockchain panel after applying the blockchain-based encryption scheme on our test image, we obtained an encrypted image



These plots and images show that the information on these images is completely hidden and unreadable. Now our images are safe and secure. We can offload those images to the cloud for further processing without the fear of any misuse of these images. We evaluate the security of the proposed scheme using information entropy analysis, the unified average change intensity (UACI), the number of pixels change rate (NPCR), histogram analysis, and noise attack.

Conclusion:

This paper gives an overview and proposed an algorithm secure image encryption scheme for an IoT-oriented network computing system based on blockchain. Although, some information on what is cryptography and how data encryption work based on blockchain explains some background about blockchain. In addition, how the blockchain store critical information securely in the IoT networks in different categories which show it in the literature review. Thus, the encryption feature, Blockchain is secure because its transactions

are done instantly and transparently. However, it gives some advantages for cryptography because it makes it possible for blocks to get securely linked by other blocks, and also the data stored on the blockchain are ensured reliability and immutability. We obtained many tests to verify that our proposed algorithm. Finally, the secure image encryption for an IoT-oriented network computing system based on a blockchain will prove helpful in safely offloading data from devices [10].

References:

1. De_Rossi, Leonardo Maria, Abbatemarco, Nico Salviotti, Gianluca, " Towards a Comprehensive Blockchain Architecture Continuum " 2019
2. G. Salviotti, L. De Rossi, N. Abbatemarco, "A structured framework to assess the business application landscape of blockchain technologies" in The 51st Hawaii International Conference on System Sciences, 2019.
3. Gwyneth Iredale, "History Of Blockchain Technology: A Detailed Guide", 2020
4. Zaghloul, E., Li, T., Mutka, M. W., & Ren, J. (2020). Bitcoin and Blockchain: Security and Privacy. IEEE Internet of Things Journal,
5. E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, "Scalable, transparent, and post-quantum secure computational integrity.," IACR Cryptology ePrint Archive, vol. 2018, p. 46, 2018
6. S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K. R. Choo, and A. Y. Zomaya, "Blockchain for smart communities: Applications, challenges and opportunities," J. of Network and Computer Applications, 2019.
7. Hany F. Atlam , Muhammad Ajmal Azad, Ahmed G. Alzahrani and Gary Wills. "A Review of Blockchain in Internet of Things and AI" 2020
8. Yves Longchamp, Saurabh Deshpande, Ujjwal Mehra, "Classification and importance of nodes in a blockchain network", The Bridge, 2020.
9. Umair Khalid, Muhamad Asim, "A decentralized lightweight blockchain-based authentication mechanism for IoT", Springer Nature, 2020.
10. Houshyar Honar Pajooh, Mohammad Rachid, Fakhuri Alam, "Multi-Layer blockchain-based security architecture for internet of things", sensors, 2021
11. Shahid Latif, Zeba Idrees, Jawad Ahmad, "A blockchain-based architecture for secure and trustworthy operations in the industrial internet of things",Elsevier,2020.