Republic of Iraq
Ministry of Higher Education and Scientific Research
University of Babylon
College of Information Technology
Software Department

Proposed Documents Security System based on Blockchain and Convolutional Neural Network

A Dissertation
Submitted to the Council of the College of Information Technology for Postgraduate Studies of the University of Babylon in Partial Fulfillment of the Requirements for the Degree of Doctorate of Philosophy in Information Technology

By

Mustafa Abdulrasool Ali Mohamed

Supervised by

Prof. Dr. Wesam Sameer Abedali Bhaya

2022A.D. 1444 A.H.

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة بابـــل
كلية تكنولوجية المعلومات- قسم البرمجيات

نظام مقترح لأمنية الوثائق بالاعتماد على سلسلة الكتل المترابطة والتعلم العميق

أطروحة

مقدمة إلى مجلس كلية تكنولوجيا المعلومات/ جامعة بابل والتي هي جزء من متطلبات الحصول على درجة الدكتوراه في تكنولوجيا المعلومات

من قِبـل

مصطفى عبد الرسول علي محمد

بإشــراف

أ.د. وسام سمير عبد علي بهيه

1444ه　　　　2022 م

بسم الله الرحمن الرحيم

وَقُلْ رَبِّ أَنْزِلْنِي مُنْزَلًا مُبَارَكًا وَأَنْتَ خَيْرُ

الْمُنْزِلِينَ 29

صدق الله العلي العظيم

سورة المؤمنون /آية (29)

Supervisor's Certification

I certify that this thesis " **Proposed Documents Security System based on Blockchain and Convolutional Neural Network** " was prepared under my supervision at the Department of Software / Collage of Information Technology / Babylon University, by " **Mustafa Abdalrasool Ali Mohamed** " as a partial fulfillment of the requirements for the degree of **Ph.D. in Information Technology**

Signature:

Name: **Dr. Wesam Sameer Abedali Bhaya**

Title: Assist. Prof.

Date: / / 2022

(Supervisor)

The Head of the Department Certification

In view of the available recommendation, we forward this thesis for debate by the examining committee.

Signature:

Name: **Dr. Ahmed Saleem Abbas**

Title: Assist. Prof.

Date: / / 2022

(Head of Software Department)

Declaration

I hereby declare that this thesis, **Proposed Documents Security System based on Blockchain and Convolutional Neural Network** submitted to University of Babylon in partial fulfillment of requirements for the degree of Doctorate of Philosophy in Information Technology-Software has not been submitted as an exercise for a similar degree at any other University. I also certify that this work described here is entirely my own except for reports and summaries whose sources are appropriately cited in the references

Signature:

Name: **Mustafa Abdulrasool Ali Mohamed**

Date: / / 2022

Dedications

To my Imam…

my Father…

my Mother…

my Family…

my Friends…

I will never forget your sincere
Love and support

Mustafa Abdulrasool Ali Mohamed

Acknowledgement

Praise be to Allah, Cherisher, and Sustainer of the world. I'm intended to His Almighty in helping me to finish what I started and present this work.

I want to express my deep appreciation and sincere gratitude to my supervisor: **Professor Dr. Wesam Sameer Abedali Bhaya**, whose dedication to this work has been boundless. His efforts to ensure the high quality of the material of this work have been invaluable. I have been lucky enough to be advised and guided by him.

Sincere appreciation is due to the department of software members for their help during this work.

Special thanks go to my examining committee for their constructive suggestion and perceptive comments.

Abstract

The development of distributed and secure electronic systems has become a vital subject in line with the development of the digital world. Especially after the COVID-19 pandemic, the reliance on computers and electronic systems has increased significantly in various areas of modern life. These systems preferred to provide exciting features such as transparency and decentralization with untampered data records. Preventing e-data forgeries and keeping them secure is an important component of any enterprise workflow, especially when sharing these data with a third party.

Thus, this dissertation aims to develop a secure, transparent, and decentralized digital document system that eliminates many security threats and adds layers of trust. The proposed system can create innovative effects on the systems that need to execute, store, update, and verify digital data among participating parties, with trust and transparency and without central authority control. So, a system for electronic document security system based on blockchain and convolutional neural network architecture has been proposed to prevent document forgery and provide privacy, transparency, and trust and get rid of the problems of the central system.

As a case study, the proposed system was applied to a Higher Education Certificates system to reduce certificates' forgeries and smoothly apply for certificates, as well as share and verify these certificates with a third party. The mechanism of the proposed model proposes permanent distributed hashes' records of students' certificates. In addition, remote verification through the portal provides immediate assurance of certificate integrity and authentication. This technique facilitates verification of a degree by a third party without the need of the issuing institution, which saves time for all parties.

The proposed cryptographic and hashing algorithms are analyzed and reviewed based on well-known tests in this domain, such as the Avalanche effect and National Institute of Standards and Technology (NIST) Statistical Test Suite. The experiment results show that the proposed algorithms have superior randomness and execution time. In addition, different tests such as Avalanche Effect and Hamming Distance, to check the resistance of the proposed Elliptic Curve Digital Signature Algorithm (ECDSA) against differential attacks, were applied. Four CNN transfer learning architectures Inception, VGGNet-19, ResNet, and VGGNet-16 are applied to images in documents with different hyper-parameters and architecture modifications. The experiment results show the accuracy of 72%, 80%, 82%, and 91% respectively.

Declaration Associated with this Thesis

Some of the works presented in this thesis have been published as listed below.

Mustafa A. Ali, and Wesam S. Bhaya. " Blockchain technology's applications and challenges: An overview." In AIP Conference Proceedings, vol. 2290, no. 1, p. 040019. AIP Publishing LLC, 2020.

Mustafa A. Ali, and Wesam S. Bhaya. " Higher Education’s Certificates Model based on Blockchain Technology" In IOP Conference Series: Materials Science and Engineering, vol. 928, no. 3, p. 032023. IOP Publishing, 2021.

Table of Contents

List of Tables

List of Figures

Table of Abbreviations

Abbreviation	Description
2D barcodes	Two-dimensional (2D) barcodes
CIA	Confidentiality, Integrity, and Availability
CNN	Convolutional Neural Network
CPA	Chosen Plaintext Attack
DApp	Decentralized Application
DDOS	Distributed Denial-of-Service
DL	Deep Learning
GUI	Graphical User Interface
HDFS	Hadoop Distributed File
HEI	Higher Education Institute
IoT	Internet of Things
IPFS	InterPlanetary File System
MIT	Massachusetts Institute of Technology
NFB	Notarizing Files over the Blockchain
OCR	Optical Character Recognition
P2P	Peer-to-Peer
PKI	Public Key Infrastructure
POS	Proof of Stake
POW	Proof of Work
RAID	Redundant Array of Independent Disks
RNG	Random Number generation
SHA	Secure Hash Algorithm
SPV	Simplified Payment Verification
VPN	Virtual Private Network

Table of Algorithm

CHAPTER ONE

General Introduction

1.1 Overview

In recent years, especially after the COVID-19 pandemic, the reliance on computer and electronic systems has increased significantly in various areas of contemporary life [1]. In addition, computers and networks with high-speed internet connections are now an essential part of our daily lives, and they are central to the progress and success of economic, communication, educational, and personal goals [2]. Consequently, that led us to the focus on developing sophisticated digital systems, which save effort and time while maintaining the works, preserving the required social distancing [3].

Although the various and observable benefits of this progress, it has also carried with it more critical threats to the security of online digital systems. One of the most critical issues that must be noted is that the network security in the current infrastructure is considered open to any type of attacks. Consequently, one should be careful of data security issues when he wants to play a digital system on such a network [4].

Today's organizations face a critical responsibility when it comes to keeping data secure. Whether it's internal proprietary information or any data related and collected from companies and clients, significant consequences organizations could face in the event of a data breach. That's why they need to have the proper security controls to guard against cyberattacks and insider threats while also providing document security and always ensuring data availability. As a result, developing information security policies are the researchers, specialists, and information security organizations concerted [5].

In general, information security policies focus on protecting three critical aspects related to data and information, which are confidentiality, integrity, and availability [6].

Each aspect is objective to address a different part of data protection. Collectively, they are frequently referred to as the CIA model or CIA triad (Confidentiality, Integrity, and Availability) [6], each attribute represents a fundamental objective of information security concept and as follow:

a. Confidentiality:

Confidentiality of information talks about ensuring that sensitive data is protected and kept away from being exposed to an unauthorized party due to a data breach or insider threat. Confidentiality can be applied using data access restrictions mechanisms such as encryption, passwords, access control lists, two-factor authentication, and biometric verification [6],[7].

b. Integrity:

The integrity of information ensures that the data is not modified by an unauthorized object/person and it is in the same format and content as its original source. It is securing the data, so it guarantees the receiver has received genuine data by comparing original data with received one. Integrity can be applied using cryptographic encryption and hashing of the data [6], [7].

c. Availability:

Availability ensures that data and system are available when you need them. It is focus on eliminate or mitigate the possibility of downtime and unreachable data using different technology and methods such as redundancy, RAID, and high-availability clusters. A common solution for such failures is to run an active/active system, where an independent processing node with a replicated database, so all nodes participate in a common application. Another solution is an active/passive system, where the second “standby” node is used if the first node fails [6], [7]. Figure (1.1) shows CIA model.

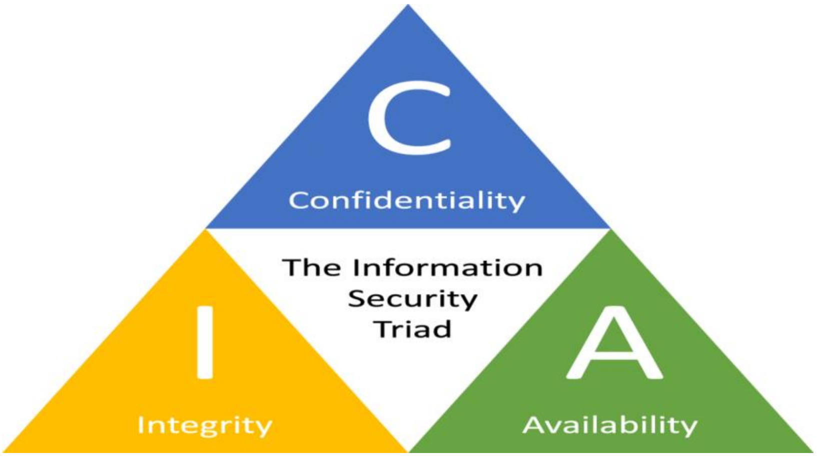


Figure (1.1) CIA triad (Confidentiality, Integrity, and Availability) [7].

Any professional Information System should have a perfect balance between security (Restrictions), usability of Graphical User Interface (GUI), and functionality (Feature). There is always an Interdepend ability between these three attributes [8]. Thus, a tradeoff between these three is necessary to maintain the system work in real world (i.e., moving towards security means less usability and functionality). So, the level of security in any system can be defined by the strength of these three components and the software engineering should balance between these three qualities to arrive at a balanced information system [9]. Figure (1.2) shows security, functionality, and usability triangle.

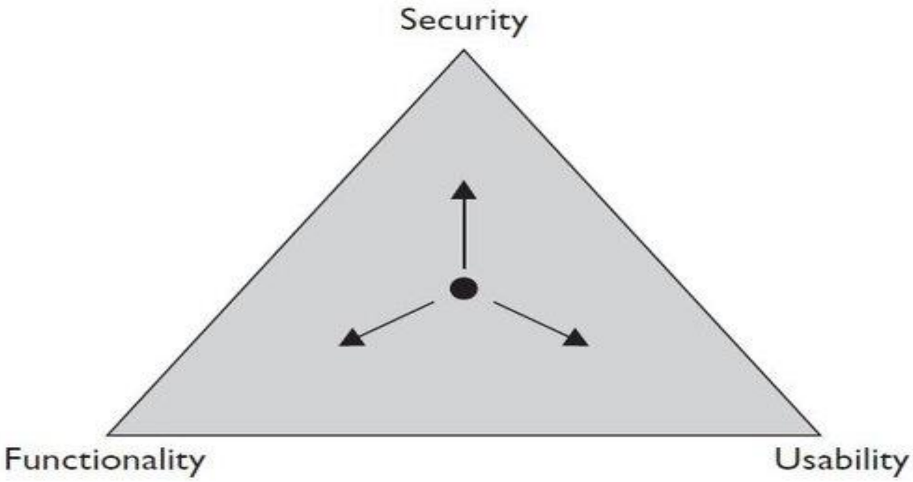


Figure (1.2) Security, Functionality, and Usability Triangle [8].

In next paragraphs, the system usability and functionality will be explorer and as follow. The system usability scale has strong related to CIA model which measures:

- **Effectiveness** (can users successfully achieve their objectives).
- **Efficiency** (effort and resource to achieving those objectives).
- **Satisfaction** (was the experience satisfactory).

Finding a balance between these three objectives should ensure their achievement without significantly affecting one of them [9], [10]. For example, if one of these objectives is given great attention, the other components will be negatively affected, so we need to achieve good security while maintaining the functionality and usability of the system.

However, there is an important issues; how to ensure the records and data that are transferred between these digital systems are not modified, as well as make sure that the sources coming from are the correct sources as they are claimed [11]. Furthermore, keeping these records and data securely and not tampered with or damaged.

Thus, researchers try to develop a dimension that allow transfer these data records through the Internet using current architecture. So, nodes can easily share data with other nodes. More nodes can easily be added to the distributed system (i.e. it can be scaled as required) [10], [12]. This dimension should be able to keep and store important data in secure and resident manner and get red from most critical malicious actions such as distributed denial-of-service (DDoS) attacks [13], [14].

Furthermore, data should be verified to ensure its integrity and authentication. Document considered a most common data type that sharing important components of any enterprise workflow. Keeping these documents secure is fundamental to enterprise security, especially in multi-site enterprises or when sharing documents with third party. Document verification is the process taken to ensure that the documents received from the owner are genuine and that the owner is legitimate [15], [16]. The verification of the Document removes suspicion about the Document content and the issuer institution. Whether the Document issued by the alleged institution, as well as the issuing institution, is authentic [15], [17]. This always validates the issuing institution and the qualifications that it provides. The goals of verification are also to ensure that the Document has not been altered by the holder and whether it has been truly issued to the owner [14], [16], [17]. Document verification is steps to seek and trace to ensure that the Document is authentic from its source, means of issuance, and other details about the basis for issuance. It is the process that establishes the originality of something using the confirmed technique. [18].

In contrast, Blockchain is a technology that considers more complex than the peer-to-peer(P-to-P) or distributed technology. In other words, P-to-P compromise on machine-to-machine (M2M) transportations where blockchain added a more complex dimension that also involves M2M and the smart contract and consensus concept [19]. Table (1.1) summarizes the differences between traditional, digital, and blockchain systems. The information in table (1.1) are extracted based on references [3]-[10] and reformat to provides useful knowledge to other researchers.

Table (1.1) The Comparison Among Traditional, Digital, and Blockchain Systems.

Criteria	Traditional system	Digital system	Blockchain system
Availability	Low	Medium	High
Integrity	Low	Medium	High
Confidentiality	Low	Medium	High
Functionality	Low	High	Medium
Usability	Low	High	High
Complexity	Medium	Low	High
Scalability	Low	High	Medium
Decentrality	Low	Low	High
Trust	Low	Low	High
Cost	High	Low	High

However, recent studies have examined different issues by designing document integrity and authentication systems that achieve security, cost, and network infrastructure.

1.2 Related Works

There are various studies about document integrity and authentication that presented in previous works and should review to start from this literature study. Recognition and preventing documents forgery based on different techniques and technology such as encryption, hashing, blockchain, neural network, and others has recently arisen as a distinct approach. Until 2022, it is difficult to identify some of the highly skilled forgeries [18], [19]. This topic has induced the attention of various researchers and studies applied in diverse environments and applications. Some of these studies are discussed in the following.

In (2014) [20], the University of Nicosia was the first university in the world who register academic certificates for an online course on the Bitcoin blockchain. A hash of an index document, which contains a list of hashes of all certificates for a specific semester is registered on the blockchain. Their approach is decentralized, permission less and transparent, but does not allow for integrated issuer verification and for validating the completeness of issued academic certificates.

Aaber and Wills (2017) [21], proposed framework that adapting current technologies in new novel approach to deliver a secure environment to share e-documents and track them. The confirmed framework secures documents not only inside the enterprise, but also when they leave the enterprise boundaries via networks or portable devices. As the author’s knowledge extends, there is no other work similar to what this paper provides regarding proposing such a framework. The framework provides a persistent and secure environment through the e-document life cycle and ability to track the document. Their framework includes components utilizing active document concept, digital right management concept, context awareness, and a central certification authority service.

In (2018) [22], the MIT Media Lab is working on a project called Blockcerts2. Their approach is similar to the one implemented by the University of Nicosia, i.e., registering the root hash of a Merkle tree of hashes of documents on a public blockchain. This approach is decentralized, permissionless and transparent. The project is not attempting to map the digital identity to the real identity of an institution and thus does not allow for integrated issuer verification and validation. Additionally, verifying the completeness of issuing documents is not possible.

Gr¨ather *et al*., (2018) [23], introduced an approach for a Lifelong Learning Passport (LLP) is presented which is very similar to the approach of Blockcerts. Their approach is decentralized, transparent and additionally they support a mechanism for issuer verification. However, they use a hierarchical scheme for issuer accreditation and therefore it is not fully permissionless.

Hasan *et al.,* (2018) [24], developed an off-chain communication exchange protocol to stabilize a secure channel for downloading digital content using Ethereum and IPFS. The integration of blockchain and IPFS technology was also undertaken, to form a framework for a secure, tamper-proof model for academic-research record-keeping with access control methods. The framework utilized smart contracts for storing the metadata of research in the blockchain network and auditing purposes. To enhance file confidentiality, the researchers encrypted the files with the master key before they were uploaded into IPFS.

Mthethwa *et al.*, (2018) [25], proposed a solution consists of 2 main processes; generation and validation process. Solution incorporates the combination of 2D barcodes, OCR, cryptographic hashing and blockchain. OCR was the first technique to be implemented, whereby documents were generated using a font known as any OCR (which is designed for OCR tools) and Tesseract was used to validate the documents. The experimental results yielded an accuracy of 100%, which is excellent. The second part of the experiment was to combine all the above techniques, whereby new documents were generated and the validation text was specified which was then added to the barcodes that are positioned at the bottom of the documents. By using this validation process, the system was able to detect when documents have been tampered with. Furthermore, blockchain has been added as one of the techniques to be employed for document verification. As this is still on-going work, experiments are still required to demonstrate the viability of the solution.

Brunner and Engel (2019) [26], present SPROOF, a platform for issuing, managing and verifying digital documents in a public blockchain. In the proposed approach, all data needed for verification of documents and issuers is stored decentralized, transparent, and integrity protected. The platform is permission less and thus no access restrictions apply. Rather, following principles of the Web of Trust, issuers can confirm each other in a decentralized way without the need of a single trusted platform operator. Additionally, scalability and privacy issues are taken into consideration.

Yatskiv *et al.*, (2019) [27] tried to prove the integrity of videos on cloud services by calculating the hash of each frame and sending the hash to the blockchain, which is trusted by interested parties. To store large amounts of data on distributed storage systems using blockchain technology, researcher utilizing one study that created the protocol for notarizing files over blockchain (NFB), to ensure communication between the Hyperledger blockchain and OKORO (a secured centralized archiving document management system).

Permatasari *et al.*, (2020) [28], suggest a good archive management system that consider information security aspects, such as availability, confidentiality, and integrity. The Cilegon E-Archive (CEA) system is a centralized system for managing the lifecycle of archives. The existing CEA system has several problems, including a single point of failure, low data availability, and difficulty in proving the originality of files. They introduces a prototype for a new CEA system that integrates IPFS and the Ethereum private network. In addition, CEA DApp is developed as an interface for users in interacting with CEA system, and its functionality is managed by a smart contract. The results show highly improved the CEA system security in terms of preventing archival forgeries.

Dharmalingam *et al.*, (2021) [29], proposes a prototype model for digitally managing and attesting the academic records using permissioned blockchain technology. By this method, the block-chaining of a student record begins from the time of admission to the Higher Education Institute (HEI) and continues to record the academic progress until graduation, having the graduation details stored as the last block in the chain. The whole blockchain of the student record will remain in the system with the participants enabling any indirect stakeholder to verify the details instantly based on the hash code or QR code. Additional privileges will be provided for direct stakeholders such as in Oman the Ministry of Manpower and the Ministry of Higher Education to access further details of the certificate-holder. The system includes the student as a stakeholder and also as a participant to ensure transparency for her/his academic records.

Gadise Adeba, (2021) [30], proposes a framework for the creation of a Smart Document with the use of a digital signature that is embedded in a Quick Response (QR) code for verification of the document. Also, the hash of the document along with transactional details is stored in a blockchain that provides a shared, immutable, and transparent history of document without depending upon any third party. The proposed solution will facilitate the verification of documents both in its electronic and paper form and provides an assurance of integrity, authenticity, and availability of information in an immutable and transparent environment.

1.3 Problem statement

Document integrity and authentication application has been applied in various sectors and encountered different challenges. Most of the challenges that need to be addressed when working with a document environment are transparency, trust, and security issues.

The origin of prevalent document fraud can be traced back to people without required qualifications who want to become rich, have power, honor, or be employed quickly. Unemployed youth, graduates, and potential college students soon learned that intellectual effort and the need for serious study is not required to achieve their wish. Instead, they seek suspect connections and then obtain forgery credentials by any means. However, hired fraudulent means became broad, especially when the matter regarding the financial and government documents.

Document environment IP-based structure and there is a tremendous increase in using these document that leads to attack the data which transferring through the communication channels. These evolutions in communication technologies highlight the need for developing a robust security algorithm. Besides, there is a necessity to evolve security systems that include data analysis, threat exposure, and integrity for un-secure communications. In contrast, when working with digital documents, some of the security issues were highlighted in recent studies are authentication, integrity, confidentiality, and availability.

1.4 Motivation

The development of distributed and secure electronic systems has become an important subject in line with the development of the digital world. The application of blockchain technology is an excellent example of these systems that provides exciting features such as transparency, trust, and high availability with untampered and permanent data records. The implementation of such technology to systems that issuing documents, especially important to many sectors such as government, economic, educational, and individuals. Moreover, these systems present an opportunity to verify shared documents quickly, securely, and independently.

On the other hand, deep learning approach has good result different area such as convolutional neural network (CNN) based architecture has been used in computer vision an image classification and recognitions, especially in last decade. The fundamental motivation behind proposing model is to create document issuing, managing, and verification systems to prevent document forgery and provide trust and transparency to these systems. We aim to put in place a robust yet fast document violation detection mechanism. This can be achieved with the benefits of blockchain and CNN based architecture that can put the power back in the hands of document issuing institutions. For example, individuals are subject to many academic studies and training from several different institutions, and they obtain several certificates, which is critical. The process of preserving these certificates in a way that is permanent, not tampered with, or forged is very important.

Also, information security is the main inspiration for dealing with other issues such as availability and integrity, encouraging researchers to deeply investigate modern approaches to deal with security issues. This work is primary concerned with designing a security system to protect sensing data from unauthorized access, disclosure, and modification. Thus, to prevent threats and find suitable solutions, there is a need to design a model for document security system.

1.5 Aim and Objectives of Dissertation

In this dissertation, proposed a design and implemented of a proposed system for a document security system based on a developed blockchain concept, cryptographic algorithm, and a convolutional neural network (CNN). Designing a model to achieve a high secure digitized document systems is required goal. The digitized guarantee created a single information source with lower fraud potential and greater efficiency.

The objectives of this dissertation are mainly based on grouping the essential elements of information security systems that must be achieved, such as confidentiality, data integrity, and authentication.

Also, the major objectives of this dissertation are to

1- Propose and design a model for document integrity and authentication system.

2- Implement a system for document issuing and verification.

3- Implement a modified cryptosystem algorithm.

4- Develop and implement a CNN model.

5- Validate and evaluate the proposed cryptosystem.

1.6 Contribution

The main contribution of this dissertation is designing and implementing a secure model for preventing documents forgery and ensuring documents integrity and authentication based on encryption algorithms, machine learning and blockchain concepts. However, the contributions of this dissertation can be summarized as the following: -

- Designing and implementing proposed model based on blockchain concept.
- Designing and implementing proposed distributed machine learning model.
- Developing and evaluate an efficient cryptographic algorithm.

1.7 Dissertation Layout

In count to chapter one, this dissertation comprises of the following: Chapter Two contains theoretical background and the essential details about the digital document, document forgery, document integrity and authentication, cryptography algorithms, a machine learning, neural network, CNN, blockchain concept, Blockchain model and types, and hashing algorithms. Chapter Three illustrates the proposed model, developing cipher algorithms, hash function, digital document certificate, software setup, and pseudocode of the primary system implemented in cipher algorithms. Chapter Four elucidates the experiment results and analysis of the proposed model and developed algorithms with an adequate discussion of the results. Chapter Five describes the conclusion of this dissertation and shows the recommendations and suggestions for future work

CHAPTER TWO

Theoretical Background

2.1 Introduction

This chapter presents the theoretical background of the techniques and concepts that are used in this dissertation. The overview will describe digital document, network architecture, databases, and cryptography. Then, the blockchain architecture, protocols, types, applications, and challenges and security issues are explored. Also, different cryptographic systems such as stream and block cipher, SHA-3, and cryptanalysis system and measurements are described. Finally, a briefly displays of the deep neural network and CNN model are presented.

2.2 Digital Document

A good and accurate understanding and definition of a digital document must first understand "What a document is?" because a digital document is seen as a special case of a document. Early in this century, the beginnings of attempts to provide a definition of what should be considered a "document" because of the rapidly growing quantity of available documents raised the previous question. Generally, the word "Document" refers to a textual, drawn, presented, or memorialized representation of information, objects, thoughts, and phenomena, whether physical or mental [31].

A digital document primarily refers to an electronic textual file format whose structure includes fonts, colors, and images. Contemporarily, documents are not defined by their transmission medium, such as paper, given the existence of digital documents [31]. Whether the textual file is paper or digital, a serious problem is document falsification, which can nullify the advantage of using those documents or even cause more damage than benefits [32]. In the following sections, an explanation of the problem of document forgery will be introduced.

2.2.1 Document Forgery

The art of forgery is as old as the alphabet. The crime of forgery has been practiced since ancient times in every country where writing existed, and paper was used. The earliest known writing language was invented around 3400 B.C. and it was used by the people of Sumer in Southern Mesopotamia. A little later, the Egyptians were inventing their own hieroglyphic writing.

Laws against forgery can be traced to 80 BC when the Romans prohibited the falsification of documents that transferred land to heirs. Forgery was prevalent in Europe in the Middle Ages. Gradually, laws were passed to prohibit forgeries in every developed country [32].

In 1562, a statute was passed in England prohibiting forgery of publicly recorded, officially sealed documents. These documents pertained to titles for land. In 1726, an expansion of the forgery laws made a false endorsement on an unsealed private document a capital crime punishable by death.

In the United States, the principal federal forgery statute, prohibiting false making, forgery, or the alteration of any writing to obtain financial gain, was enacted in 1823. The American Law Institute’s Model Penal Code of 1962 simplified and defined the elements of forgery and became the standard for defining the crime of forgery [32].

In the same context, the development of information and communication technologies has extended to different fields and has become an essential part of business development, and electronic documents have become the natural alternative to paper data in those systems. This transformation has led to the emergence of electronic forgery crime, and this crime has increased and spread because of the development of tools and technical skills for forgery [33]. Until 2022, it is difficult to identify some of the highly skilled forgeries [19].

2.3 Network Architecture

A computer network is a colocation of two or more autonomous computers that connect and communicate to one another using a common transmission medium to allow resources sharing. There two common architecture of computer network which are a client server network and a peer-to-peer (P2P) network. Networks offer many benefits such as reducing the effort, time, and cost [34],[35].

2.3.1 Networks Impacts

Networks can allow users to reduce expenses and improve efficiency by sharing data and common equipment among many different computers. Proposed model exploits some of these benefits to do its tasks, and as follows:

- **Sharing files:** In a network environment, any authorized user can access data and information stored on other computers on the network.
- **Remove distance:** Information can be accessed across the world.
- **Reduces time:** Access information at anytime from anywhere in the world as it delivered faster than any physical transportation.
- **Easily backup and recovery:** They can be performed efficiently and automatically as the almost same data is stored on all peers.
- **High flexibility:** Gives users the opportunity to use software and data without affecting their functionality. Moreover, users can use separate passwords to access authorized information they need to get or share.
- **Higher availability and robust:** If one or a group of peers fails, the whole network does not go down and working is performed without interruption.

2.3.2 Classification and Architecture of Computer Networks

Architecture refers to the broad design of the rules and logical layout of the network, which the hardware and software must follow to communicate (i.e., patterns of communication). The rules that must be followed are protocols, in this sense network architectures are comprised of hardware, software, protocols, and the connected devices. There are various network architectures, each one has a certain characteristics and application domain. In general computer networks can be classified according to their size and geographic scope, type of physical topology, node's role, etc. [36],[37].

According to network node's role there are two of the most widely used types of network architecture are either decentralized peer-to-peer (P2P) or centralized (Client/Server). The network nodes play a different role in a client-server architecture, where the server node is a superpower computer that efficiently provides data and service to other client nodes. Instead, the network nodes play almost the same role in P2P architecture and share their data and resources without the need for a dedicated server. It is worth mentioning that the proposed system has been implemented using permission network.

2.4 Distributed File System and Databases

The InterPlanetary File System (IPFS) is a protocol and peer-to-peer network for storing and sharing data in a distributed file system. IPFS consists of several innovations in connecting protocols and distributed systems that have been mixed to make a file system like no other [38]. However, there are other types of distributed file systems such as Hadoop Distributed File System (HDFS) is the main data storage system used by Hadoop applications. HDFS employs a (Name Node) and (Data Node) architecture to execute a distributed file system that provides performance access to data across highly scalable Hadoop clusters. HDFS is fault-tolerant and is designed to be run on low-cost hardware. HDFS provides high throughput entry to application data and is suitable for apps that have big data sets and enables streaming access to file system data in Apache Hadoop [39].

2.5 Cryptography

Generally, cryptography is the process of secure information by converting sensitive plain text into nonreadable format and vice-versa. It can be defined as an approach mainly based on mathematically theory procedures and algorithms to secure messages and information in computers and network communications. Earlier to the modern age, cryptography was equivalent to encryption. Currently, modern cryptography concerns four central practices, which are data integrity, confidentiality, authentication, and non-repudiation. In theory, it is possible to crack a well-designed cipher, but it is not possible to do so in many practical ways [40],[41],[42]. However, figure (2.1) shows cryptography schemes which are asymmetric, symmetric, and hash function.

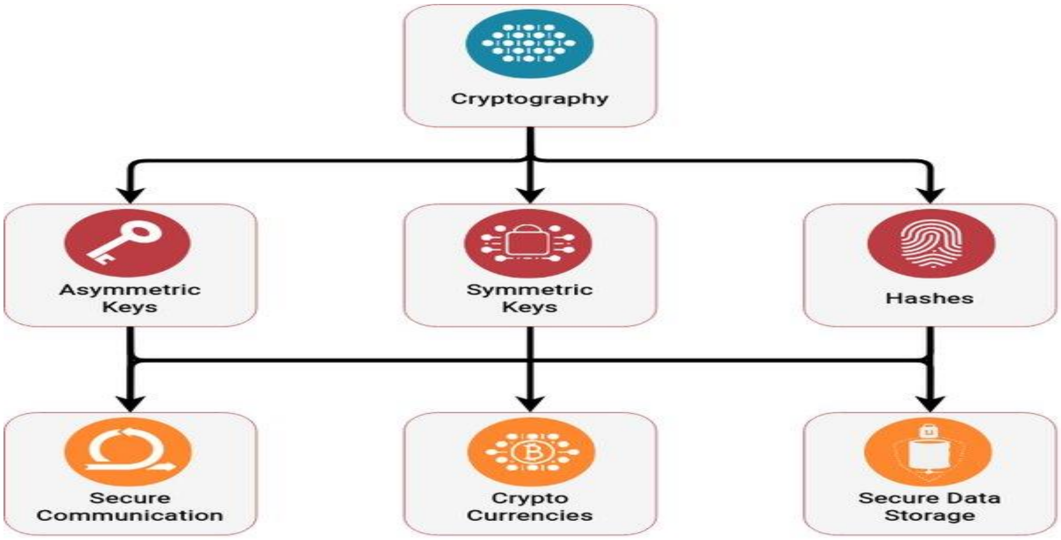


Figure (2.1) Cryptography Systems schemes [40]

Firstly, asymmetric cipher algorithms are built based on two keys, public and private, for message encryption and decryption. The public key can be shared with everybody, and the private key is reserved. In this cryptosystem, one key is implemented for encryption and an alternative for decryption [43].

Secondly, in the symmetric key approach, the same key is used for both encryption and decryption processes. Furthermore, asymmetric approaches are used for exchanging secret keys to prepare for using symmetric cryptography.

Lastly, hashing algorithms are one-way functions that generate a fixed-length hash value from any given length of the input, and they are used to verify the integrity of data. The result is non-invertible, which means it can only process one-way mathematical procedures. However, because large amounts of data would be expensive to encrypt and decrypt, researchers usually focus more on the cost of encryption and decryption than anything else [43].

2.5.1 Asymmetric Cryptosystems

The asymmetric cryptosystem uses two keys (private and public) that are mathematically related to each other. The strength of security lies in keys' properties since it is computationally infeasible to calculate one key using the other. Each sender and receiver will have their own key pair in this system. The asymmetric cryptosystem can also provide integrity and authentication [44].

2.5.1.1 Digital Signatures

Digital signatures are mathematical techniques used to authenticate a message, software, or digital document. It's like a handwritten signature or stamp seal, but more secure. It uses asymmetric public key cryptography to verify the origin, identity, and status of electronic documents.

For example, the elliptic curve cryptography (ECC), using two keys (private and public). The signer uses his private key to encrypt the related data, and only the signer's public key can decrypt it [45]. If the recipient can't open the document with the signer's public key, the document is damaged. The hash algorithm is used to generate a hash value, and then the author's private key is used to encrypt this hash.

2.5.2 Symmetric Cryptosystems

The symmetric cryptosystem uses the same key for encryption and decryption, the sender and receiver need to know the key before exchanging messages [46]. For this, the system employs key exchange protocols (like the Diffie-Hellman Protocol) to ensure that the sender and receiver agree on the secret key before starting the communication.

2.5.2.1 Block Cipher

Symmetric key cryptosystems are mainly based on block ciphers, which have a fixed block size. The primary operations of cryptography are confusion and diffusion. The confusion process produces a complicated relationship between a generated key and ciphertext such that every bit in this operation impacts the ciphertext bits' output. On the other hand, the diffusion process circulates the effect of every bit in the state of plain text through several alterations in the form of ciphertext to present a ciphertext robust against statistical attacks. Substitution box (S-box) plays a significant role in confusion operation that satisfies cipher algorithms' data security by mapping a table that translates and converts bits in the encryption process from p-bits to q-bits form and vice versa in the decryption process [47].

2.5.2.2 Stream Cipher

The second form of symmetric cryptography is a stream cipher that processes one bit or byte each time in the encryption and decryption operations. It is considered convenient for constrained devices and requires low computing resources. The operations of such algorithms are concluded in the generation of random keys and produced bits that employ XOR bitwise operations based on the plaintext and random bits. However, some works consider stream ciphers to be less secure than block cipher algorithms [48].

2.5.3 Secure Hash Algorithm SHA-3

The Secure Hash Algorithm 3 (SHA-3) is the standard and newest member of the hash function. SHA-3 is a subset of the broader cryptographic primitive family of Keccak. It is based mainly on the sponge operations, which receive random bits of input and generate a fixed-bit-dimension based on random permutation. It allows inputting ("absorbing" in sponge terminology) any amount of data, and outputting ("squeezing") any amount of data, while acting as a pseudorandom function regarding to all previous inputs. Each round of Keccak-f comprises five logic processes with bit-wise permutations and 24 rounds for every operation.

In contrast, the block size of an entry is 64-bits for the Keccak-f, and each round operation is five × five matrices. The five steps of round process have been defined as "THETA, RHO, PI, CHI, and IOTA". Moreover, some Boolean functions are used, such as bitwise XOR, AND, and NOT [49]. There are some improvements and changes made by researchers to this algorithm to increase speed and security such in [50],[51].

2.5.3.1 The Sponge Construction

The sponge function considers the underlying structure of SHA-3. Figure 2.2 describes the diagram of SHA-3 based on sponge construction. The absolute values r and c in the S(f) represent the block bits of b = r + c, where r denotes the bit-rate and c the capacity of the block state. Firstly, the block states are initialized to the value (zero) and the block bits are padded and then divided a message into sequences of r bits. In contrast, sponge operations are mainly based on two distinct phases, which are the absorbing and the squeezing. The absorbing phase is the process of r input sequence bits, which are XORed with the initial r block bits. In this face, Keccak-f operations are enclosed with each block of the message. After the sequence bits of input strings are all processed and absorbed, functions are completed, and then the shifts to the squeezing process. In the second process of squeezing operation, the initial r bits of the message are generated as a static output of block size, enclosed with operations of Keccak-f, and the result size of the block is selected by the operator. The last c state of the sequence is not directly impacted by the input sequences and is only output after completing the squeezing operations. Moreover, the c value regulates the sponge functions' achievable security states [49],[50].

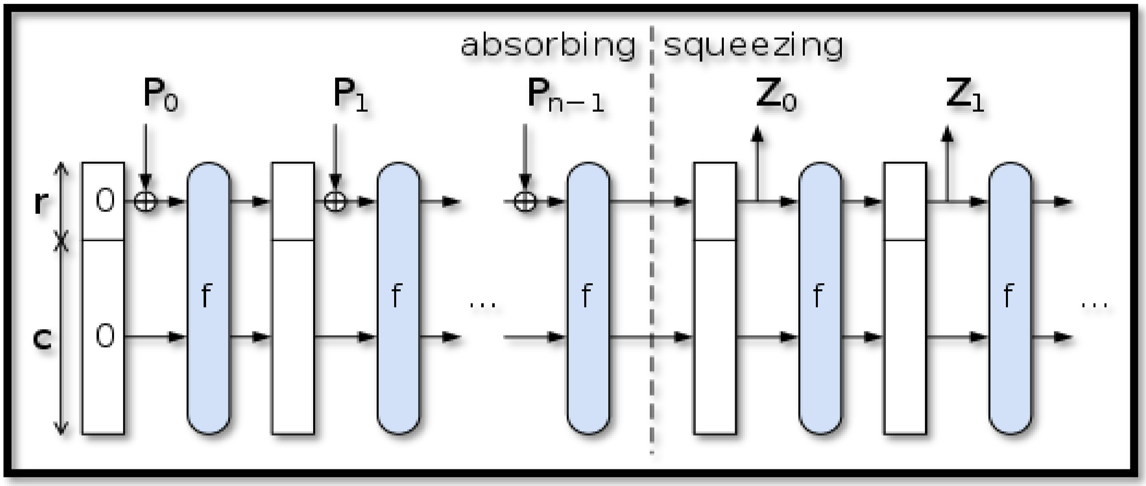


Figure (2.2) Diagram of SHA-3[49]

2.6 Blockchain

Blockchain emerges as a novel distributed digital ledger with consensus of a majority scheme for economic transaction. It already improved economic society lifestyle due to its great impact on commercial and financial and it is influence will continue cause effect in many places. Recently, major implementations across different sectors that includes the education, health care, and supply projects [52]. The digital data that needs to be executed, stored, verified, and continually updated among participating parties with security, privacy, and trust and without a central control authority can be relying on Blockchain. Decentrality helps to get rid security breaches comparison the current model, in which third parties collect and control massive amounts of critical data [53]. The next section will explore blockchain attributes and their effectiveness, as well as their applications and challenges that they encounter during implementation.

The Blockchain innovation was designed by Satoshi Nakamoto in 2008 to fill in as an open exchange record of the digital currency called Bitcoin [54]. Bitcoin was the first cryptocurrency not organized by governments or a single organization [54]. Bitcoin was first known to a few people, but it has incrementally reached hundreds of thousands of transactions every day [55]. At Nov. 2021 Bitcoin exceed value of $68,000 USD per coin, and this increasing attract a big attention. Indeed, the wealth of Bitcoin and currencies do not define the blockchain and the largest strength of the blockchain may be lying beyond cryptocurrencies or even the economy [56]. Until today, cryptocurrency was the most common application of blockchain, used for trade things since it enables a global market of anonymous transactions like money in the real world without any controls from the government.

The advantages of Blockchain technology exceed the regulatory requirements and technical challenges. However, Blockchain technology has been straightforward and precise over the last decade, and it is being effectively applied to both financial and other world applications. The community can face difficulty finding trusted mediators, and that's where blockchain can play a vital role. Blockchain keeps consistent records that can be successively updated but cannot be removed, which builds detectable footprints of each activity proceeding on the blockchain network. As a result, the doubt of alternatives to the truth or facts has decreased [57]. Application states could be visible publicly with cryptographic assurances that the application will be executed as specified by the protocols of the blockchain.

Blockchain may be the most promising technology after the Internet. It is increasingly getting attention from companies and individuals to collaborate, and it is expected to become the new technology of evolution in the economic systems with progressively increased use of the internet to conduct e-commerce and share personal data and life events [58].

One main developing use case of blockchain technology includes "smart contracts". A smart contract is a computer program that can start and execute the terms of a contract automatically. When preconfigured conditions in a smart contract between blockchain network participating parties are met, the network entities involved in that contractual agreement can automatically make payment according to the contract in a transparent way [58]. Blockchain technologies are now applied to an important range of applications, such as financial markets, IoT, supply chains, voting systems, and medical treatments. Certainly, blockchain technology technical questions haven't been fully explored or answered. However, this innovative technology needs combat to overtake the high levels of energy use, security, regulations, and scalability issues [54],[58],[59]. Over time, these issues no doubt will be faced.

2.6.1 The Models of Blockchain

Blockchain technologies consist of a number of techniques and disciplines such as cryptography, mathematics, peer-to-peer networking, and distributed consensus algorithms to solve the synchronization problems of distributed databases [60]. A blockchain is a tamper-resistant database of transactions consistent among large number of network entities. The blockchain technology uses cryptography to be secured against attack and it customizes consensus mechanisms to keep the transaction databases consistent every time a new transaction needs to be confirmed [60],[61].

On a blockchain network, transactions are collected and stored in a chain as blocks. Then the block hash is stored in the next block, and each subsequent block saves the hash of the previous block. That makes a cryptographically secured chain. Any tampering of the block's data will affect the hash of this data, which makes the hash of tampered data not match the original one. Additionally, all subsequent blocks' hashes must be recalculated to be linked again. This is feasible theoretically, but it’s unfeasible since the blocks grow continuously as other nodes add blocks to the chain [62].

At present, there are various types of blockchains that come in public, permission, or private versions, which go beyond the bitcoin blockchain to support different fields with different advantages and features. For example, the Ethereum blockchain allows more functionality to create smart contracts executed on a generic, programmable blockchain under decentralized control. This allows smart contracts and customized rules for ownership, transaction formats, and state transition functions with no need to depend on any reliable third party [63]. Blockchain technology has progressed, as evidenced by the following key elements:

A. Distributed

Blockchain is a peer-to-peer (P2P) network scheme. Although decentralization is enabled by blockchain, nothing in blockchain requires it, and it is based on the requirements of the application. All nodes in the blockchain can create, store, update, and verify incoming data blocks [64],[65].

B. Transparent

The block record/updated by a blockchain node is visible to the entire node in the blockchain. Moreover, every incoming block is verified by all other nodes, which makes the blockchain transparent and more trustable. "Blockchain technologies solve the entity-to-entity trust problem" [64],[65].

C. Autonomy

The blockchain's autonomous nature comes from its consensus property, so every node on the blockchain system can transfer, validate, and update data blocks safely if they are accepted by other nodes. The idea is to make everyone present in the chain a trusted and even untrusted person to become a trusted node, which gains trust for the whole system [64],[65].

D. Immutable

Blockchain records will be preserved forever. Blocks in the blockchain cannot be altered by anyone unless someone has gained 51% all nodes power of. As a result, he can take control and could make blocks inaccurate [64],[65].

E. Anonymity

Blockchain technologies enable transaction without third trust party, moreover transactions can be anonymous, only need to know the blockchain wallet address. Furthermore, most blockchain system is open to everyone, record can be check publicly with keeping member privacy [64],[65].

2.6.2 Blockchain Work Procedures

The procedures of blockchain work are as follows:

1- Whenever any blockchain node sends a new block of data or an update comes into the chain, the consensus algorithm broadcasts that change to the network. The majority is present in the chain to verify the present block.

2- All nodes that receive a new block in the network perform the execution algorithm of proof of work (PoW) or proof of stake (PoS) as it is implemented in the blockchain for that block.

3- If the majority of nodes in the chain approve that the received change is legal, then the present block is added to the chain of blockchain.

4- If the majority of nodes in the chain do not approve the received change (i.e., addition or validation of the block), then that change will be discarded.

5- Distributed consensus algorithm permits blockchain to be distributed ledger. It means that there is no need for a centralized database and all nodes in the blockchain network prove this block and will incessantly extend the chain.

2.6.3 Structure of Blockchain

In general, blockchain contains a tamper resistant database of transactions (sequence of blocks) united through a large number of blockchain network nodes. Every block contains list of transactions records and main data, current block hash, hash of previous block, timestamp and other information. Each block in the blockchain contains the previous block hash and the previous block called the parent block [66]. The first block called genesis block it only contain hash of its block and it does not contain any hash of previous block, so it has no parent block. Figure (2.3) shows the chained blocks structure of Blockchain design with block fields.

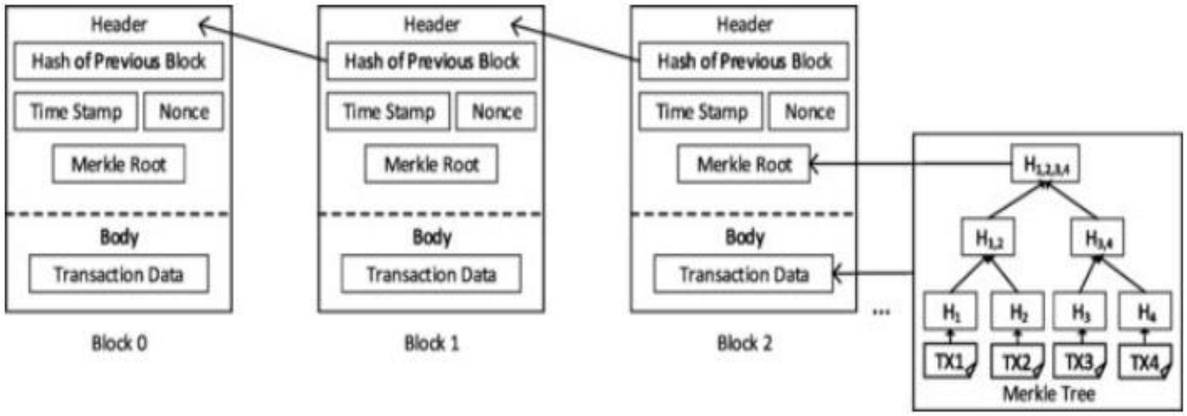


Figure 2.3 General Structure of Blockchain.

Main data. Data is stored in the chain as blocks and the blockchain applicate service defines these data types such as transaction records, bank clearing records, or contract records.

Hash. Transactions of varying lengths must be hashed through a given hashing algorithm, which all give an output that is of a fixed length and then broadcast to all nodes. Since it could be contained thousands of transaction records in block of all node's, Bitcoin blockchain used Merkle tree function to generate a final hash value. This final hash value will be record in block header (hash of current block), and each subsequent block saves the Merkle root of the previous block. Ethereum system stored in a “Patricia tree,” a developing of Merkle tree. Chained hash keeps the blocks well formed, challenging to tamper with, keep the blockchain secure, and almost unbreakable.

Timestamp. Block generation time. This time is specified in milliseconds and when the node receives a new block from the blockchain network, it verifies that the timestamp value of the block does not outpace the UTC time by more than 100 milliseconds. In blockchain and its new concept of consensus mechanism, it is very diverse and challenging on how to hand out the ordering.

Additional information, such as signature of block, nonce values, or other data that user could defined. A blockchain isn’t run from a single server, but on a network of computers that hold all data and changes to the data in the blockchain. These computers are called “miners” essential to a blockchain that uses a proof-of-work mechanism to achieve consensus. Proof-of-work is the most common consensus mechanism, used by both bitcoin and Ethereum [67].

2.6.4 Blockchain Consensus Algorithms

Consensus function is a mechanism to keep the database consistent whenever new transactions need to be validated and that make each blockchain node have an agreement. It can make sure the last block has been added to the chain correctly, guarantee the message stored by node was the same one which can protect from fork and malicious attacks [67],[68].

A. Proof of Work

A proof of work (PoW) mechanism creates a piece of data which is difficult (costly: time, electricity, and computing power) to generated, but easy to confirm by others and satisfies specified requirements [68]. Generating a PoW can be a random process with low probability so that a lot of trial and error is required on average before a valid PoW is produced. The computing PoW data, it's called “mining". All blocks have a random value called “Nonce" in their headers, by exchanging this nonce value, PoW have to generate a value that makes this block header hash value less than a “Difficulty Target" which has already been set up. Difficulty is adjusted by time, and it means how much time it will take when the node calculating hash value less than target value. Because of low probability of successful generate, this makes it unpredictable which worker nodes in the blockchain network will produce the new block [69].

B. Proof of Stake

The PoW mechanism will cause a lot of cost to be wasted, while Proof of Stake (PoS) does not need high computing power. With PoS, the resource are compared to the amount of Bitcoin a miner holds, if someone holding 1% of the Bitcoin, he can mine 1% of the “Proof of Stake blocks" [70]. A PoS method might provide increased protection from a malicious attack on the network [71]. Additional protection comes from two sources:

1) Executing an attack would be much more expensive.

2) Reduced incentives for attack. Attacker would need to own a near majority of all assets. Therefore, the attacker suffers severely from his own attack.

2.6.5 Types of Blockchain

Blockchain network is divided into three types [72], as it shown in figure (2.4).

A. Public blockchains: They are open for the general population, and everyone can check the transaction and verify it, and it can also participate the process of getting consensus [72]. Example of Public Blockchain are Bitcoin and Ethereum both have open-source code.

B. Permissioned blockchains: They control jobs that the nodes can play inside the system and node authority can be choose in advance. Typically, it has partnerships as business to business, the data in blockchain can be open or private, can be seen as partly decentralized [72]. Hyperledger is consortium blockchains.

C. Private blockchain: It in general be littler and don't utilize a token and node will be firmly controlled, not every node can participate this blockchain, has strict authority management on data access [72]. Sometimes we need public blockchain because its convenience, but sometimes we maybe need private control like consortium blockchains or private blockchain, depending on what service to offer.

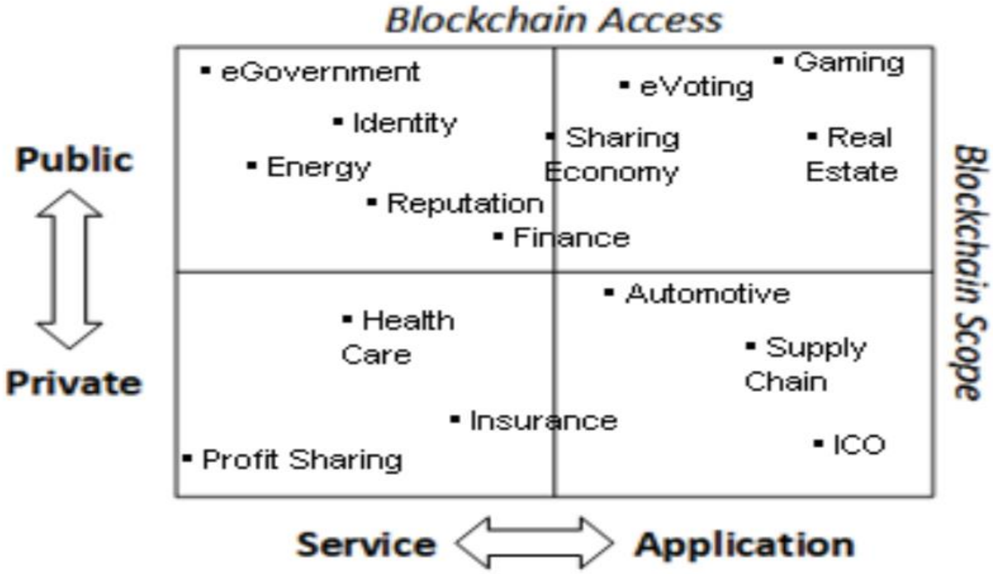


Figure (2.4) Blockchain Technology Types [72].

2.6.6 Blockchain Applications

Till date, Bitcoin is the most used application using blockchain technology [73]. But now days it is applied in almost every field, like finance, agriculture geospatial areas, gaming, telecom industry, and …etc. Blockchain enables any type of digital or digitised asset and associated transaction to be recorded, certified, and tracked between parties, no matter the physical distance. In this trustless network, trust is not connected to a person or a company, but the burden of trust is within the system ‘trust is built in blockchain [74], everyone has the ability to monitor and check the chain for themselves.

A. Cryptocurrency: Bitcoin

Bitcoin is a digital currency which aims to do away with all the problems we have paying for things online. It is the electronic cash which does not depends on any bank. Money is transfer through peer-to-peer network [75]. Bitcoin is extremely fast instead of traditional bank. When we send money to someone, we can’t get it back. This seems that no one can blame that they can’t get their money.

B. Smart Contract

Smart contract, also called distributed apps are very popular. It is tiny program stored in blockchain and it uses distributed ledger to store contracts. It is same as contract in the real world. The difference is that it is digital. A part of smart contract is the smart property, which declare the ownership rights of an asset via registration in blockchain network. Private key is used as a smart property protection from security measures [76]. The only person who has the key can ascertain that the asset belongs to him/her, which can be verified based on the corresponding public key. The private key that corresponds to an property can be handover to the new owner in case the old owner sell the asset. Copyrights, trademarks, patents, and other kinds of properties are inherently smart properties, therefore, managing them is easier as dealing with as encoded and processed as documents in digital form. The fact that the physical asset ownership is more difficult to manage and are not protected from frauds [77]. If anyone needs to register an asset such as a house in the chain of blockchain network, a unique identifiable tag will be assigned to it. The tag information’s is protected from being tampering by preventing any operation that try to be amended these information The implementation of smart properties is one of the colored coins. The colored coin’s goal is to expand bitcoins blockchain capabilities to other assets [77]. This term used for alternative currencies, smart properties, company stock, deterministic contracts etc. Using this term we are talking about a class of methods for representing and managing real world assets on top of the Bitcoin blockchain.

C. Hyperledger

Hyperledger is not a crypto currency, a blockchain, or a company. It is the project under Linux foundation. It is the open-source umbrella project of development blockchains, where individuals and company from all over the world can help in developing Hyperledger and build spatialized blockchain platforms and tools as a software and as a platform to different industry use cases [78]. Hyperledger Fabric is most mature robust and popular open-sourced community of communities of all Hyperledger platforms.

D. Internet of things (IoT)

IoT increasingly grows at a quick rate and devices are becoming qualified more common place to communicate information networks in business, where data such as location temperature or other properties need to be share network parties. A permission blockchain ledger can maintenance a tamper evident records and this opens new ways of automatic business processes among partner without having to set up a costly centralized infrastructure and all participate have access to the same data. IoT permits packets transmitted that carry required status of information to passes through multiple paths. The contract assign the conditions that must be met during the shipment from the manufacture to the retail store and all parties must commit to terms of the contract [79]. For example, temperature sensor embedded in the package stores the temperature of package locally and sends it to the blockchain through the IoT platform that could be explore and shared across all parties. In this example, carriers met the contractual obligation, and the shipment reached its destination place with allowed temperature that recorded using blockchain allows the business partner to observing temperatures trustily and without any third-party control.

E. Supply Chain

Blockchain technology implementation in supply chains is consider new in scientific attentions as first academic scientific papers with this subject published in 2016 [80], and a large growth occurs during year 2017 [81]. The operation in supply chain are very complicated and complex and it involves many details that needs to be shared between involved parties. So, blockchain based systems could ease interactions in global and distributed supply chains between distant and untrusting actors, including producers, retailers, distributors, transporters, suppliers, and consumers. As a result, secured and unique records are shared among all participating partners along the network of supply chain, with the goal of improving operational flows, resource management and route-optimisation planning.

The main important characteristics of blockchain technology that inherent to supply chain implementation are guarantee of secure and automatic verification and execution through smart contracts, trustable exchange of information in real time that could be accessible to all parties [82]. In addition, to ensure that the processed and distributed of a product through parties at a specific date and time, with no chance that anyone could alteration these records. Another important advantages of blockchain implementation in this filed are guarantee product origin as well as tracking product flow path that passes from its place of origin to final consumer, decreasing the time of tracking a product from the source to the final destination from weeks to few seconds [82]. Furthermore, decreasing the direct communications among participants, demand estimate, Ease of paperwork processing, reducing of fraud and fake product risk [83], etc.

Open access to data of origin verification and originality can be a powerful weapon in fighting fraud and counterfeits. Such features have very grate benefits that can be used in many fields especially in luxury jewellery and pharmaceutical industry. The World Health Organization estimates that 50% of the pharmaceutical on online markets are counterfeit medicines [83].

There are many different phases which medicines through pass (raw materials provisions, medicinal foundations, manufacturer, refills, wholesale warehouses, retailers, and finally patients). so blockchain technology is appropriate to this complex supply chain. This is by ensuring that phases of drugs industry visibility and called proper reaction in case of if a problem arises.

Every physical product can be provided with labelling that hold a ‘QR code’ that confirm authenticity and origin which can be tracked through blockchain [84]. QR code can provide access to all truly relevant data about product origin, processing, transportation, temperature, safety, and quality, which all recorded on blockchain. Furthermore, help final consumers to make informed decisions and they could connect to a blockchain-based application, and thus become a member of supply chain with rights to directly express his opinions and needs. Feedbacks from customers could be coming in real time. These solutions give each consumer confidence in the products they want to buy and can also assess the quality and value of products, which eventually contributes to increasing loyalty to the company’s brand.

2.6.7 Blockchain Challenges and Security Issues

There are number of ways to reveal data in centralized systems such as pattern matching. So centralized server is vulnerable for theft of data, as well, blockchain have some challenges and problems that must face them [85]. Blockchain has helped the security of distributed network.

2.6.7.1 Fork Problems

Any software needs constant updates to fix issues or increase performance. In the world of crypto, those updates are called forks. Fork problems are associated to rules of decentralized networks nodes, the agreement when the software upgrade [85]. Therefore, rules are understood and if rules are changed, then fork is done, and blockchain miners needs to agree these new rules. Fork issue is a very imperative because it relating a wide-ranging of blockchains.

There are two types of fork, the Hard Fork and the Soft Fork. Once the new version of blockchain software distributed, updated agreements in consensus rules also improved to the all nodes. In Hard Fork, a adjustment in a blockchain protocol that is incompatible with the previous software versions, nodes that don’t update to the new version won’t be able to push new blocks or process transactions to the chain [85],[86]. As a result, blockchain nodes can take one of four states as follow:

- Updated nodes able to process transaction and approve block that sent by non-updated nodes.
- Updated nodes do not able to process transaction and approve block that sent by non-updated nodes.

- Non-updated node remained able to process transaction and approve block that sent by updated nodes.
- Non-updated node do not able to process transaction and approve block that sent by updated nodes.

Fork happens because of these four diverse situations in takes consensus, and fork type can be known according to these cases. In general, because of open-source nature most blockchain and as more people, groups, and government with differing goals enter to this technology [87], forks will continue to be vital to the development of blockchain technology.

A. Hard Fork

Typically, a hard fork is a radical change to a network's protocol that makes a new version not compatible with previously version. It happened when a group of miners and developers did not agree on introduced updates to the set of consensus rules that is not compatible with the older network [88]. As a result, some nodes continue to operate under the same rules, while another nodes that have computing power stronger are off and generates a new blockchain with an updated software setup. In this process, protocol is usually forked into two incompatible chains that result from the ordinary chain as it shows in figure 2.5.

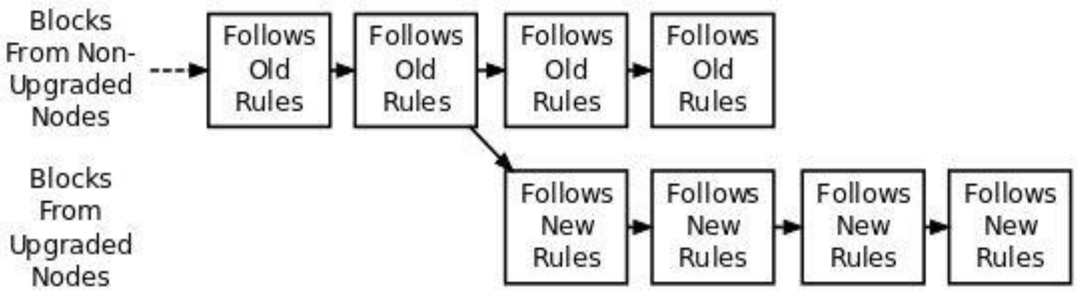


Figure (2.5) A Hard Fork [88].

B. Soft Fork

Soft Fork is an adjustment to the blockchain protocol where still work with older version. Non-updated node will recognize the new blocks and transactions of updated nodes as valid; it means a backward compatible [89]. Non-updated node transactions may be agreed or not by updated nodes, that encourages non-updated nodes to update to the new protocol since they are not as efficient as the updated ones. The outcome updated and non-updated nodes will still work on the original chain [89]. When Soft Fork happens, nodes in blockchain network can gradually and voluntarily upgrade their software to follow the new rules. In this process, we only have original chain, and stability and efficiency of blockchain did not affect when upgrade network nodes

2.6.7.2 The Majority Attack (51% Attacks)

A 51% attack on a blockchain network refers to miners or a group of miners targeting to take control more than 50% of blockchain computing power. As a result of success attack they can control this blockchain [90]. Means these miners has authority to decide which new transaction getting permission to be added or not to chain and they can change the transactions data, it may cause doubles pending attack, halt the block confirming transaction, and interruption miners mining any available blocks. This attack can done because of PoW consensus mechanism that mean probability of mining a block depends on the effort done by the miners. This attack was more feasible when the blockchain computing power was much lower and susceptible to reorganization with the coming on of new mining technologies ASCI miners [91].

2.6.7.3 Blockchain Scale

As the number of transaction increases, the chain of blockchain will growing, the loading of computing and store will also become more difficult. A lot of computing power and time it will be taken to synchronize data, at the same time, chain still continually get bigger and bigger which brings problems to clients when running blockchain [92]. Simplified Payment Verification (SPV) is transactions approve technique that decrease blockchain information storage, which only have to use blocks headers.

2.6.7.4 Time Confirmation Problem

Traditional online credit card transactions generally take a while of two days to confirm transactions, compared with bitcoin transaction take a minimum 60 minutes to approve transfer Bitcoins to a wallet. Two factors affect the transaction time of Bitcoin which are load on Bitcoin’s network (number of transactions that processes in a day), and transaction fee attached to a transaction (fee decides which transaction gets the priority) [93]. It is much better than the traditional, but there is other blockchain transaction take less than 1 minutes (Lightning Network). Lightning Network allows the formation of a network where any peers on the network can make transactions between them even if they do not directly have a channel open between them [94].

2.6.7.5 Regulations Problem

Use Bitcoin for example, the characteristics of decentralized system, will weak the central bank's ability to control the economic policy and the amount of money, that makes government be cautious of blockchain technologies, authorities have to research this new issue, accelerate formulating new policy, otherwise it will have risk on the market [87],[95].

2.6.7.6 Cost Problem

A lot of cost including time and money it will have pay to change current system, particularly when it's an infrastructure [95]. Integrate blockchain technology should not only create economic benefits, but also bridge with conventional organization and also achieve the requirements of supervision that which typically encounter difficulties from internal organization which is existing now.

2.7 Neural Network

The recent advancement in artificial intelligence and machine learning has contributed to the growth of computer vision and image recognition concepts [96]. From controlling a driver-less car to carrying out face detection for a biometric access, image recognition helps in processing and categorizing objects based on trained algorithms.

When it comes to identifying images, humans can clearly recognize and distinguish different features of objects. This is because humans brains have been *trained unconsciously* with the same set of images that has resulted in the development of capabilities to differentiate between things effortlessly.

Contrary to human brains, computer views visuals as *an array of numerical values* and looks for patterns in the digital image, be it a still, video, graphic, or even live, to recognize and distinguish key features of the image.

2.7.1 Deep Neural Network

The way a system interprets an image is completely different from humans. Computer vision uses image processing algorithms to analyze and understand visuals from a single image or a sequence of images. An example of computer vision is identifying pedestrians and vehicles on the road by, categorizing and filtering millions of user-uploaded pictures with accuracy.

Image recognition is the ability of a system or software to identify objects, people, places, and actions in images. It uses machine vision technologies with artificial intelligence and trained algorithms to recognize images through a camera system [96]. Much fueled by the recent advancements in machine learning and an increase in the computational power of the machines, image recognition has taken the world by storm.

2.7.2 Convolutional Neural Networks

In the field of deep learning (DL), the Convolutional neural network (CNN) is the most famous and commonly employed algorithm [97]. The main benefit of CNNs compared to its predecessors is that it automatically identifies the relevant features without any human supervision. CNNs have been extensively applied in a range of different fields, including computer vision, speech processing, Face recognition, etc. The architecture of CNN consists of several layers. Each layer in the CNN architecture, including its function, is described below:

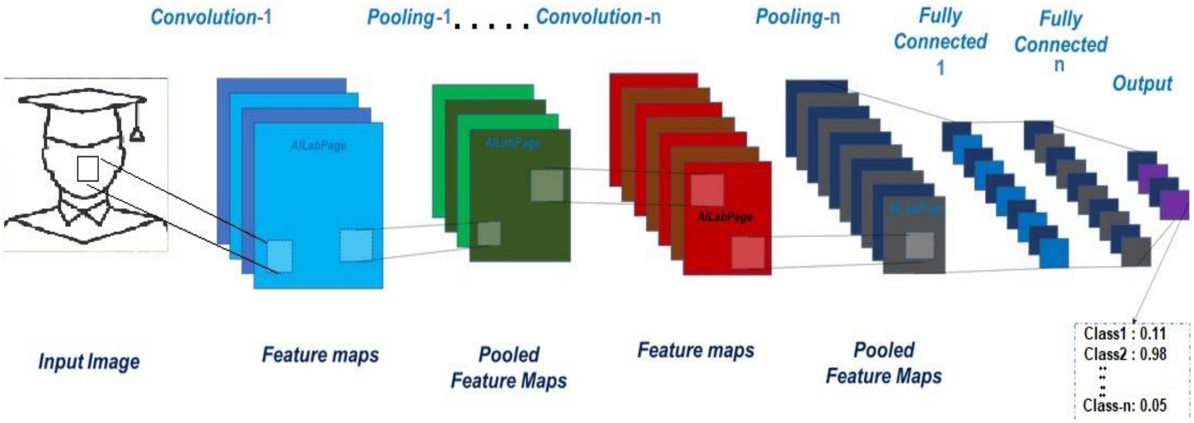
A. Convolutional Layer: Consists of a collection of convolutional filters (it is the most significant component is the convolutional layer so-called kernels). that applied to an input image, and expressed as N-dimensional metrics, is convolved with these filters to generate the output feature map.

B. Pooling Layer: The main task of the pooling layer is the sub-sampling (shrinks large size feature maps to create smaller feature maps) of the feature maps. These maps are generated by following the convolutional operations.

C. Activation Function (non-linearity) Mapping the input to the output is the core function of all types of activation functions in all types of neural networks. The input value is determined by computing the weighted summation of the neuron input along with its bias.

D. Fully Connected Layer: Commonly, this layer is located at the end of each CNN architecture. Inside this layer, each neuron is connected to all neurons of the previous layer, the so-called Fully Connected (FC) approach. It is utilized as the CNN classifier or can used other classifier.

The previous section has presented various layer-types of CNN architecture. In addition, the final classification is achieved from the output layer, which represents the last layer of the CNN architecture. Some loss functions are utilized in the output layer to calculate the predicted error created across the training samples in the CNN model. This error reveals the difference between the actual output and the predicted one. Next, it will be optimized through the CNN learning process [98].



2.8 Cryptanalysis Measuring Methods

The robustness of any cryptographic algorithm can be examined based on randomness and sustainability against different Cryptoanalysis methods. The attackers generally attempt numerous possible methods of Cryptoanalysis to attack the encrypted data. Differential attack (DA) analysis considers one of the major attacks that must examine to test the robustness of cryptography algorithms. DA is numerical measurement based on two vectors and examines changes in the plaintext and ciphertext. Thus, if a small change in plaintext produce a huge differences in the encrypted text will be considered a robustness cryptography against differential attack [99].

Also, DA is usually examine as a chosen plaintext attack (CPA), defining that the attacker should be able to gain ciphertexts for some data of plaintexts [100].There are other methods for measuring cryptoanalysis, and the widest methods applied are based on plaintext or ciphertext.

In recent studies, most attacks are examined based on the known-plaintext attack (KPA) and the CPA. In the KPA approach, the attacker attempts to gain some plaintext and compare the plaintext with the ciphertext to acquire the corresponding key. In recent cryptoanalysis, various cipher algorithms are vulnerable to the KPA [101][102]. Hence, it is not easy to experience the existence of KPA for the proposed algorithms. On the other hand, the CPA approach mainly uses diverse techniques to acquire the matching encrypted data of a selected plaintext [103].

In contrast, to secure the cipher algorithms, different keys must be generated arbitrarily and randomly, sensitive to initial parameters and seeds. Therefore, the proposed cipher algorithms must analyze each value of the data as distinct values and show the sensitivity to the initial parameters. Thus, the proposed algorithms must be resistible and unbreakable against different cipher attacks [103].

2.8.1 Avalanche Effect

One of the main properties that used recently in cryptography is the avalanche effect approach. This approach is linked to a definite model of mathematical procedures implemented for encryption algorithms. Avalanche effect property is considered as a little modification in both the generated key and the plaintext to produce a substantial ciphertext modification [104]. In other words, it measures the result of the ciphertext concerning the slight change made for plaintext or a generated key. In cryptography, this method is a desirable property for block ciphers algorithms, wherein if slightly changed in the input, such as a single bit, the output will be modified significantly. The good cipher algorithm must approach the value 0.5 and above.

Thus, if a crypto algorithm would not show the behavior of avalanche effect to a substantial modification, then a cryptanalyst may have the ability to predict the plaintext or the generated key based on the ciphertext only and chosen-plaintext attack. This can make sufficient to break the algorithm used different attack methods such as cipher attack only [105]. Thus, the avalanche effect property is essential for design a strong cryptographic algorithm against cipher attacks such as cipher attack only and chosen-plaintext attack.

2.8.2 Histogram Analysis

Variances in histogram values can measure the encrypting algorithms that stand to show the difference between plaintext and ciphertext. The histogram represents a function mi that computes the number of observations representing every disjoint category (different values) in the mathematical expression. Therefore, if n considers the total amount of elements and k is the overall number of disjoint categories, the histogram m_i can be computed using the following mathematical equation [106]:

$$n = \sum_{i=1}^{k} m_i . \qquad \text{.... (2.1)}$$

2.8.3 Correlation Coefficient Analysis

Correlation coefficient analysis (CCA) denotes the relation between two vectors, and the result of the defined algorithms always lies between -1 to +1. The values of +1 consider positively correlated, and the values of -1 denote negative correlation. Furthermore, low CCA values indicate robust confusion and diffusion. Different studies used CCA in the cryptosystem to prevent any information seepage concerning the data correlations.

2.8.4 Hamming Distance

Hamming Distance (HD) is used as a metric for comparing two binary vectors of the strings data type. This metric is used an equal length of two binary strings where the number of bits positions are different[109]. HD measures the difference between two strings, plaintext (x) and ciphertext (y), that denoted as d(x, y). HD is calculated between two string vectors with same length with an XOR operation is performed between ($x \oplus y$) and then counted the entire number of 1s in the resulting string vector.

The HD of ciphertext is very significant about the robustness of the cipher algorithm. The ciphertext must show the balance of the number of "1" bits and would be equal to many numbers of "0" bits. Any deviation considers an alignment and makes the attackers capable of decrypting the ciphertext. Here, the larger the HD, the higher is the diffusion [106].

2.8.5 Statistical Randomness Tests Based Cryptosystem

Random number generator (RNG) plays a vital role in various cryptographic applications. Statistical tests are broadly implemented to assess the quality and robustness of the RNG outputs [107]. The NIST tests are considered the most efficient Statistical analysis used to decide whether sets of observations and data on a specific feature are subject to randomness behavior and a certain distribution density. Also, NIST suites are implemented in cryptosystems, particularly in examining the unpredictability and randomness of bits sequences.

The output value of NIST tests named “P-value” ranges among the values (0 and 1) in terms of the random distribution of the binary sequence. Thus, if the P-value is approximate to 1, the binary sequence's robust randomness is considered. The NIST suite compromises 15 experiments, and every test is based on the p-value result gained through a given binary sequence in a specific algorithm using certain statistics functions.

The NIST functions must determine whether the threshold value matches enough the probable statistics observations of binary data [107]. The tests should examine the binary data pass the tests or not, and if data pass, then the algorithm is appropriate for security consideration.

1. Monobit Test

This analysis aims to examine when the number of values ones and zeros in the data sequence is almost equal to the proposed values expected to a random binary data. The analysis measures the closeness of the portion of the numbers (ones) to ½, and the same for the fraction zeros should be about the same for all the values in the binary sequence. Besides, other analyses depend mainly on the result of the frequency analysis.

2. Frequency Experiment Within a Block

The analysis aims to focus on finding when the frequency of numbers (ones) of the length of every sequence (M-bits) of data is around M/2, as should be expected as the assumption of the randomness behavior.

3. Runs Analysis

This experiment examines the entire amount of runs in the data blocks when run considers a continuous sequence of matching block strings. A run is a sequence of measurement k comprised of equal bits constrained with bits of reverse values. Specifically, the run test examines the numbers of zeros and ones when the oscillation changes fast or slow.

4. Longest Run of One's Analysis

This experiment aims to find the longest run of numbers calculated in the M-sequence bits. This analysis determines when the length of the numbers of ones calculated through the data sequence are steady and match the fixed size of the longest run of the numbers expected to the present in random behavior. Thus, if there is an anomaly in the probable size of the longest run of numbers, one indicates an anomaly in the suggested size of the longest run of numbers of zeroes [107].

5. Binary Matrix Rank Analysis

This analysis determines the degree of disconnect sub-matrices of the whole observed data. This experiment focuses on searching for the linear dependence between a specified length of subsequences in the original string. In other words, this test examines how quiet the counted rate of numbers for the several sequence orders that equal to the expected rate of ranks in the expected statement of randomness [107].

6. Discrete Fourier Transform (DFT) Analysis

The DFT analysis aims to find the **repetitive patterns** and appears similar to others in the sequence data under test. This test should show a deviation of the proposed patterns of randomness behavior. Besides, the purpose of this experiment is to check when the number of repetitive patterns exceeding the specific threshold of randomness [107].

7. Non-Overlapping Template Matching Analysis

The experiment aims to see template matching by using a non-overlapping method. The test checks the prespecified existences of non-periodic sequence blocks of bit-string. This test is mainly based on numbers of occurrences within the threshold of the statistical limit of data sequence under the statement of randomness. In other words, the goal of this test is to find various assurance of a specific non-periodic slide pattern in the data sequence. Hence, an *m*-bits pattern is applied to find a specific m-bit sequence that matches with. In contrast, when the specific pattern of m-bits does not occur, the slide moves one-bit position; otherwise, the window slides are reset to the next sequence after a specific pattern and continuous movement [107].

8. Overlapping Template Matching analysis

This experiment examines the number of occurrences of the pre-specified overlapping pattern as the focus target that matches the proposed sequence strings. In other words, the test proposes to search patterns identical in an overlapping manner which checks for existences of a pre-specified sequence of bits and to search if the number of such existences is against a bit-string under the statement of randomness [107].

9. Universal Statistical analysis

This experiment aims to compute the logarithmic (L) distances of sequence bits for each block. This measurement is based on the numbers of bits among sequences that similar to a specific pattern. The L function computes the distances of sequence bits where the sum of L distances among bits of the identical patterns is vital for finding the random distribution. Applying this analysis, the bit string can determine if the data sequence could be meaningfully compressed or unmeaningful; hence, if the meaningfully compressed sequence would produce non-random behavior [107].

10. Linear Complexity Analysis

This analysis examines the gained long sequence from the Linear feedback shift register approach (LFSR). The longer bit string from the LFSR is obtained can be called random; in contrast, the shorter bit string from LFSR is pointed to non-randomness [107].

11. Serial Analysis

This analysis aims to examine the frequency of probable patterns that meeting *m*-bit through the whole sequence. This test determines if the number of existences of the 2^m *m*-bit sequence overlapping to approximately the same as the bits patterns expected for a random statement [107].

12. Approximate Entropy Analysis

This analysis is based on repeating patterns where the larger entropy would mean the high randomness. The entropy test compromises to an n-bit string which is computed by matching the occurrence m -bit string of the interference patterns and finding m+1 sequence patterns. The matching pattern among entropies of m and (m+1) -sequence is called the analysis of approximate entropy[107].

13. Cumulative Sums Analysis

The analysis is based on the highest diversion of a data sequence from values zero to a random movement declared by the total quantity of adjusted (-1, +1) values in the bits string. This measurement aims to examine when the total amount of the partial data values happening in the observed bit strings is highest or lowest relative to the proposed behavior for the total amount of random statement. [107]

14. Random Excursions Analysis

The analysis examines the sum of rounds with the same K visits of bit strings in a total amount of random walk. The total amount of random movement should result from fractional counted sequences after the zero, and one-bit strings are translated to the suitable (-1, 1) values sequence. The round of a random change contains a sequence of random moves taken at the beginning and back to the beginning. This measurement aims to examine where the amount of random visits to a defined state in the round deviates from the one that should suppose for random strings [107].

15. Random Excursions Variant Analysis

The analysis examines the sum number of times when a specific sequence is visited in a total amount of random walks. This measurement aims to find excursions from the probable number of visits to several random movement sequences [10

CHAPTER THREE

Proposed System

3.1 Overview

In this chapter, the structure and implementation of the proposed system (Document Security System based on Blockchain and Convolutional Neural Network). Furthermore, the work stages and algorithms of the proposed system, will be explored.

The proposed model deals with document integrity and authentication where integrity means that the document is not modified by an unauthorized operation, while authentication means the document came from the claimed genuine source. Furthermore, it ensures documents and system availability even when the sources of the documents are down. The proposed system enables remotely verifying of documents' integrity and authentication and detects forgery. Document verification is the process taken to ensure that the documents received from the owner are genuine and that the owner is legitimate. The verification of the Document removes suspicion about the Document content and the issuer institution. Whether the Document issued by the alleged institution, as well as the issuing institution, is authentic. The goals of verification are also to ensure that the document has not been altered by the holder and whether it has been truly issued to the owner. Document verification is a procedure to seek and trace to ensure that the Document is authentic from its source (i.e., the process that establishes the originality of something using the confirmed technique).

As a result, the most concerning issues are storing, transferring, and verifying the documents in a reliable, transparent, fast, and secure manner. In addition, prevent indoor and outdoor intruders from attacking and manipulating them.

The proposed system has been employed a blockchain concept, asymmetric encryption algorithm, and deep learning convolutional neural network (CNN) model to overcome these issues. Depending on a new suggested blockchain model that store a distributed fingerprint for each document according to consensus algorithm in encrypted form, as well as utilized a CNN model which would add more security layers to the system process.

The proposed work presents consensus algorithm that cooperate with a cryptosystem algorithm to add trust and to improve the security, reliability, and transparency. The cipher algorithms are the most convenient approach implementing into the proposed systems to add authentication and to handle indoor and outdoor security issues. The proposed cryptosystem system is used for the encryption/decryption of transfer data and for data authentication by digital signature algorithm, as well as proposed hashing algorithm is used to provide a zero-knowledge proof in share store and verification process.

Moreover, the blockchain consensus algorithm is used as a distributed voting mechanism in document deploying, updating, and verifying processes. Consensus algorithm provides more security, reliability, transparency, and trust to system work and process and shows a clear link between how the documents are collected and how they are delivered.

In addition, in the proposed system deep learning CNN architecture is proposed and implemented as an intelligent method for the recognition and verification of image data in terms of the parts that belong to the document. CNN models are distributed across blockchain network parties and are used in the image verification process. Figure (3.1) presents a block diagram that describes the proposed model.

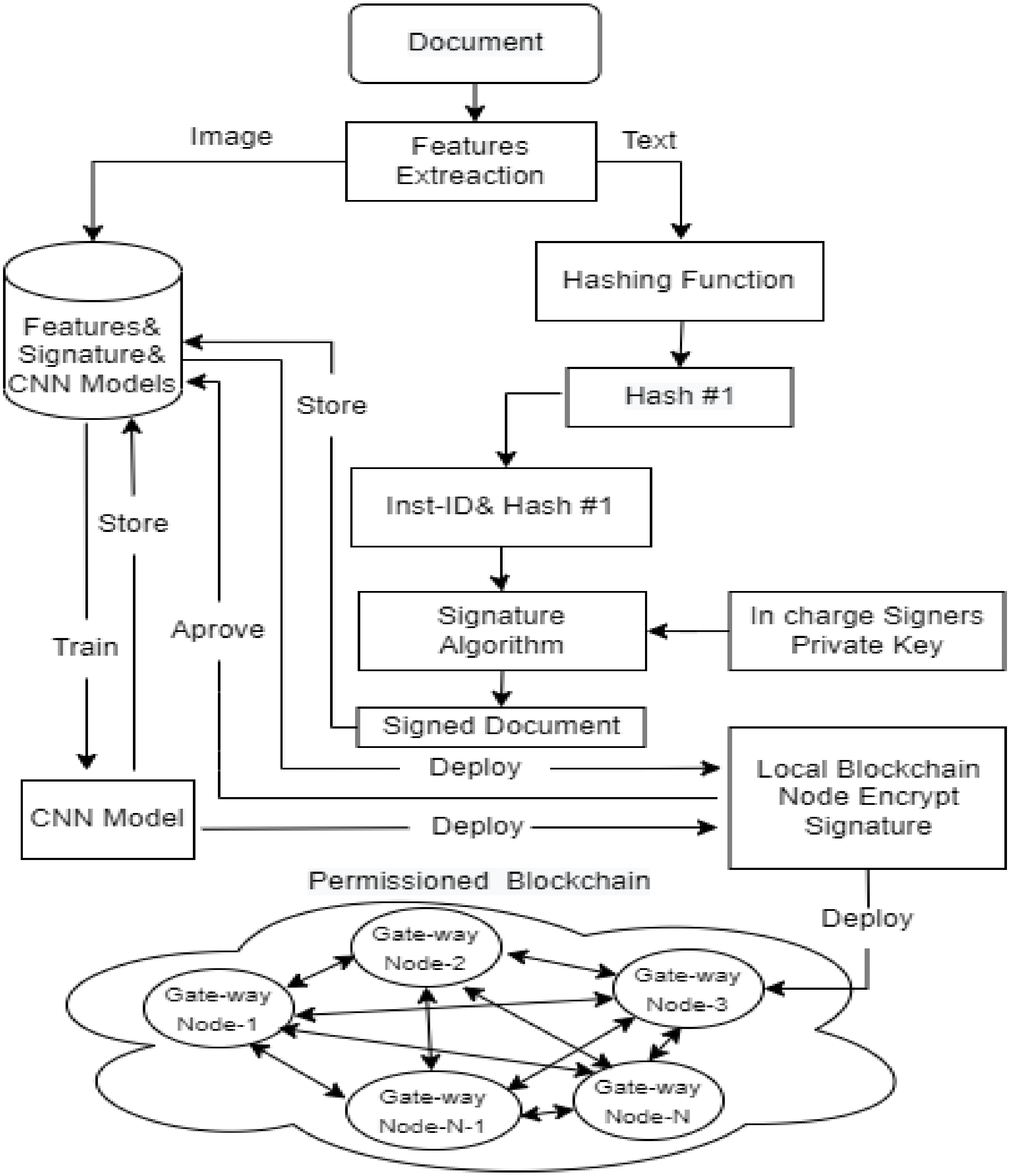


Figure (3.1) Block Diagram of the Proposed Model.

3.2 The Design and Structure of Proposed Model

The proposed system is implemented to ensure the integrity and authentication of document in a reliable, fast, secure, and trust manner. It also allows clients to electronically check a validity of the related document. The proposed model stores the validity of document in a safely electronically compact hashed scheme depending on blockchain concept. Furthermore, it provides availability because of the distributed hash storage and allows any related verifier from anywhere at any time to confirm the validity of the document. This model proposed a permission blockchain distributed system and CNN model to deployed verifications of document. It prevents the process of documents forgeries, as well as to add transparency and trust in the document issuing system by distributed confirming process of the authenticity of the issuance of those documents. So, the blockchain proposed by the model should involve all concerned members. It allows the network parties to add, update and confirm documents through a consensus mechanism.

The outline architecture of the proposed model is clarified by the scheme in figure (3.2), where it shows three main components, which are local agents, global agents, and hashed codes distributed database. Firstly, the local agents are run locally in source of document issuing institutions and they extract important features (usually application specified) from document. In general, the extracted features are classified into two types: text and image. The local agents apply proposed hash algorithm (M-SHA3) to text and then apply the proposed ECDSA algorithm on generated hash code to provide both text integrity and authentication. In addition, the extracted images are collected, grouped, and stored locally then they used to train the proposed CNN models. Local agents (local node) store in theirs database the origin issued signed document, as well as a copy their hash code and trained CNN model.

After the document text gets hashed and signed as well as CNN model gets trained, they will be sent to global agent (Gate-way node) for deploying across blockchain network nodes. The global agent will sent these signed hashes for each documented to master node (Cluster heads) to get consensus approve before they written in global agent node database, as well as global distributed hashed database.

Global distributed hash database consists of all signed hashes related to all generated signed documents from any local agent belong to blockchain contributing institutions. In addition, it contains the hashes of all CNN model structure and weight as well as the hash of consensus algorithm. It is distributed and store in all parties (Gate-way node) of blockchain networks. The data in distributed hash database are added and updated according to consensus algorithm, and its structure and schema does not allow data to be deleted.

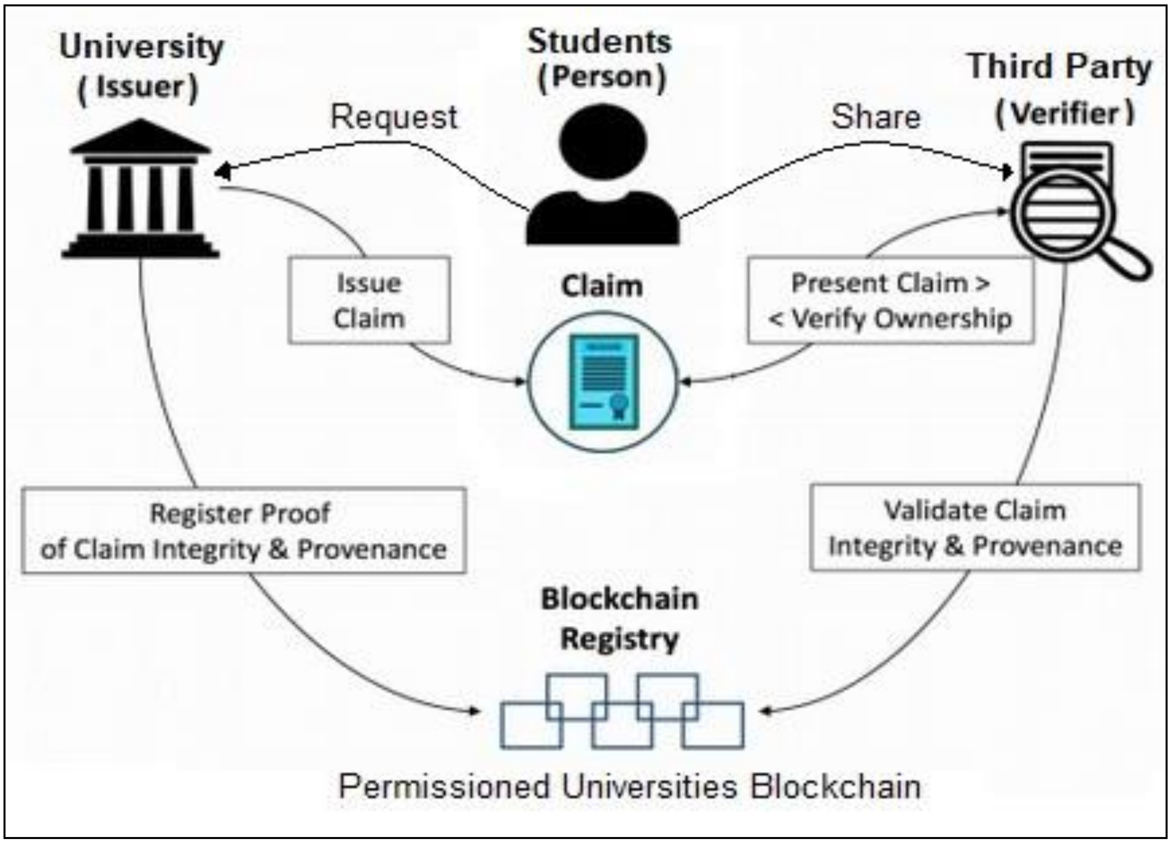


Figure (3.2) The Proposed Model Structure.

3.3 The Components and Stages of Proposed System

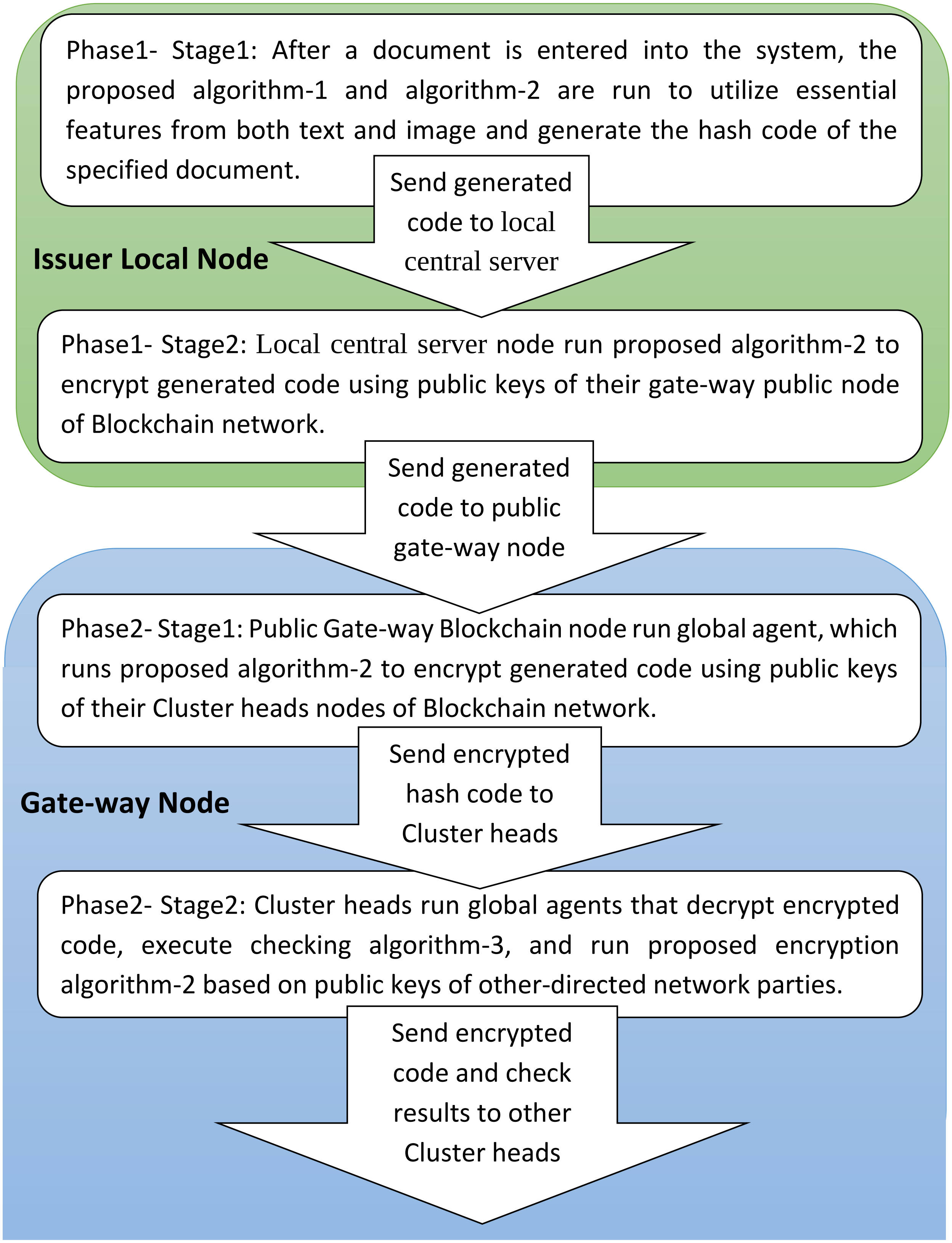
The proposed system consists of three main components which are: first the local agents that locally stored hash database and it is installed and run on the local devices (local nodes). The second component is global agent that deployed on a network server (Gate-way node) with permissioned access. Finally, global distributed hashed database and CNN model that can installed and run on local and global nodes. There is also a client's agent or web portal that used to apply for document or to verify document originality. In general, the work methodology of the proposed system can conceptually divide into three phases, and as follows:

In the first phase (select essential textual features from credentials document and create new checksums), the local agent will utilize important features from credentials textual sections to create new hash code by using textual features as input to M-SHA3 hash functions with digests (hash values) of 256 bits for each Certificate document and encrypt this hash code using private key (create signatures) of in charge persons (Head exam committee, Dean, Register department Chief, Assistant Dean for Scientific Affairs, University President, and University Student Affairs department) as work needs. Then the encrypted hash code (Signed Certificate) sent to local central server. The local central server sends encrypted hash code to global agent (permissioned public gate-way node) to get consensus conformations. Local central server and global agents temporally stored in their hash database the encrypted hash code until it gets proved when agree conformation from other blockchain parties (Universities) is accomplished.

The second phase (get consensus), the global agent that located online encrypt the encrypted hash code (Signed Certificate) using public key of Cluster head node. Then send encrypted hash code to same Cluster head node of Blockchain network. Cluster head node will send the received file to all other cluster heads and will receive the conformation from them and calculate the returned conformation result by execute the proposed consensus algorithm.

The third phase (store hashing code) if the consensus algorithm of Cluster heads get consensus of 51% or greater of agreement will send hashing code and consensus result to server agent that located in student Affairs department in each university as well as to local agent node. Consequently, if it is acceptable verification, store consensus result and temporally hashing code as a valid hashing code in a server node database as well as, in local agent database if it has the original certificate issuer.

The next sections show the block diagram figure (3.3), the knowledge, the specification, and flow diagrams of the proposed system. Figure



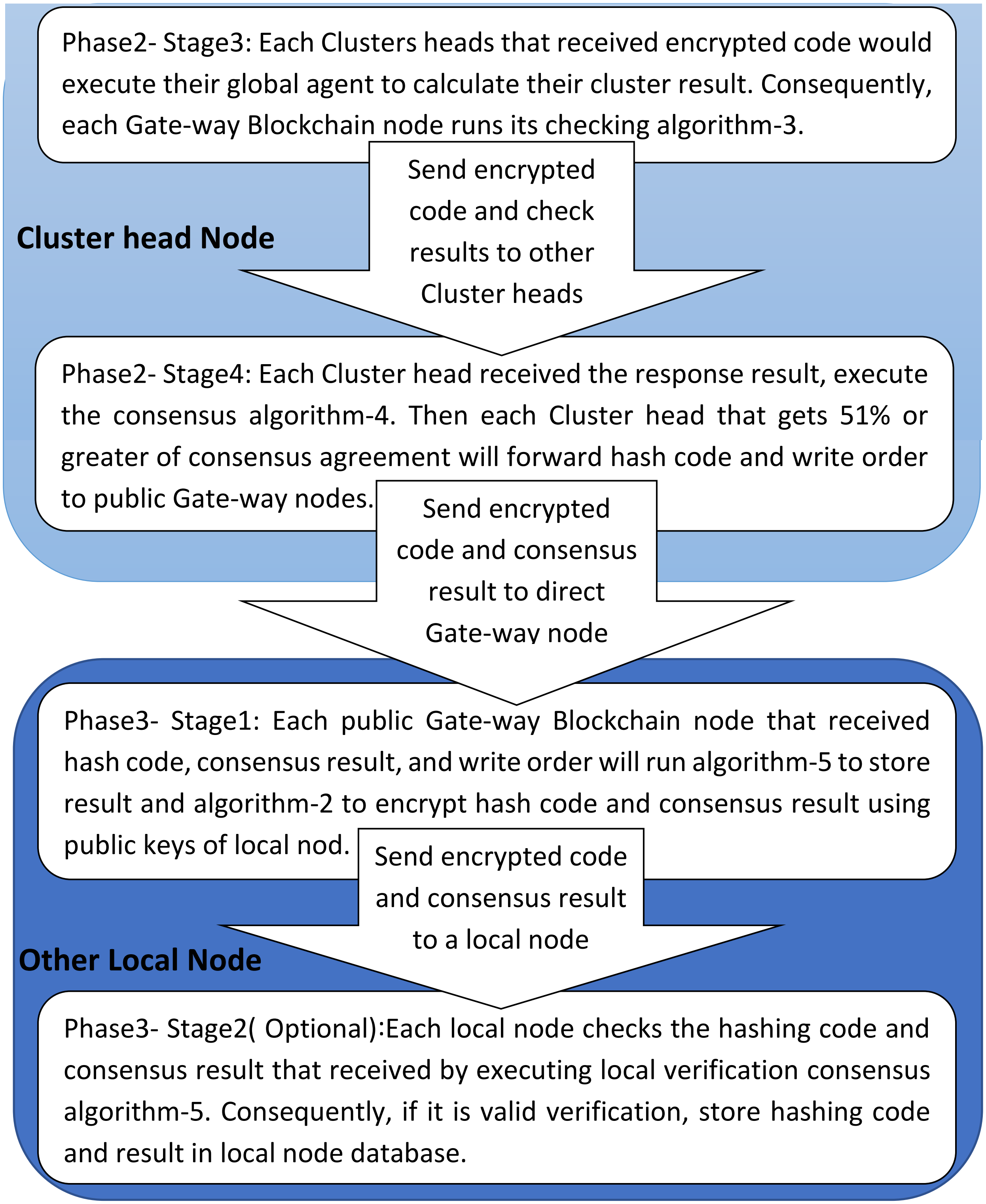
Phase1- Stage1: After a document is entered into the system, the proposed algorithm-1 and algorithm-2 are run to utilize essential features from both text and image and generate the hash code of the specified document.

Phase1- Stage2: Local central server node run proposed algorithm-2 to encrypt generated code using public keys of their gate-way public node of Blockchain network.

Phase2- Stage1: Public Gate-way Blockchain node run global agent, which runs proposed algorithm-2 to encrypt generated code using public keys of their Cluster heads nodes of Blockchain network.

Phase2- Stage2: Cluster heads run global agents that decrypt encrypted code, execute checking algorithm-3, and run proposed encryption algorithm-2 based on public keys of other-directed network parties.

Send encrypted code and check results to other Cluster heads



Phase2- Stage3: Each Clusters heads that received encrypted code would execute their global agent to calculate their cluster result. Consequently, each Gate-way Blockchain node runs its checking algorithm-3.

Send encrypted code and check results to other Cluster heads

Cluster head Node

Phase2- Stage4: Each Cluster head received the response result, execute the consensus algorithm-4. Then each Cluster head that gets 51% or greater of consensus agreement will forward hash code and write order to public Gate-way nodes.

Send encrypted code and consensus result to direct Gate-way node

Phase3- Stage1: Each public Gate-way Blockchain node that received hash code, consensus result, and write order will run algorithm-5 to store result and algorithm-2 to encrypt hash code and consensus result using public keys of local nod.

Send encrypted code and consensus result to a local node

Other Local Node

Phase3- Stage2(Optional):Each local node checks the hashing code and consensus result that received by executing local verification consensus algorithm-5. Consequently, if it is valid verification, store hashing code and result in local node database.

Figure (3.3) General Workflow of Proposed System Block Diagram

3.3.1 Local Agent Structure

The local agent is run on the computer in the registration department in the faculties at the university, and the local agent is responsible for storing and processing grades and verifying their validity with the collection of the required signatures from the specified persons within the college. As well as exporting certificates within the college with uploading an encrypted copy on the blockage to ensure the correctness of the stored and exported information. The local agent is also responsible for creating document requests for graduate students.

The first phase of the proposed model work begins with the process of submitting the graduating student's grades by the department's examination committee to the proposed central system of the university. After completing this process, the system directs these results to the dean of the faculty, the person who in charge, or the person with authority and here there are two cases. The first case is returning the results to the examination committee for modification within the terms and conditions. The second case agrees to approval (consider as a signed) and issue students' grades and certificates. Then each signed students' certificate is hashed by the system and forwarded with the hashes to the college's registration department. As well as the same copy of these certificates is sent to the student affairs department at the university. The output of the hash function is a string of a certain length, which is the hash value. The proposed model extracting the hash value for each student's certificate separately which is considered a verification checksum for each certificate.

After receiving certificates carried out by the approval of the authority holder, these certificates with their hashes are stored in a local database individually by the college’s registration department and the student affairs department at the university. The system sent and deployed only hash values on the universities' blockchain network if the match of hash values occurs between the Student Affairs department compared with the College Register department for the same certificates, and if no match means suspicious altering has occurred in certificates, and a person with authority revisions are required. Algorithm (3.1) list Certificates Issuer steps while figure (3.4) shows the Certificates Issuer Flowchart. The Merkle tree are uses for storage all the data of record and creates a digital fingerprint of the data set, allowing the system to check if it is correct. A Merkle tree is formed by recursively generating a hash for each row that creates a continuum of data connected to some of it through it; This hash is known as Merkle Root. They are generated from below, using transaction identifiers, which are hashes of individual transactions. Each non-leaf node is a hash of its previous hash, and each leaf node is a hash of transaction data which forms a record chain.

Algorithm (3.1) The proposed Certificates Issuer Algorithm

Input: Student degrees

Output: Document with HC#3

Begin:

```
1.  Input student degree by exam committee.
2.  Sign the degree by exam committee and generate Hash Code (HC#1)
    and send it to Dean.
3.  If the Hash Code not match
4.      Alert generation
5.      Go to 1.
6.  Else
7.      If the dean not approve
8.      Go to 1
9.   End if
10. Sign the degree by Dean and generate Hash Code (HC#2) and sent it
    to Head
11. If the hash not match
12.     Alert generation
13.     Go to 1
14. Else
15.     If the Head not approve
16.     Go to 1
17.     Else
18.       Approve the document generate Hash Code (HC#3)
19.       Save the document and HC#3 in register local storage of the department.
20.       Save the document and HC#3 in register local storage of the affriance.
21.       Replicate university permissioned Blockchain.
22.     End if
23. End if
```

End.

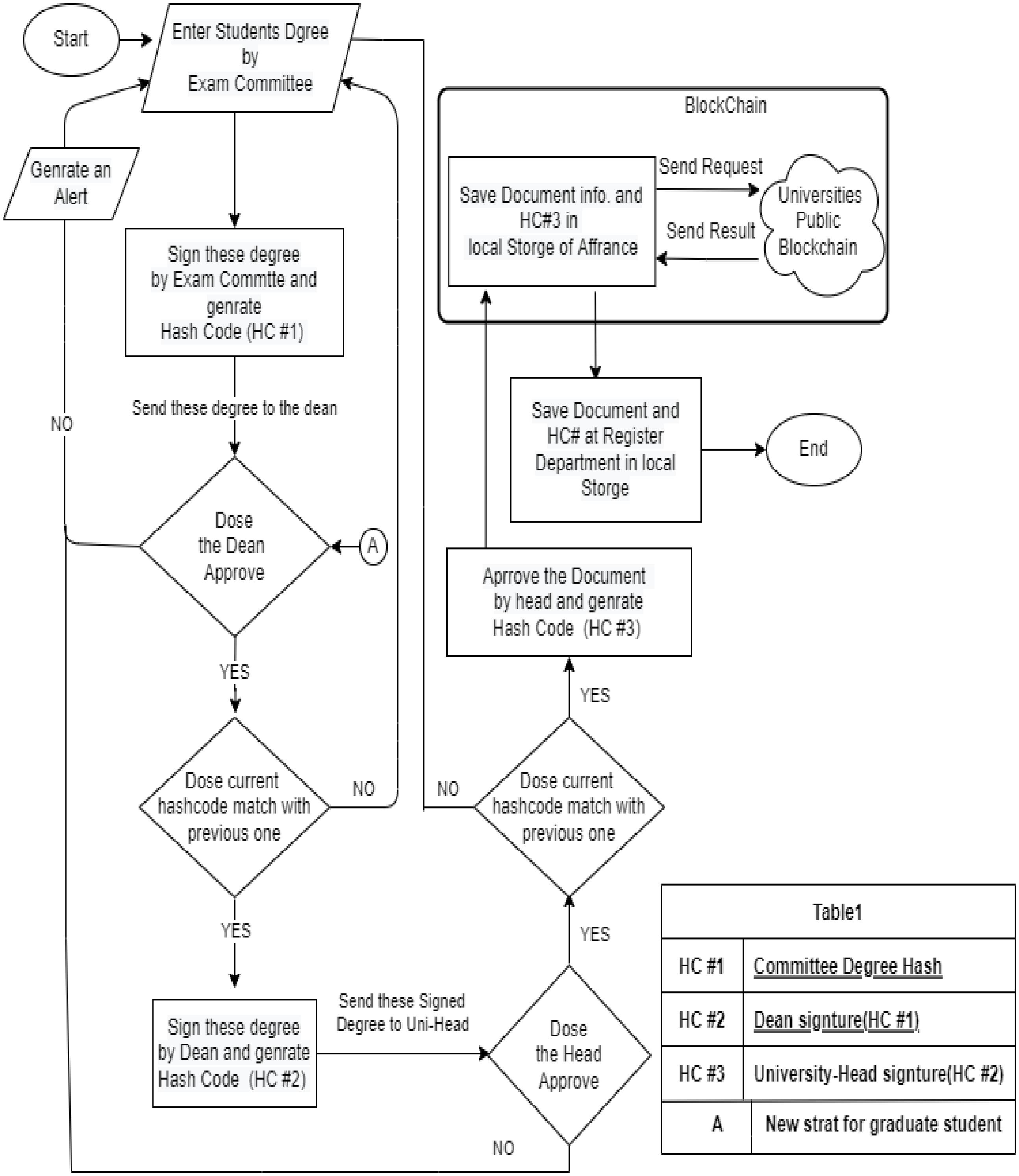

Start
Enter Students Dgree by Exam Committee
Genrate an Alert
NO
Sign these degree by Exam Commtte and genrate Hash Code (HC #1)
Send these degree to the dean
Dose the Dean Approve
A
YES
Dose current hashcode match with previous one
NO
YES
Sign these degree by Dean and genrate Hash Code (HC #2)
Send these Signed Degree to Uni-Head
Dose the Head Approve
NO
YES
Dose current hashcode match with previous one
NO
YES
Aprrove the Document by head and genrate Hash Code (HC #3)
BlockChain
Save Document info. and HC#3 in local Storge of Affrance
Send Request
Send Result
Universities Public Blockchain
Save Document and HC# at Register Department in local Storge
End

Table1	
HC #1	Committee Degree Hash
HC #2	Dean signture(HC #1)
HC #3	University-Head signture(HC #2)
A	New strat for graduate student

Figure (3.4) Certificates Issuer Flowchart.

3.3.2 Global Agent Structure

Each of the most popular blockchain platform, such as Bitcoin, Ethereum, and Hyperledger Fabric, has its own consensus mechanism, algorithm, and implementation. In the mainstream blockchain technology, there are many common consensus algorithms. They differ in terms of computational complexity, fault-tolerance, and resilience. The performance, consistency, scalability, and efficiency of blockchain consensus mechanism need further improvement and optimization. So, a new consensus algorithm has been proposed to commodity the work need. The proposed consensus algorithm depends on voting of blockchain parties and each partners have their weights voting process when new certificate has been published on blockchain network. The weights are calculated quarterly and they depends mainly on the following University factors: **number of current student**, **number of previously published certificate**, **University creating date**, **number of blockchain node**, **computation power of server agent**, **number of cooperation in verification certificates, average period of run time**, **average number of responses time, number of master node, and date of join to blockchain network**, etc. Figure (3.5) shows proposed global agent workflow. The process of selecting the Master node among the individuals of the nodes is carried out using the master's selection algorithm, which depends on several primary factors, some of which were mentioned previously, and the most important thing that is referred to is the penalty factor. The penalty factor is an indicator executed for each node in the cluster and represents the accuracy and validity of these nodes. It is a positive value (node score), if the results given by the node are correct it is increased and it decreases when the results are incorrect. In this algorithm, all the factors are placed in addition to the penalty factor. A total indicator of the point value is made in the network. The assessment is stored on a special table. On the basis of the highest 30% of the points, the first order of points is determined for the new master and the first and second are reserved, randomly from these options In order to maintain the principle of randomness and transparency in the selection process.

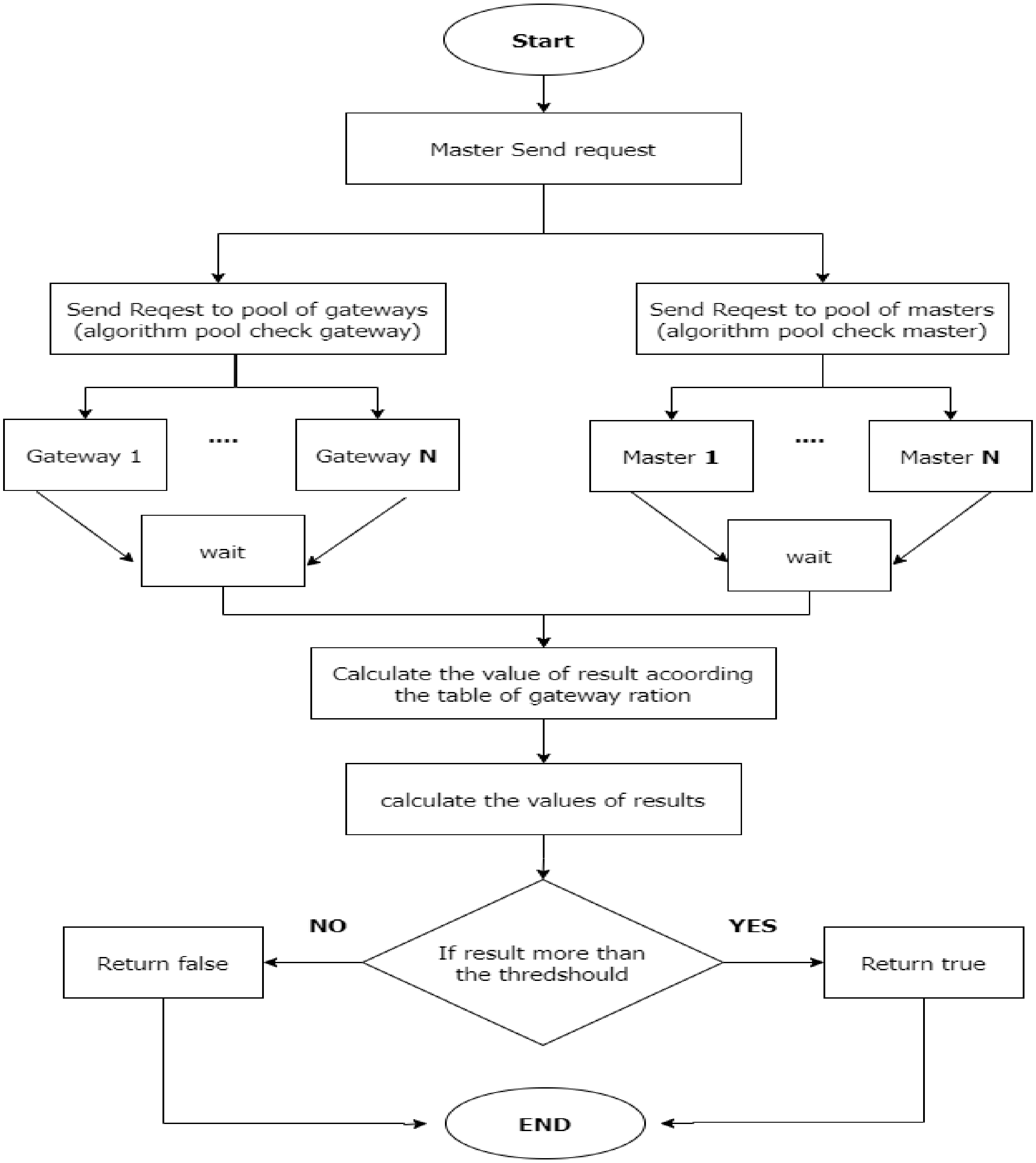

Start
Master Send request
Send Reqest to pool of gateways (algorithm pool check gateway)
Send Reqest to pool of masters (algorithm pool check master)
Gateway 1
....
Gateway N
Master 1
....
Master N
wait
wait
Calculate the value of result acoording the table of gateway ration
calculate the values of results
NO
YES
If result more than the thredshould
Return false
Return true
END

Figure (3.5) Proposed Global Agent Flowchart.

3.3.3 Confirmation Agent Structure

All blockchain network parties except the Certificate generating university cooperate in verification process. The verification process mainly depends on public keys of Certificate issuer to decrypt the encrypted hashed code of Certificate to ensure the originality of Certificate. The Confirmation agent check the previous record of the certificate if match has found this mean the certificate will linked and stored in database, but if there is no match the certificate will store in temporally database to get future conformation or it will not approved. Algorithm (3.2) show proposed Confirmation Algorithm. Figure (3.6) explain the Universities Certificates Confirmation Flowchart

Algorithm (3.2) The Proposed Certificates Confirmation Algorithm

Input : Encrypted Document
Output: Encrypted Verification

```
Begin
    1.  Decrypt certification using published university public key
    2.  If IDs are not match
    3.      Save data in temporary storage with time stamp.
    4.      Go to step 10
    5.  End if
    6.  If facial recognition <90
    7.      Go to step 10
    8.  Else
    9.     If consensus<50
    10.         Encrypt the result using university private key.
    11.         Encrypt the result using website public key and send
    12.         Go to step 17
    13.    Else
    14.         Save and send the hash and consensus result
    15.    End if
    16. End if
    17. Send to university permissioned block chain.
End
```

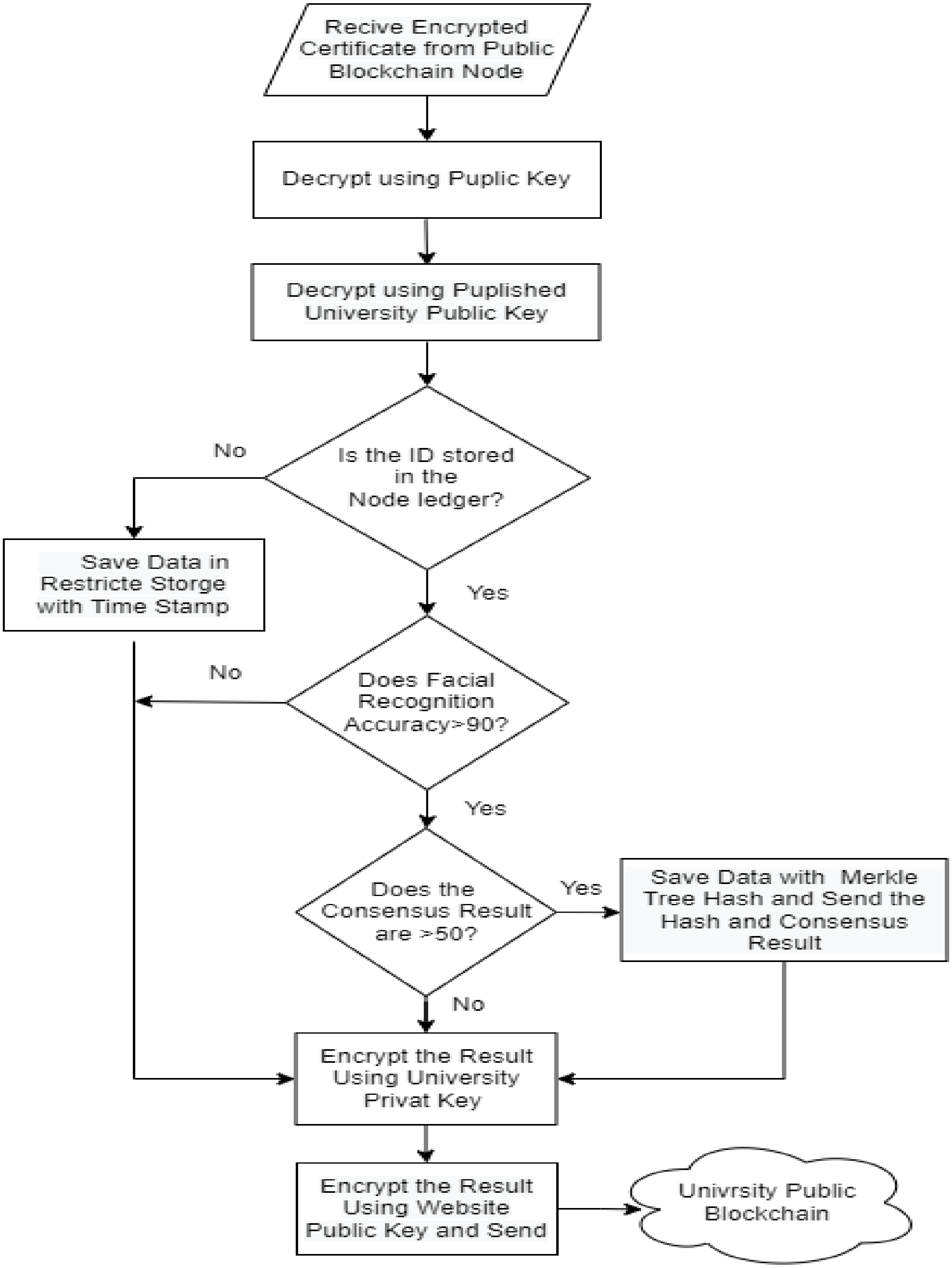

Recive Encrypted Certificate from Public Blockchain Node
Decrypt using Puplic Key
Decrypt using Puplished University Public Key
Is the ID stored in the Node ledger?
No
Save Data in Restricte Storge with Time Stamp
Yes
Does Facial Recognition Accuracy>90?
No
Yes
Does the Consensus Result are >50?
Yes
Save Data with Merkle Tree Hash and Send the Hash and Consensus Result
No
Encrypt the Result Using University Privat Key
Encrypt the Result Using Website Public Key and Send
Univrsity Public Blockchain

Figure (3.6) Universities Certificates Confirmation Flowchart.

3.3.4 Request Agent Structure

The proposed system allows any graduated students from any one of the participating universities in this system to request a graduation certificate from anywhere in the world at any time. It provides a web portal and application (site or mobile) based on the Internet that allows the student to request a certificate to the desired destination according to the rules. In the case of using the web portal, the student should enter important information such as the full name, college, department, and the destination to which the certificate is to be addressed in addition to a valid email address.

The issued certificate is sending to the student's email address. In the case of using the mobile application, it will be an electronic wallet in which the student receives and save all the certificates issued to him. Furthermore, by this wallet, all the details of the student can be identified through a specific serial number or a public key when contacting the system or when requesting the certificate. It also saves all previously issued certificates. Upon receiving the application submitted by the student to get the academic certificate, the system will verify the student’s identity and whether he has the right to apply for the certificate. If the information provided by the student is correct, the system will direct the application to the registration department in the specified college for the required procedure.

The Registration Department performs a first validity check by extracts the student's information and grades stored locally and calculates the hash value for this information and compares it with the hash value stored on the blockchain network to ensure that there is no tampering with locally stored certificate information. Upon completion of the verification of the validation process of the students' information, this information with the destination to

which the certificate is to be addressed that taken as requested from the student shall be submitted as an unsigned student certificate issued to
the Dean’s office for approval (signing).

After obtaining the approval of the dean, the date and number of the certificate issued are given by the system. To deploy the newly created certificate information, it is sent to the Student Affairs Department that performs a second validity check by calculating the hash value of the new certificate's main information and comparing it with the stored hash value in the universities blockchain network. When a match occurs, it means that there is no tampering with the newly created certificate main information and sends a newly created hash value of the new student certificate to the blockchain network to be approved and stored.

After obtaining the approval of the members participating in the network to publish and store the value of the new hash, the process of storing the new hash is performed and a confirmation message sends to the system. Upon completion of the storage process, a copy of the certificate required by the system is sent to the student's electronic wallet or via the electronic email, as mentioned previously. Students can also go to the college’s registration department to receive the hard copy of that attested certificate.

3.3.5 Validation Agent Structure

This phase is considered the practical and actual result of the system, as it represents the benefit of applying the proposed model. Actual works of this phase begin when an institution or a company wanted to verify the validity of the certificates submitted to it to obtain the advertised position. As the proposed system provides a webpage or application that can be accessed from anyone, any time, and anywhere in the world without the need to participate or pay for the system.

The gate could be a web portal, or an application based on the Internet, which enables anyone to verify the correctness of the students' certification instantly. Even when the absence of the institution that granting this certificate for any reason, such as stopping its work or being exposed to any natural or intentional disaster such as fires or floods.

When the graduate student provides his gained higher certificate information to obtain a specific position within a specific company(get hire). Therefore, the company or organization needs to verify the validity of the submitted certificate from the concerned person. In this case, the company employer can verify the validity of the provided certificate in a real, reliable, and safe way through a portal belong to the system. The work of this phase begins when enters only the important information of the certificate which is the name, average grade, date, issue number, agency, or the certificate is uploaded electronically (if the certificate is submitted to the company electronically) through the portal by an employer in the company. The received information of the certificate submit to the portal is entered at the same hash function used when creating and stored the original certificate hash on the blockchain network. Then a query is created to perform a search for a match of the generated hash within universities blockchain network stored hashes. If a match is found means that the certificate information is correct and the validity message will be shown. If there is no match for any reason such as a mistake in the entry process or a process that changes any information from the certificate information (forging the certificate). In this case, there will be no match of the stored hashes on the blockchain network, and the system will be shown a message of failure or error through the portal. Fig.4. show steps to verify the certificate. Algorithm (3.3) list the steps of Certificate Validation algorithm.

Algorithm (3.3) The proposed Certificate Validation Algorithm

```
Input: Certificates Information
Output: Validation Reslut (Vaild or Not Vaild)
Begin
  1. Enter specified information.
  2. Hash information and encrypt using specific public key.
  3. Decrypt and search in public block chain Hashed database.
  4. If hash is found
  5.     Encrypt Hash Code using each university public key
  6.     Decrypt and check the hash and image at each university and send
         the result in encrypted form.
  7.     Receive the result.
  8.     If approve >50% and recognition>90%
  9.         Send the approver to the verifier
  10.    Else
  11.        Send response alert to verifier
  12.    End if
  13. Else
  14.    Send response alert to verifier
End
```

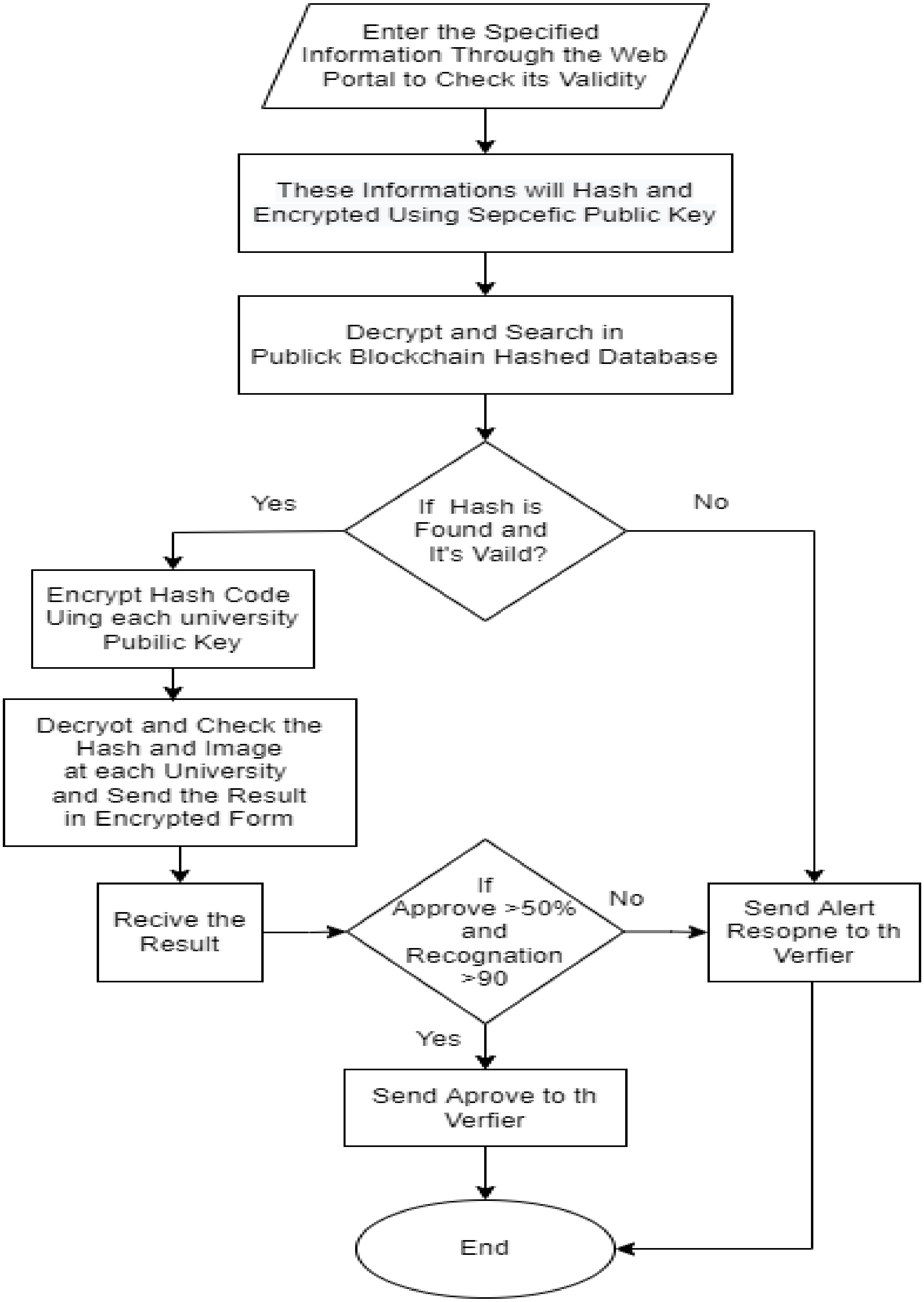

Enter the Specified Information Through the Web Portal to Check its Validity
These Informations will Hash and Encrypted Using Sepcefic Public Key
Decrypt and Search in Publick Blockchain Hashed Database
If Hash is Found and It's Vaild?
Yes
No
Encrypt Hash Code Uing each university Pubilic Key
Decryot and Check the Hash and Image at each University and Send the Result in Encrypted Form
Recive the Result
If Approve >50% and Recognation >90
No
Yes
Send Alert Resopne to th Verfier
Send Aprove to th Verfier
End

Figure (3.7) Certification Validate Flowchart.

3.4 The Proposed Modified Secure Hash Algorithm M-SHA3

The secure hash function was used to obtain a one-way encrypted and compressed copy of the students' certifications, and these hashes are stored on the blockchain after the verification processes by participant's parties are done. As a result of using the proposed techniques above in the proposed model, we prevent the process of issuing a tampered certificate. Furthermore, allowing nonparticipants parties of blockchain networks such as other companies and organizations to verify the originality of certification.

The proposed M-SHA3 algorithm is relying on the chaos keys which is generating by the chaotic system to get more randomness and less time to produce a hash value by reducing the number of random permutations of traditional algorithm from 24 to 12 rounds, and instead use chaos keys as initialize values of (r, c).

The proposed M-SHA3 algorithm passed all NIST tests and shows high randomness and considers efficient to be applied in cryptosystems as it shows in section (4.9). Algorithm (3. 4) shown the proposed M-SHA3-256 Algorithm

Algorithm (3. 4) The proposed M-SHA3-256 Algorithm

```
Input:
M where M is the Plain data
K where K is chaos keys
Output:
Z where Z is hash value-256 bits length
Begin
1.  Pad the input M (P padded bit string) such that m=len(P)/r is an integer.
2.  Break P bit string into r bits chunks to generate m blocks (b1,b2,….bm).
3.  Use the K as the initial value in (r,c) values.
# Absorbing phase
4.  for i=1 to m do
5.      New state (S) = combination of $b_i$ bits XORed r bits with c values to the
        Kecak function (apply permutation 14 rounds to the result).
6.      Divide S into (r,c)  combination.
7.  end for.
# Squeezing phase
8.  Initialize Y to be the empty string.
9.  While the length of is less than 256:
10.     Append the first r bits of S to Y.
11.     Apply Kecak function to S, yielding a new state S
12. end while
13. Z =truncate Y to 256 bits and return hash digest Z.
End.
```

3.5 The Proposed Digital Signatures Algorithm

Digital signatures are a fundamental building block in blockchains; they are primarily used to verify the authenticity of transactions. When users submit transactions, they must prove to every node in the system that they are authorized to generate those assets. Every node in the network will verify the conditions of the submitted transaction.

Elliptic Curve Digital Signature Algorithm (ECDSA) key sizes are relatively short, and it can be easily implemented poorly. Most notably, ECDSA suffered from an implementation in which identifiers for a transaction could be modified by altering the signature of the transaction.

Despite its problems, ECDSA has generally served Bitcoin well over the years. However, ECDSA lacks a key desirable property: there is no efficient way to compress and verify signatures together.

The proposed system design of ECDSA is presented in this section. The improved ECDSA scheme generating the signature using two secret keys, therefore, the verification process will be achieved by the corresponding two public keys. This enhancement will reduce the probability of revealing secrets when random number or/ and public key are reused, as well as use two private keys 1 and 2 for generating different digital signatures on different messages.

These improved algorithms need more computation, however, the security of the improved ECDSA has been improved and the implementation results show that the new design algorithms are reasonably efficient and more secure than conventional algorithms. Algorithm (3.5) shows improved ECDSA parameter generation steps.

Algorithm (3.5) Improved ECDSA parameter generation algorithm

INPUT:

E where E is the EC

P where P is a valid point on the curve

N where n is the EC order.

OUTPUT:

Q1where Q1 is the first public key

Q2 where Q2 is the second public key

d1 where d1 is the first private key

d2 where d2 is the second private key

STEP:

1. Choose an EC defined over F2m . The number of points should be divisible by a large prime *n*.

2. Choose a point $P \in$ E(2) of order *n*.

3. Choose a statistically unpredictable and unique integers 1 and 2 within the interval [1, *n* -1].

4. Calculate 1 = 1*P* and 2 = 2*P*.

A's public key is , , , 1, 2 , A's secret keys are 1 and 2.

3.6. Image Dataset

Images dataset have been collected for real student from 3 collages in Karbala University and more than 10000 students' faces and it has the following properties:

- Controlled condition Dataset.

- Official personal images 2-4 for each student.
- Images have been collected for real student from 16 collages in Karbala University and more than 10000 students' faces.
- Controlled condition Dataset.
- Official personal images 2-4 for each student.

3.7 Image Preprocessing

Dataset have been collected for the students and labeled as classes where the class category has been identical to the student ID. Other image preprocessing will be discussed in this suction such as image resizing, normalization, face detection and dataset augmentation.

3.7.1 Image resizing

Image scaling is a resizing method that comprises rebuilding an image from one pixel grid to another by either raising or lowering the total number of pixels included in an image sample. This process is referred to as image scaling. Using one of the image scaling algorithms, picture resizing uses interpolation to estimate missing values at missing points by interpolating known data (the values at surrounding pixels). As a way to fill in the blanks, this is done in this manner. This method yields better results than the more traditional methods of image scaling. Resizing dimensionality needs to be increased to match the deep learning model's requirements for prediction and to provide generality to the samples. Algorithm (3.6) show same size resizing facial images.

3.7.2 Image Normalization

Each pixel is represented by an integer number that ranges from 0 to 255 and indicates the pixel's intensity. These pixel values make up the information that goes towards creating an image. Neural network models deal with weight values that are fairly modest when it comes to input processing. When huge integer values are utilized as inputs, the learning process can either be severely derailed or considerably retarded. If the pixel values are normally visible, the range of their intensities can be adjusted using the normalization procedure. Instead of the previous range of values, which was between 0 and 2, the new range of possible values for each pixel value is between 0 and 1. By multiplying each pixel's value by 255, which is the pixel's greatest value, the image's pixel values are normalized across all channels. This is done irrespective of the image's actual range of pixel values. This is done on a channel-by-channel basis. During the normalization procedure, a grayscale picture of n dimensions with intensity values that fall within the (Min,Max).

3.7.3 Images Augmentation

For expanding the training set in the used data set some augmentation processes have been applied for each class category. Some of processes used are image shearing, zooming, horizontal flipping, rotation, brightness, width, and height shifting.

Algorithm(3.6) Resizing Facial Images to the Same Size

Input: Segments of different sizes.

Output: Segments of the same size.

Begin:

```
For each segment in image
    Calculate segment width (columns number)
    Calculate segment height (rows number)
End For
W the largest segment width (max(w))
H largest segment height (max(h))
For each segment in image
    Difference of width W – w
    Difference height H – h
    Pad of Width (difference of Width /2) // pad of Width represents the addition to left and rights for resizing small segments.
    Pad Height (difference of Height /2) // pad of Height represents the addition to up and down for resizing small segments
    The New width (first column – pad of width, last column+ pad of width)
    New height (first row – pad of height, last row+ pad of height)
End For
End
```

3.8 The Proposed Convolutional Neural Network

Automatic classification of person images plays an important role in individual recognition, verification, and identification. A CNN is a type of DL model that extends the capability of the feature extraction, pattern recognition, and classification performance of the raw input data without any preprocessing. The CNN architecture is divided into two parts: feature extraction and classification.

A deep learning model generally works well when it has a huge amount of data (more data we have better will be the performance). Furthermore, training algorithm should also include many hyperparameters, which strongly reflect the CNN model's performance. A four deep neural network CNN transfer learning architecture ResNet, Inception, VGGNet-19, and VGGNet-16 to image recognition with of different hyper-parameters and architecture modifications are applied. Figure (3.8) shows general CNN model that used in image classification.

In this study, a transfer learning model based on 16-layer deep model architecture (VGG16) that utilized to extract facial high-level features from our dataset. Then, multiple machine learning models (classifiers) which provided the best classification accuracy among all four CNN models.

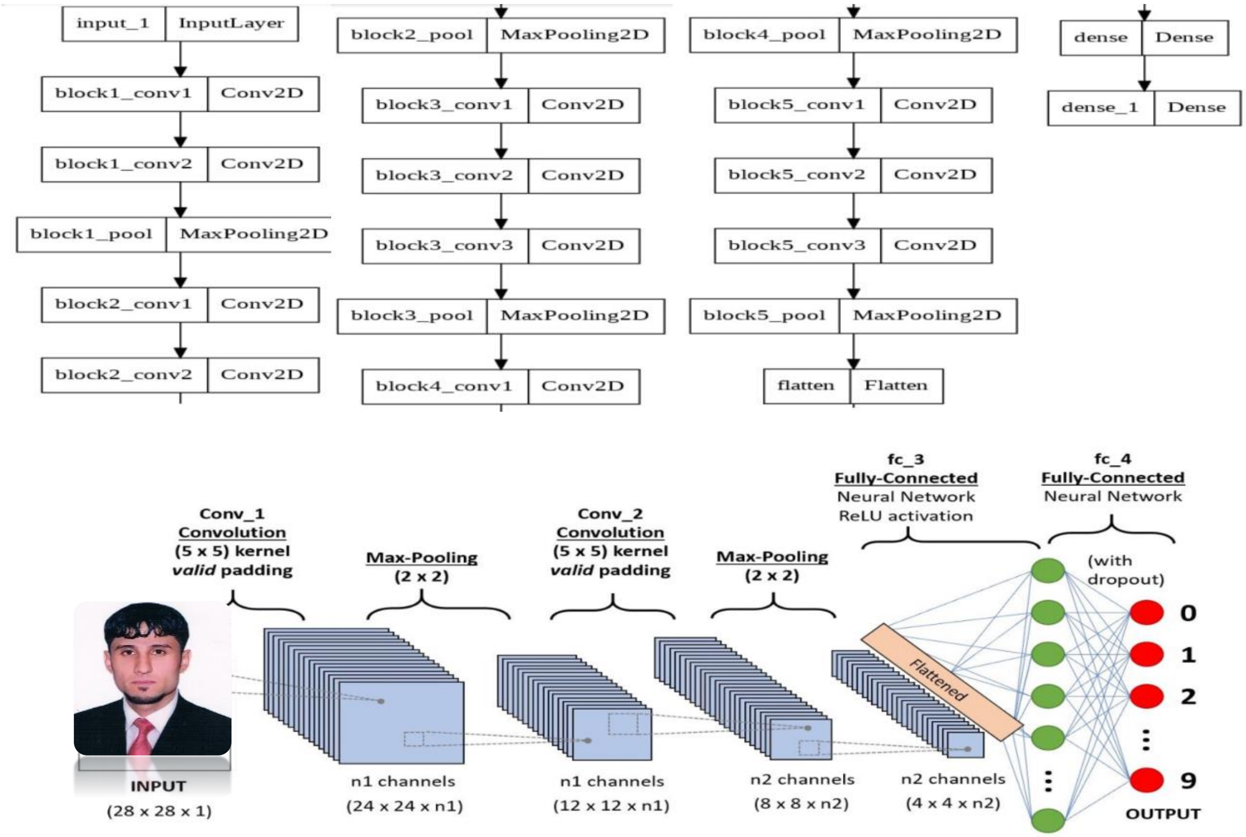


Figure (3.8) General CNN Model used in Image Recognition.

The 3D convolution layer creates feature maps from input samples as a patio-temporal feature extractor. This shows that the convolution layer is identical to the input space local filters and that the filter kernel coefficient is calculated during model training.Algorithm (3.7) CNN Convolution Process

Algorithm (3.7) The CNN Convolution Process.

```
Input: Image.
Output: Image Normalized Feature Map.
Begin:
For i = 1 to no. of filters
    mask Initialization (W) randomly, bias Initialization (B) equal to 1// B is a constant
    For j = 1 to row
        For k = 1 to column
            net=0
            Form v = j-d to j+d // kernel rows and columns. Where d specify size of kernel
                For u= k-d to k+d // d=1 the same value of L*L kernel (W) with size 3*3
                    net = net + [ I(v, u) * W(v, u) + B]
            End v
                End u
            F(net) = Maximum (net, 0) // activation function
            Feature-map[j,k,i] = f(net) // i the obtained feature map with value equal to the filters number, where feature map approximate to distinctive filter
            Normalization of Batch Feature-map [j, k, i].
        End k
    End j
End i
End
```

Pooling and subsampling make features noise- and blur-resistant. The pooling and subsampling layer reduces the feature resolution to achieve this. Algorithm (3.8) The CNN pooling Process.

Algorithm (3.8) The CNN pooling Process.

```
Input:    Feature Map Normalization
Output: Feature Map Down sampled.
Begin
    k1 = 0 // index row initialization of the resulted feature map
    For r = 1 to rows of the feature map normalization
        k2 = 0 // column index initialization of feature map
        For c = 1 to columns of the feature map normalization
            Maximum = normalization of feature-map(r, c)
            For i = r to r+1
                For j = c to c+1
                    If normalization of feature-map(i,j) > Maximum
                        Maximum = normalization of feature-map(i,j)
                End j
            End i
            Down sampled fm[k1, k2] = maximum // the obtained index in the down sampled pooling process has been achieved the feature map.
            k2 = k2 + 1
        End c
        k1 = k1 + 1
    End r
End
```

CHAPTER FOUR

The Experiment Results

4.1 Introduction

This chapter introduces and clarifies the implementation and experiment results that obtained through the proposed model and evaluate the proposed algorithms in Chapter Three. The algorithms analysis and evaluate measurement process described in this chapter have been applied on PC model that has Intel core i5-2430M CPU, 8 GB RAM, and Windows10 64-bits OS. The environment and characteristics of proposed system has been implemented in Dot Net Framework (VB.net and C#), PHP, and Python programming language with Microsoft SQL Server 2019 and MySQL Databases on an ordinary personal computer with the following specifications: Intel core i7-10750H CPU, 16 GB RAM, RTX 2060 6GB Video Graphic, and Windows11 64-bits OS.

4.2 Topology and Configuration of the Proposed Model

The proposed blockchain network is a permissioned network of authorized decentralization nodes. The proposed blockchain nodes can be divided and classify to two types according to their work: master node and worker node as it shows in figure (4.1). The first type which is named worker node represents the Institution gate-way node. The gate-way node (worker node) indicates Institution online node that mirror to Institution local node. Each contain worker node will connected to one master node. In contrast, master node represents head of a region of nodes (cluster of nodes) that connect with other regions master nods. The manner of connection among master nodes functioning on a fully connected peer-to-peer (P2P) network system. While star connection manner is used between master node and their cluster worker node. There is also local node that privately located inside Institution. Every node in a cluster network has a copy of the shared ledger which gets updated timely. They can verify initiated transactions that usually received from local node (create and deploy new hash code) or to verify and written new transactions received from other master node.

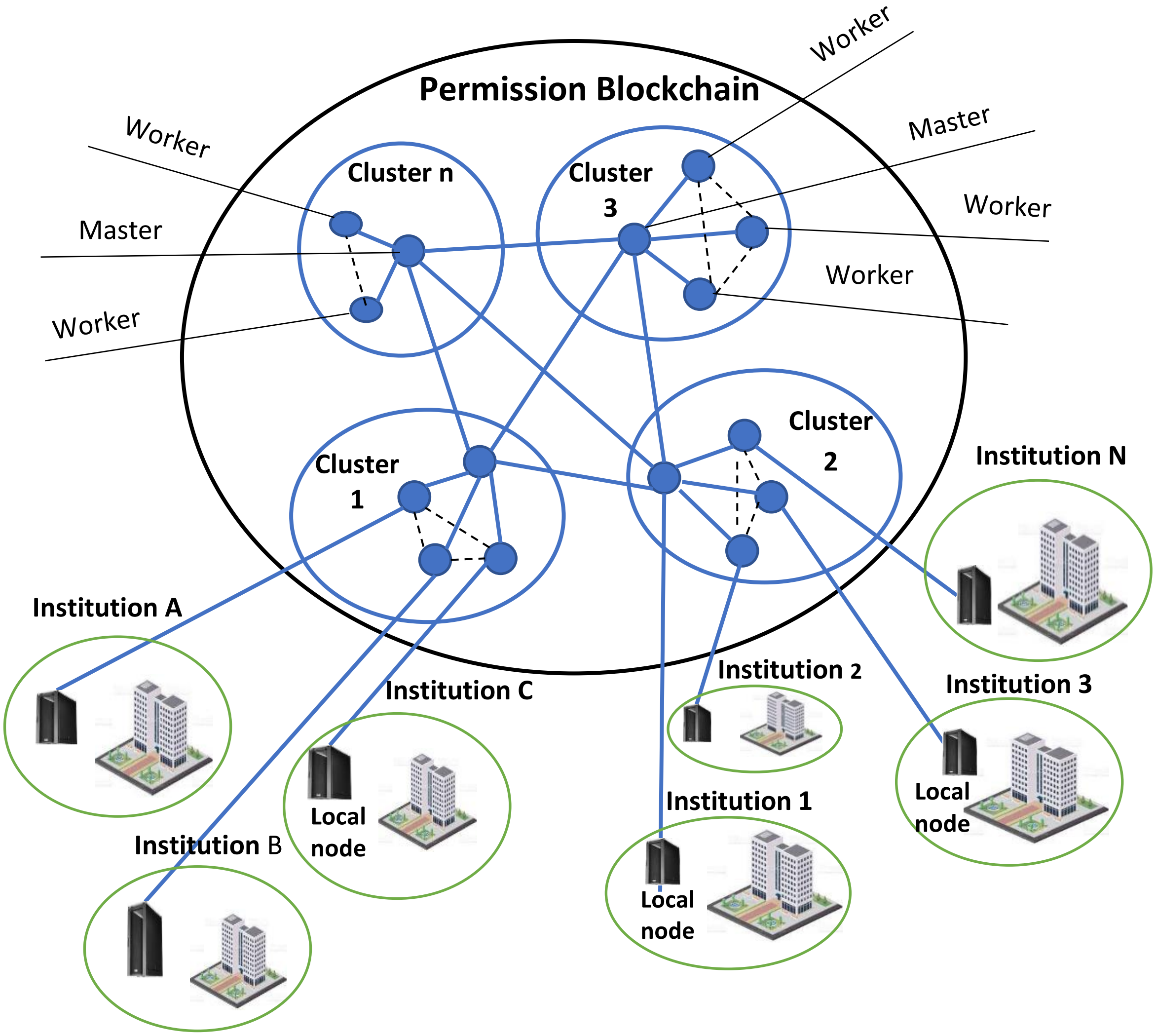


Figure (4.1) Topology of Proposed Model.

4.3 Case study

In this work, the proposed system is considered and applied for a **Higher Education's Certificates (or Transcript of Records)** issuing and verification as a case study to secure the student Certificates from malicious modification and accidents inside and outside the Institutions. The proposed system can be applied to many areas such as Credentials, Land Registration, Intellectual Property Rights, Digital Identity, Supply Chain, and all areas that meet the conditions of section 2.6.5.

The proposed system was applied to creating, issuing, sharing, and verifying for Higher Education Certificates based on blockchain, we use the blockchain to distribute register cryptographically signed digital records with shareable tamper-proof properties. So, the goal is to enable a wave of innovation that dramatically improves Higher Education Certificates fraud protection and gives individuals the capacity to possess and share their own official records. In addition, to enable third parties to certainly and fast verify that a record hasn't been altered since being issued. Once, Certificates are registered (recorded) on the Blockchain they cannot be altered. If someone attempts to create an altered or spoofed Certificate that looks like an original, it won't verify against the Blockchain record.

The main advantage of the proposed model is to ensure the validity of students' certificates in a fast and direct manner. In addition, it allows students to apply for certification electronically. The proposed system stores the validity of certificates in a safely encrypted compact form method depending on blockchain and CNN models. Furthermore, it allows ensuring the validity of students' academic certificates by any interested verifier and from anywhere at any time. This model proposed a permission blockchain distributed system to deployed verifications of students' certificates and transfer learning CNN model to prevent the process of forgery certificates, as well as to add transparency and trust in the creating, issuing, and deploying process.

Figure (4.2) shows workflow of research proposed model. A high-level overview of component and workflow steps of the proposed system will describe and illustrate. The permission blockchain proposed by the model involved in all student affairs departments belongs to Universities of the Ministry of Higher Education. It allows the network participating to add, update, and confirm the student's credential by a consensus mechanism.

The proposed system includes three main phases, which are issuing, demanding and creation, and verifying the validity of the certifications. Each one of these phases will be explained in the following sections.

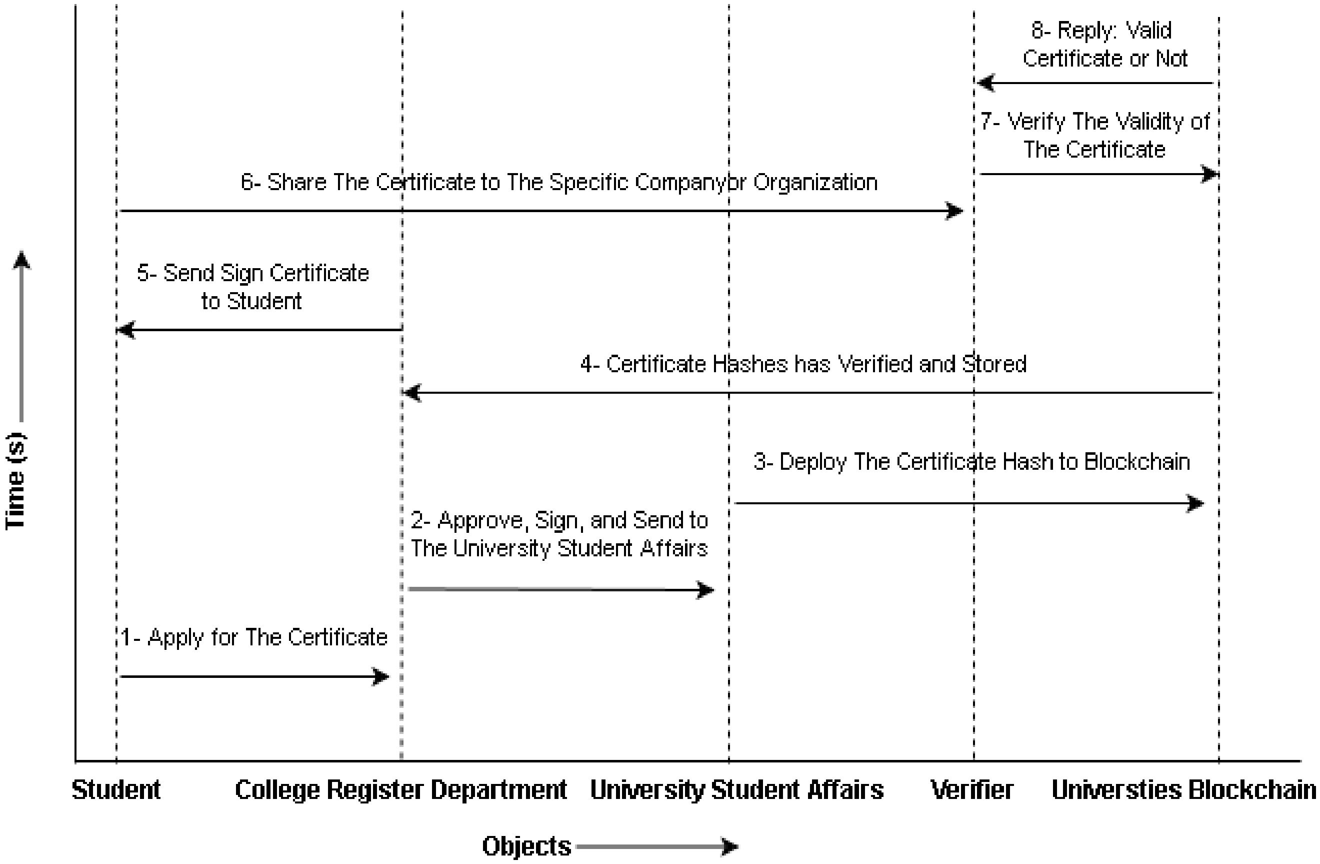

8- Reply: Valid Certificate or Not
7- Verify The Validity of The Certificate
6- Share The Certificate to The Specific Company or Organization
5- Send Sign Certificate to Student
4- Certificate Hashes has Verified and Stored
3- Deploy The Certificate Hash to Blockchain
2- Approve, Sign, and Send to The University Student Affairs
1- Apply for The Certificate
Time (s)
Student
College Register Department
University Student Affairs
Verifier
Universties Blockchain
Objects

Figure (4.2) The Proposed System Workflow.

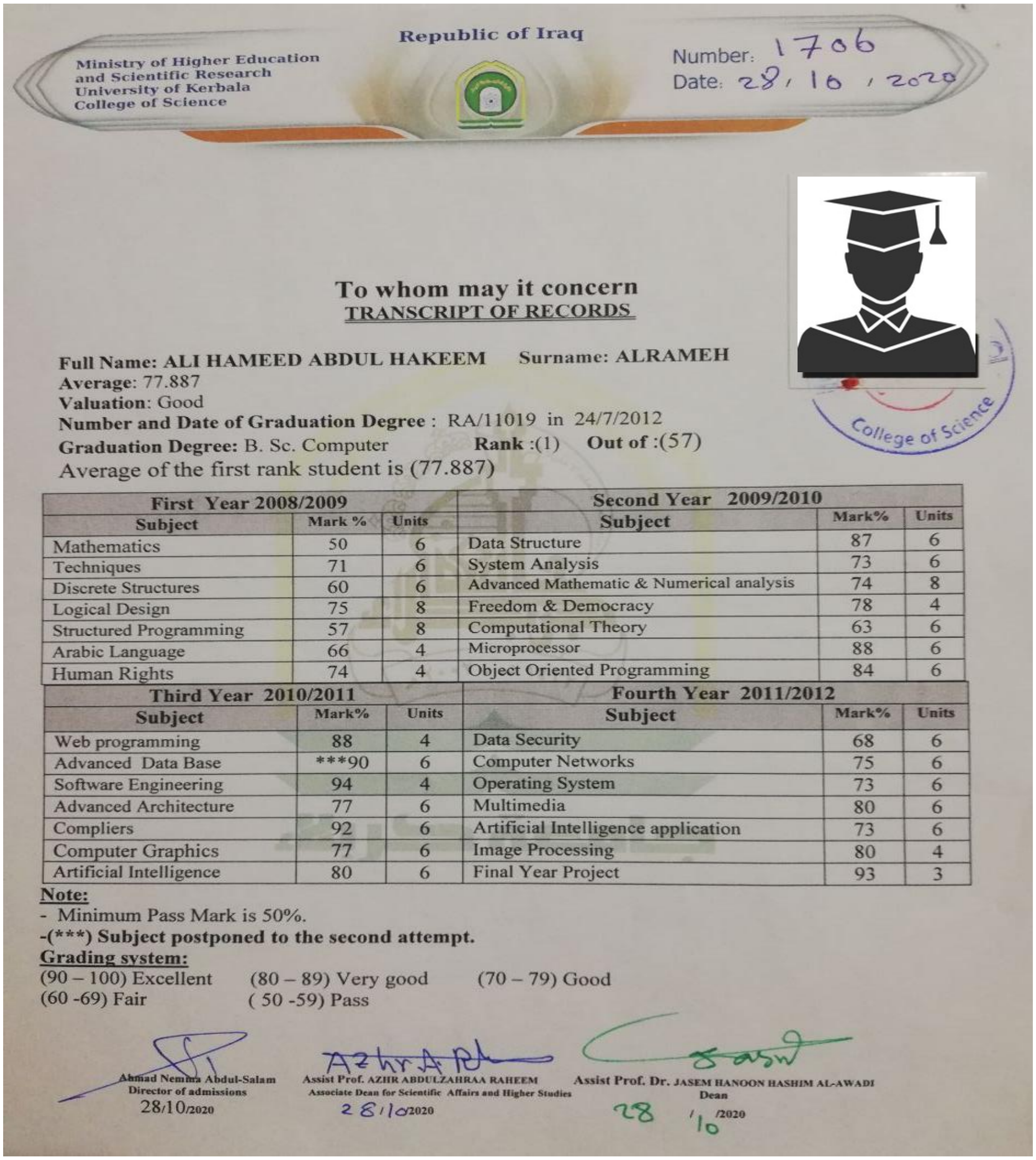
4.4 Data Collection

To validate the proposed system, a real-world Higher Education’s Certificates dataset has been collected; The data is collected from the Colleges of the University of Kerbala. The dataset consists of 10,000 students' certificates and each one of these certificates contain both texts and image. The important and required text fields are extracted and listed in the table (4.1).

Table 4.1: The Important Fields of Student Certificates Dataset.

No.	Data fields	Description
1	University Name	Name of higher education institution having authority to award academic degrees for students.
2	College Name	Name of a constituent part of an educational institution.
3	Student Full Name	Student's First and Last Name.
4	Student Identifier	A unique number associated with student’s academic record
5	Average	Average grade throughout the academic degree study.
6	Rank/ Out of	Academic achievements measure up to classmates.
7	Study Time	Time of study (morning or evening)
8	University Type	Public or Private University
9	Average of the First Rank Student	The average of the first student in the class
10	Graduation Degree	Generally, fall into four categories: associate, bachelor's, master's, and doctoral for a specific discipline.
11	Number and Date of Graduation Degree	Generally, the university order (number and date) to grant the student the completion of degree
12	Issuing Number	A number assigned to each certificate
13	Issuing Date	Date of issuing the certificate

Consequently, the student certificates consider the most important among the document types and the repeatedly required for hired and job qualification requirements. Figure (4.3) shows Higher Education's Transcript of records (Certificate) of student.



Republic of Iraq

Ministry of Higher Education
and Scientific Research
University of Kerbala
College of Science

Number: 1706
Date: 28/10/2020

College of Science

To whom may it concern
TRANSCRIPT OF RECORDS

Full Name: ALI HAMEED ABDUL HAKEEM **Surname: ALRAMEH**
Average: 77.887
Valuation: Good
Number and Date of Graduation Degree : RA/11019 in 24/7/2012
Graduation Degree: B. Sc. Computer **Rank** :(1) **Out of** :(57)
Average of the first rank student is (77.887)

First Year 2008/2009			Second Year 2009/2010		
Subject	**Mark %**	**Units**	**Subject**	**Mark%**	**Units**
Mathematics	50	6	Data Structure	87	6
Techniques	71	6	System Analysis	73	6
Discrete Structures	60	6	Advanced Mathematic & Numerical analysis	74	8
Logical Design	75	8	Freedom & Democracy	78	4
Structured Programming	57	8	Computational Theory	63	6
Arabic Language	66	4	Microprocessor	88	6
Human Rights	74	4	Object Oriented Programming	84	6

Third Year 2010/2011			Fourth Year 2011/2012		
Subject	**Mark%**	**Units**	**Subject**	**Mark%**	**Units**
Web programming	88	4	Data Security	68	6
Advanced Data Base	***90	6	Computer Networks	75	6
Software Engineering	94	4	Operating System	73	6
Advanced Architecture	77	6	Multimedia	80	6
Compliers	92	6	Artificial Intelligence application	73	6
Computer Graphics	77	6	Image Processing	80	4
Artificial Intelligence	80	6	Final Year Project	93	3

Note:
- Minimum Pass Mark is 50%.
-(***) **Subject postponed to the second attempt.**

Grading system:
(90 – 100) Excellent (80 – 89) Very good (70 – 79) Good
(60 -69) Fair (50 -59) Pass

Ahmad Nemma Abdul-Salam
Director of admissions
28/10/2020

AzhrA
Assist Prof. AZHR ABDULZAHRAA RAHEEM
Associate Dean for Scientific Affairs and Higher Studies
28/10/2020

Assist Prof. Dr. JASEM HANOON HASHIM AL-AWADI
Dean
28/10/2020

Figure (4.3) Example of Student Higher Education's Transcript of Records.

For face recognition, student faces dataset was collected and prepared using a manual approach that checks and cleans a huge amount of images data to get good dataset face recognition and face verification. The dataset contains a set of face images taken in March 2021 in the Kerbala campus. There are one to three different images of each of 10000 distinct subjects, and the size of the dataset is 2.41GB. Subject ages range from 18 to 49 with a median age of 22 years. All the images were taken against a bright homogeneous background with the subjects in an upright, frontal position. The files are in JPEG and BMP format. The images have different (Height * Width) pixels. The images are organized in two main directories - males and females. In each of these directories, there are directories with unique identifier as a serial number, each corresponding to a single individual. Additional information and associated metadata about the image's datasets are listed in table (4.2).

Table 4.2: Images Students' Faces Dataset.

No.	Data fields	Description
1	Name	University Students' Face Dataset
2	Color Images	Yes
3	Image Size	Different Size
4	Number of unique people	10000; 4700 Male, 5300 Female
5	Number of Image per person	Ranges from 1 to around 3
6	Total Images Number	There is a total of 16000 images in the database
7	Conditions	All frontal views, Slight tilt of the head, Neutral expression, No wearing any objects.
8	Are Images Available Outside the Institution	No
9	Available for Public	No

4.5 The Experimented Data

The experimented data are divides into two type numerous face datasets available, some of them are under controlled conditions and others are under uncontrolled conditions. The used datasets used for face recognition are consists of face images under different kinds of controlled conditions. The existence faces are with natural expression, different light conditions, no wearing sunglasses or scarf. The images are of different size with .jpeg and .bmp format that converted into .jpeg format using Image Magick tools.

4.6 Dataset Preprocessing

Image Augmentation artificially creates training images (expand the size of a training dataset) through different ways of processing, such as random rotation, shifts, shear, and flips, etc.

- Image shearing

- Image zooming

- Image horizontal flipping

- Image rotation

- Image brightness

- Image rotation: the rotation range [0-25]

- Image width shifting

- Image height shifting

Table 4.3: Augmented Images Students' Faces Dataset.

No.	Data fields	Description
1	Name	University Students' Face Database
2	Color Images	Yes
3	Image Size	240 x 240
4	Number of unique people	10000; 4700 Male, 5300 Female
5	Number of Image per person	Ranges from 12 to around 36
6	Total Images Number	There is a total of 222000 images in the database
7	Conditions	All frontal views, Slight tilt of the head, Neutral expression, Rotation 0-to-20-degree, No wearing any objects.
8	Are Images Available Outside the Institution	No
9	Available for Public	No

Splitting Dataset to Training and Testing

The training data is the general term for the samples used to create the model, while the test or validation data is used to qualify performance. Figure (4.1) shows splitting data into training and testing sets. This process it presented in the following points.

- Training data. This type of data builds up the machine learning algorithm.
- Validation data. During training, validation data infuses new data into the model that it hasn’t evaluated before.
- Test data. After the model is built, testing data once again validates that it can make accurate predictions.

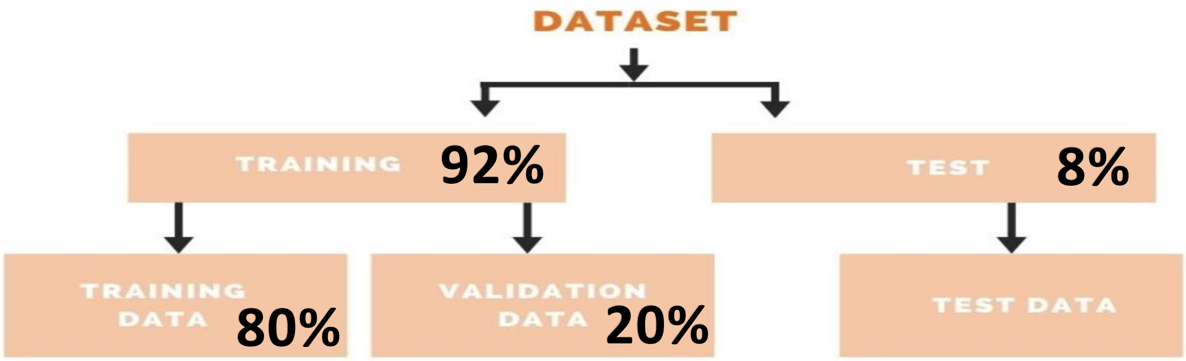


Figure (4.4) Divided Dataset to Training and Testing.

4.7 Case study

This study proposed a Document integrity and authentication model based on blockchain technology that is prevent Documents forgery and detect any type of modification on these documents such as higher students' certificates inside an important facility such as a university. In addition, provide compact verification codes for these certificates in distributed storge manner. These verification codes store inside local node as well as outside node. Each node (inside and outside) has the same structure and same data in encrypted compact form.

To understand the expected outputs from applying this model to the certificates system, it must be compared with the current systems of issuer the paper and electronic certificates. Moreover, explain the problems and weakness to solve or enhance them using blockchain technology. This section describes the most important problems in the current systems.

Certifications acquired over a long period from different accredited educational institutions throughout the country or the world, need to be approved for their originality. The verified process is becoming more difficult and takes long periods due to the increase in the number of universities, colleges, courses, and students. Educational institutions spend a lot of time, effort, and resources in creating academic certificates for students as well as verifying transcripts and data starting from their date's births, records of accomplishment, and capabilities.

The trust, security, transparency, and speed along with automation through digitization are offered by blockchain technology that comes as leverage to the education industry across the world. The results of adopting the proposed model are summarized below:

1- Easy Verification Mechanism and Accurate Information: A portal can be used by the third-party who want to verify the certificate.

2- Convenient**:** The students need to no longer provide many papers with proof of their originality each time they use to apply for a job.

3- Cost-effective: The digitization of the process of the creation and validation of the certificates reduces the costs for all parties.

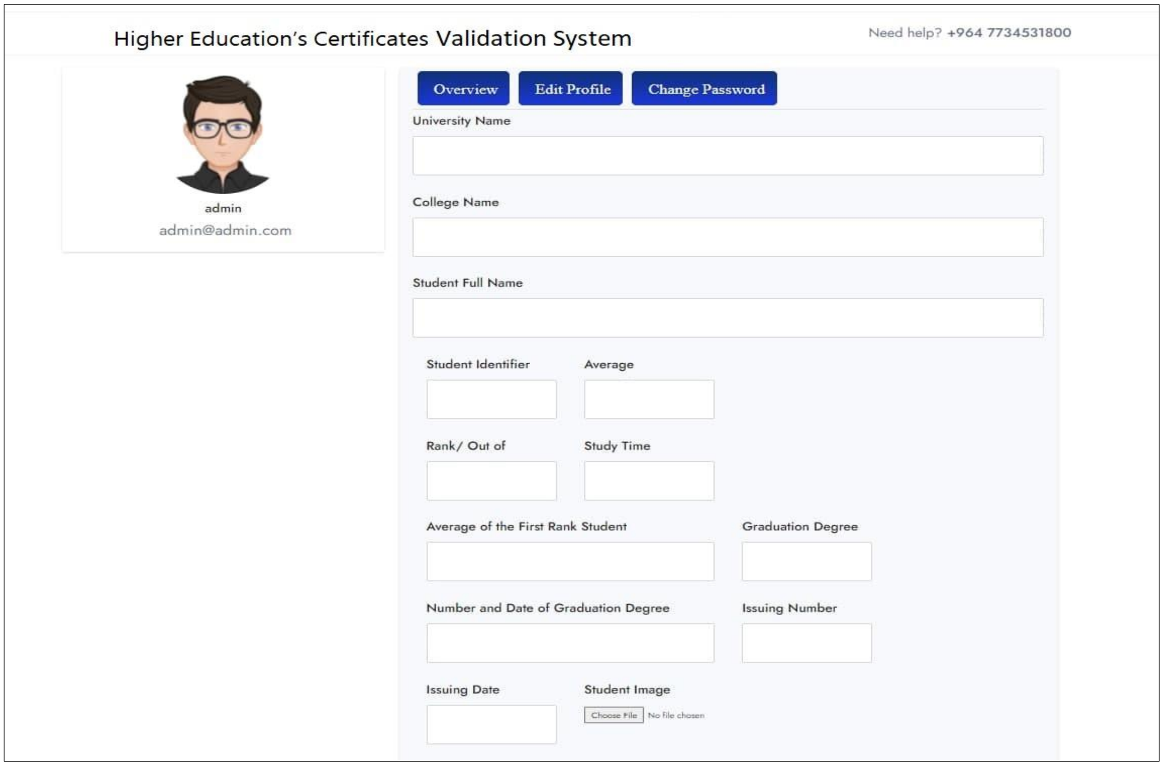
4- Time-efficient: The increased speed of creating and verifying the certificates as the certificates can be delivered and verified digitally.

5- Data Privacy and Security: Students academic achievement are stored in local and private database of educational institution, as well as store hashes of those credentials are stored on blockchain that are cryptographically protected. As result, prevent of the issuance of a forgery certificates and at the same time students creational is safe and reliable.

6-. Secure Transactions, Transparent, and Immutable Data: The hashes are approved and authorize by a consensus mechanism. Moreover, all blockchain participant store the same transactional data that are vastly improve the trust in the whole system.

7- Availability: The verification of certificate is there at any time and from anywhere even when the problem of unavailability of the educational institution such stops using the network, that their equipment malfunctions, or even stop institution work.

On the other hand, to develop a reliable and secure blockchain certificate system with high functionality and usability, a group of solid technical and mathematical foundation experts of blockchain are needed. This presents a shortcoming for practitioners and researchers in the field of education. Blockchain technology is difficult to comprehend by educators, learners, and other professional parties. Universities need to know how the adoption of the blockchain will affect their privacy, database rights, and other confidential information. This study aims to establish a model for blockchain technology accreditation for certificate verification systems. Figure (4.6) shows validator remote portal.



Higher Education's Certificates Validation System

Need help? +964 7734531800

admin

admin@admin.com

University Name

College Name

Student Full Name

Student Identifier

Average

Rank/ Out of

Study Time

Average of the First Rank Student

Graduation Degree

Number and Date of Graduation Degree

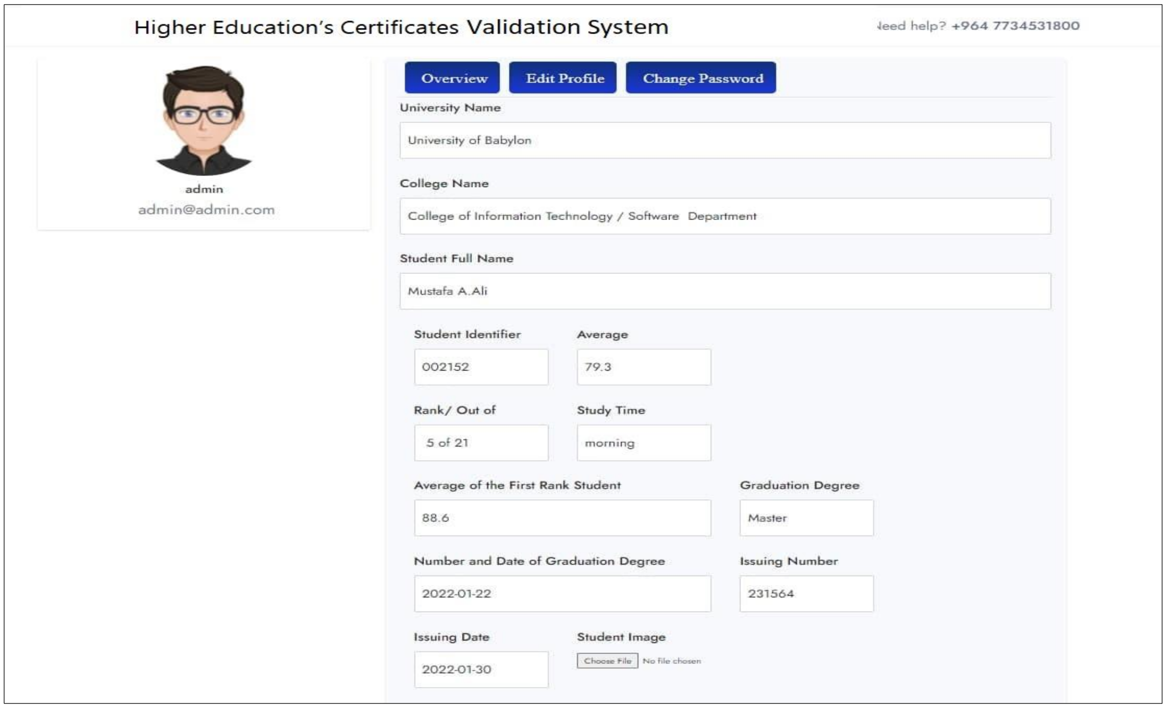
Issuing Number

Issuing Date

Student Image

No file chosen

Figure (4.6.a) Main GUI to Validate Student's Certificate (Remote Portal)


Higher Education's Certificates Validation System
Need help? +964 7734531800
Overview
Edit Profile
Change Password
admin
admin@admin.com
Choose File

University Name: University of Babylon

College Name: College of Information Technology / Software Department

Student Full Name: Mustafa A.Ali

Student Identifier: 002152

Average: 79.3

Rank/ Out of: 5 of 21

Study Time: morning

Average of the First Rank Student: 88.6

Graduation Degree: Master

Number and Date of Graduation Degree: 2022-01-22

Issuing Number: 231564

Issuing Date: 2022-01-30

Student Image: No file chosen

Figure (4.6.b) Main GUI to Validate Student's Certificate (Remote Portal)

4.8 The Proposed System Analysis

In the related studies, there are different approaches to the analysis and tests that have been implemented to test the robustness and characteristics that evaluate the cryptographic systems. The validation of cryptosystems can be measured and calculated using statistical features, correlation analysis, randomness, and key sensitivity. The cipher algorithms' encryption speed is a major concern that measures encryption algorithms' efficiency.

The analysis tests are implemented on the proposed cipher algorithms to examine the proposed cryptosystem of M-ECDSA and M-SHA3 to evaluate the security robustness and efficiency. NIST suite was considered the most useful test that examined the cryptosystems; thus, it was implemented, and the results were examined and presented for the proposed cryptosystem. The results show that the new design algorithms are reasonably efficient.

4.8.1 Correlation Coefficient Analysis

The correlation coefficient analysis (CCA) denotes the relation between two vectors, and the result of the defined algorithms always lies between -1 to +1. The values of +1 consider positively correlated, and the values of -1 denote negative correlation. Furthermore, low CCA values indicate robust confusion and diffusion. Different studies used CCA in the cryptosystem to prevent any information seepage concerning the data correlations. This approach is recently used in cryptoanalysis and for proving robust cryptographic algorithms. The CCA process is done using Four different states with the different first byte of the plaintext and calculated based on the relationship between plaintext and ciphertext as illustrated in the table (4.4) below.

Table 4.4: The CCA of the ECDSA and Proposed Algorithms.

Algorithm	State1	State2	State3	State4
ECDSA	-0.5360	0.3258	-0.6872	- 0.3589
M-ECDSA	-0.6872	0.2987	-0.5863	-0.3596

4.8.2 Avalanche Effect

Avalanche effect property is considered as a little modification in both the generated key and the plaintext to produce a substantial ciphertext modification. The good cipher algorithm must approach the value 0.5and above. This method is a desirable property for block ciphers algorithms, wherein if slightly changed in the input, such as a single bit, the output will be modified significantly. Table (4.5) shows the performance of the avalanche effect of the developed ECDSA algorithms and the original ECDSA algorithm.

Table 4.5: Avalanche Effect of ECDSA and Proposed Algorithms.

Algorithm	State1	State2	State3
ECDSA	0.515	0.537	5.78
M-ECDSA	0.521	0.565	0.511

The three states represented the data that have been tested were similarly excepted the last few letters which is different. The avalanche effect of the proposed algorithms showed a high difference and drastic change in ciphertext output.

4.8.3 The Histogram Analysis

The histogram Analysis measures the variances of the encrypting decryption values. In this analysis, a histogram is used by converting the string data into integers in range (0 to 9). The analysis is based on uniform distributed values that have been visualized through the histogram analysis. The result of the histogram analysis shows that the original data was completely different from the encoded data.

Figures (4.7, 4.8) respectively illustrate the histogram analysis of the original and proposed algorithms. The red pillars represented the plain text, and blue pillars represented the ciphertext. In the figures (4.7 ,4.8) the x axis represents the integer values for each the plaintext and cipher text. In contrast, y axis represents the frequency of the integer values for each the plaintext and cipher text.

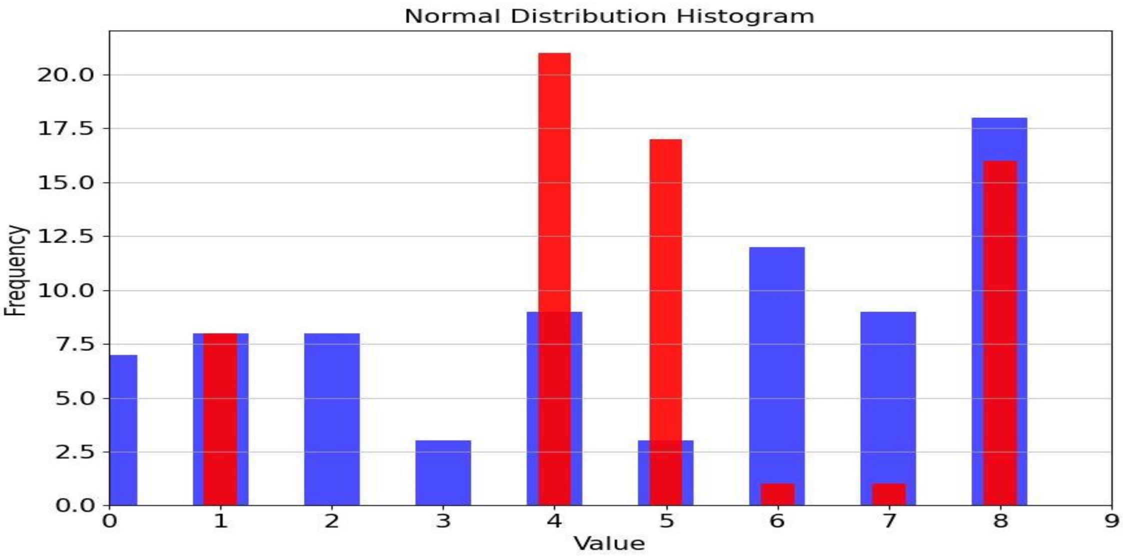


Figure (4.7) The Histogram of the ECDSA Algorithm

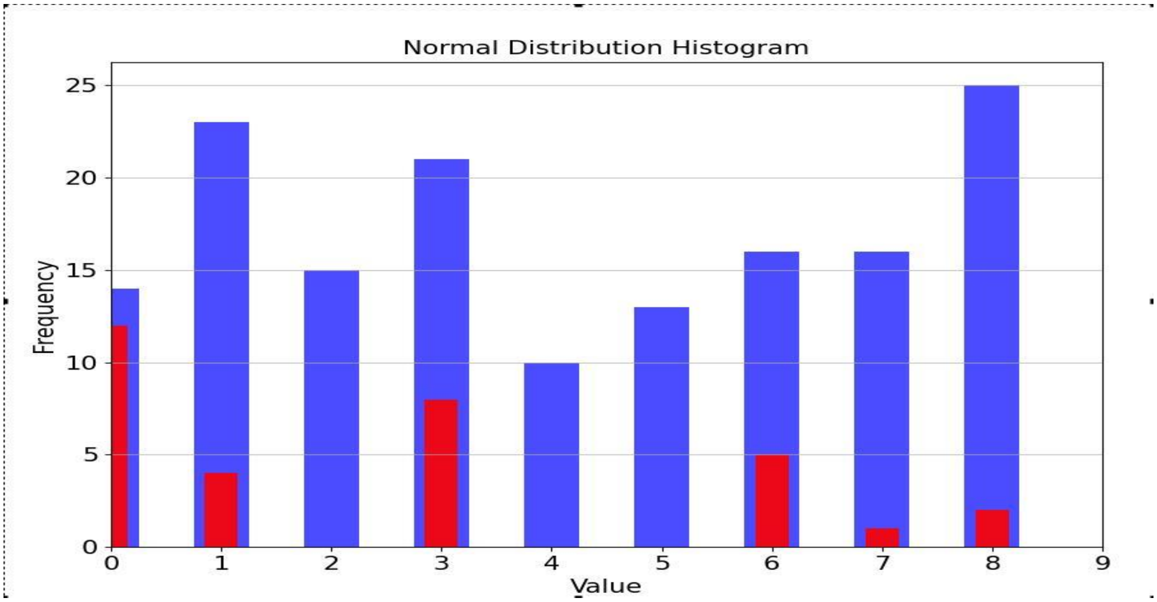


Figure (4.8) The Histogram Result of the M-ECDSA Algorithm

4.8.4 Hamming Distance

Hamming Distance (HD) measures the difference between two strings, plaintext (x) and ciphertext (y), and denoted as d(x,y). HD is calculated between two string vectors, and an XOR operation is performed between ($x \oplus y$) and then counted the entire number of 1s in the resulting string vector.

In this method, the same vectors x and y are used in the previous CCA analysis, and Table (4.7) below illustrates the HD for the ECDSA and the proposed algorithms where the smaller the HD, the higher is the diffusion.

Table 4.6: The HD for the ECDSA and Proposed Algorithms.

Algorithm	State1	State2	State3	State4
ECDSA	0.3850	0.5258	0.4872	0.2589
M-ECDSA	0.2872	0.4987	0.5073	0.2611

In the table (4.6) above, the proposed algorithm had high HD scores of the states than the ECDSA algorithm. Thus, the proposed algorithm considers robustness against cipher attacks.

4.8.5 Statistical Randomness Tests Based on NIST Suite

There are different statistic tests for examining the randomness properties of cryptography algorithms. The well-known NIST statistical test suite has used for measuring the randomness of the proposed algorithm cipher algorithm. The results of the test of all 15 NIST statistical tests are shown in the table (4.7).

Table 4.7: The NIST Test Results of the Proposed Algorithm.

NIST Tests	Proposed Algorithm
Frequency	0.7398
Block Frequency	0.9151
Cumulative Sums	0.6615

Runs	0.7913
Longest Run	0.8984
Rank	0.5681
FFT	0.6821
Non-Overlapping	0.5123
Overlapping Template	0.7254
Universal	0.6823
Approximate Entropy	0.22564
Random Excursions	0.8312
Random Excursions Variant	0.5998
Serial	0.6291
Linear Complexity	0.8912

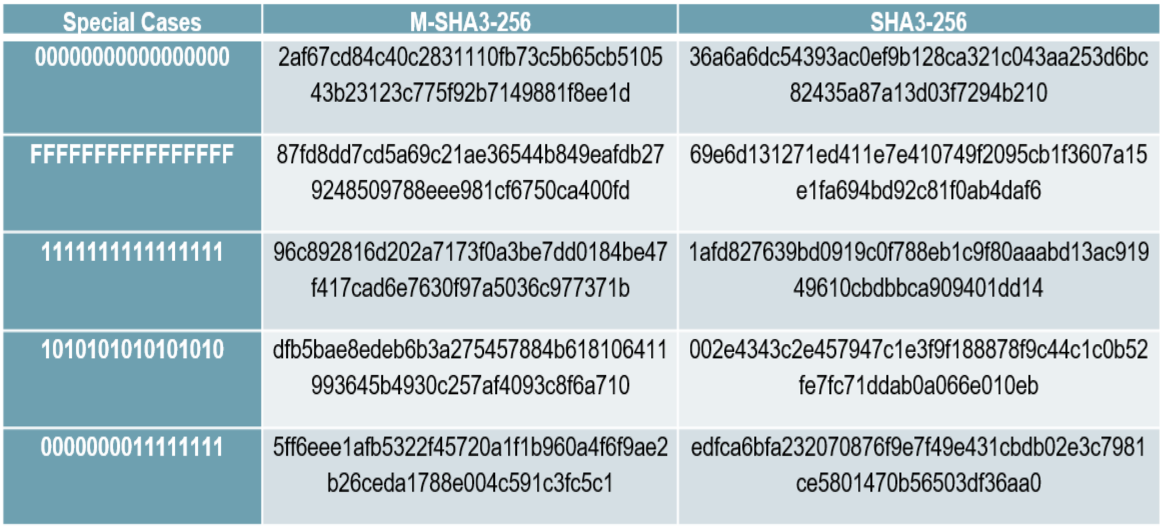
4.9 Test Results of the Proposed (M-SHA3) Algorithm

SHA-3 (Secure Hash Algorithm 3) is the latest member of the Secure Hash Algorithm family of standards, released by NIST. SHA-3 is a subset of the broader cryptographic primitive family Keccak involves core operation, which is sponge construction. Sponge construction is based on a wide random permutation and allows inputting ("absorbing" in sponge terminology) any amount of data, and outputting ("squeezing") any amount of data, while acting as a pseudorandom function with regard to all previous inputs.

The M-SHA3 algorithm that was developed based on the SHA3 architecture and implement is relying on the Chaos equations to get more randomness and less time while keep the security at high level. In M-SHA3 we reduce the number of random permutations of traditional algorithm from 24 to

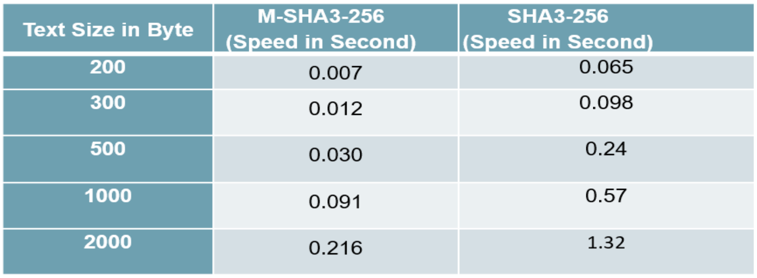
12 cycles, and instead the chaos keys was used as initialize values for (r,c). The generated hash values randomness results of M-SHA3 and SHA3 when using same data are shown in Table (4.8). Table (4.9) shows M- SHA3 has less time to run than SHA3.

Table 4.8: Comparison Randomness between Original and Modified SHA3.



Special Cases	M-SHA3-256	SHA3-256
0000000000000000	2af67cd84c40c2831110fb73c5b65cb5105 43b23123c775f92b7149881f8ee1d	36a6a6dc54393ac0ef9b128ca321c043aa253d6bc 82435a87a13d03f7294b210
FFFFFFFFFFFFFFFF	87fd8dd7cd5a69c21ae36544b849eafdb27 9248509788eee981cf6750ca400fd	69e6d131271ed411e7e410749f2095cb1f3607a15 e1fa694bd92c81f0ab4daf6
1111111111111111	96c892816d202a7173f0a3be7dd0184be47 f417cad6e7630f97a5036c977371b	1afd827639bd0919c0f788eb1c9f80aaabd13ac919 49610cbdbbca909401dd14
1010101010101010	dfb5bae8edeb6b3a275457884b618106411 993645b4930c257af4093c8f6a710	002e4343c2e457947c1e3f9f188878f9c44c1c0b52 fe7fc71ddab0a066e010eb
0000000011111111	5ff6eee1afb5322f45720a1f1b960a4f6f9ae2 b26ceda1788e004c591c3fc5c1	edfca6bfa232070876f9e7f49e431cbdb02e3c7981 ce5801470b56503df36aa0

Table 4.9: Comparison of Hashing Time between M-SHA3 and SHA3.



Text Size in Byte	M-SHA3-256 (Speed in Second)	SHA3-256 (Speed in Second)
200	0.007	0.065
300	0.012	0.098
500	0.030	0.24
1000	0.091	0.57
2000	0.216	1.32

Furthermore, the proposed M-SHA3 algorithm passed all NIST tests and shows high randomness and considers efficient to be applied in our system. Compression between NIST Tests of original and modified SHA3 algorithms are showed in Table (4.10).

Table 4.10: Results of NIST Tests for the Proposed M-SHA3 Algorithm.

NIST tests Results Name	SHA3	M-SHA3
Frequency (Mono bit) analysis	0.1487	0.8837
Block Frequency analysis	0.3787	0.1844
Cumulative Sums analysis	0.2469	0.91003
Runs analysis	0.38671	0.9602
Longest Run analysis	0.1824	0.9692
Rank analysis	0.1423	0.9442
DFT analysis	0.3422	0.6627
Non-Overlapping	0.4828	0.8952
Overlapping analysis	0.6548	0.1114
Universal analysis	0.0646	0.9236
Approximate Entropy analysis	0.0101	0.8659
Excursions analysis	0.3398	0.9625
Excursions Variant analysis	0.5875	0.65001
Serial analysis	0.4524	0.8643
Linear Complexity	0.51624	0.3056

CHAPTER FIVE

Conclusions and Future Works

5.1 Introduction

This chapter introduces the primary conclusions that have been obtained during the design and implementation of the proposed system and explore potential future areas for research. This chapter is organized into two main sections. The first one is dedicated to revealing most of the conclusions of this dissertation. The second suggests some future works that are related to this dissertation.

5.2 Conclusions

The proposed model can create innovative and destructive effects on the systems that need to be executed, stored, verified, and continually updated digital data among participating parties with trust and transparency and without central authority controlling. Blockchain presented a new dimension of secure, transparent systems through distributed connections of people, objects, data, and processes in one single system. The development of distributed and secure electronic systems has become an important subject in line with the development of the digital world.

Thus, this work aimed to develop a secure, transparent digital systems model that eliminates many security threats and adds layers of protection and trust. The implementation of such technology to systems for document's integrity and authentication such as student's certificates. The process of preserving these certificates in a way that is permanent, not tampered with, or forged is very important, especially when the individuals are subject to many academic studies and training from several different institutions and they obtain several certificates, is critical.

The advantage of this system is used to secure the published document through public channels and communicated network nodes. Moreover, it is important to present an opportunity for third parties to verify shared certificates quickly, securely, and independently.

As a case study, the proposed model is applied to the Higher Education certificates system to easily request document certificates, share, and verify these certificates with a third party. Moreover, the mechanism of the proposed model proposes permanent distributed hashes records of students' certificates to reduce forgery. The proposed model fulfils for preventing forgery certificates and managing digital academic credentials mainly in terms of trust, high outputs, availability, transparency, and resource consumption, especially with the existence of many educational institutions nowadays.

The proposed model used CNN trained model on documents images which is more powerful than other classical handcrafted methods from many aspects. The proposed method can recognize images more accurately than the handcrafted method, because of feature extraction is the crucial phase for the success of these methods due to the difficulty in designing robust features to cope with the variations in the given images. Currently, recognition research is shifting towards features extracted by CNNs, which can learn more specific features robust to the wide image variations and achieve state-of-the-art recognition performance. Additionally, it required less prediction time because of its pre-trained offline time taken. In addition, provide more security accordingly database is still private, and images are not transferred to other institutions or be online. Furthermore, to increase the CNN model accuracy the images number to each person are increased by using augmentations methods while the size of the model and original database is still the same as a result these processes are performed temporally in the training phase.

5.3 Future Works

After applying the proposed model, some suggestions and improvements that may be considered in future works, and to achieve these considerations, the following works listed are recommended:

1- Further studies to design and facilitate the creation and implementation of the blockchain solution in education are recommended, as well as applying and implementing the proposed model to other sector such person's identity, land registration, and others.

2- More focus on a digital signature and try to develop a new algorithm that works incorporates the signatures (multi-signature).

3- Enhance the current CNN model or use another model that achieve high recognition rate as well as build one unified model without transferring data from within the institutions.

4- Local data could be added to public server in some applications to make the data and model online in other case study.

5- Applying another encrypting protocol and comparing the result with the proposed protocol.

References

References

[1] A. Aristovnik, D. Keržiˇc, D. Ravšelj, N. Tomaževiˇc and L. Umek, "Impacts of the COVID-19 pandemic on life of higher education students: A global perspective." *Sustainability* 12.20, 8438, 2020.

[2] A. Al-Ansi, M. Al-Ansi, A. Muthanna, I. Elgendy, and Andrey Koucheryavy "Survey on intelligence edge computing in 6G: characteristics, challenges, potential use cases, and market drivers." *Future Internet* 13.5, 118, 2021.

[3] C. NGUYEN, Y. SAPUTRA, N. HUYNH, N. NGUYEN, T. KHOA, B. TUAN, D.NGUYEN, D. HOANG, T. VU, E. DUTKIEWICZ, S. CHATZINOTAS, AND B.OTTERSTEN. "A comprehensive survey of enabling and emerging technologies for social distancing—Part II: Emerging technologies and open issues." *Ieee Access* 8 : 154209-154236 ,2020.

[4] J. ZHANG, B. CHEN, Y. ZHAO, X. CHENG, AND F. HU. "Data security and privacy-preserving in edge computing paradigm: Survey and open issues." *IEEE access* 6 ,18209-18237, 2018.

[5] H. Morgan. "Cyber security risk management in the SCADA critical infrastructure environment." Engineering Management Journal 25, no. 2 (2013): 38-45.

[6] K. Khando, S. Gao, S. Islam and A. Salman. "Enhancing employees information security awareness in private and public organisations: A systematic literature review." *Computers & Security* 106 , : 102267, 2021.

[7] J. Lima, F. Salinas, L. Oquendo, F. Sanchez, G. Fonseca and D. Quiroz. "Information security management frameworks and strategies in higher education institutions: a systematic review." *Annals of Telecommunications* 76.3 255-270, 2021.

[8] C. Larissa, and K. Schneider. "Explainability as a non-functional requirement: challenges and recommendations." *Requirements Engineering* 25.4, 493-514, 2020.

[9] M. Lennartsson, J. Kävrestad, and M. Nohlberg. "Exploring the meaning of usable security–a literature review." *Information & Computer Security* (2021).

[10] Terpos, E., Mikhael, J., Hajek, R., Chari, A., Zweegman, S., Lee, H. C., ... & Usmani, S. Z. (2021). Management of patients with multiple myeloma beyond the clinical-trial setting: understanding the balance between efficacy, safety and tolerability, and quality of life. *Blood cancer journal*, 11(2), 1-13

[11] K.Maxat. "Blockchain and e-government innovation: Automation of public information processes." *Information Systems* 103, 101862, 2022.

[12] A. Manzoor, A. Braeken, S. Kanhere, M. Ylianttila and M. Liyanage. "Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain." *Journal of Network and Computer Applications* 176,102917, 2021

References

[13] B. Bhushan, C. Sahoo, P. Sinha ad A Khamparia. "Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions." *Wireless Networks* 27.1 ,55-90, 2021.

[14] C. Pfleeger and S. Pfleeger. "Analyzing computer security: A threat/vulnerability/countermeasure approach." *Prentice Hall Professional*, 2012.

[15] R. Castro, and M. Au-Yong-Oliveira. "Blockchain and higher education diplomas." European Journal of Investigation in Health, Psychology and Education 11, no. 1, 154-167, 2021.

[16] S. Balsubramanian, R. Prashanth and S. Ravishankar. "Mark sheet verification." *2009 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication*. IEEE, 2009

[17] S. Sale, O. Ghazali and Q. Al Maatouk. "Graduation certificate verification model: a preliminary study." *International Journal of Advanced Computer Science and Applications* 10.7 (2019).

[18] Bibi, Maryam, A. Hamid, M. Moetesum, and I. Siddiqi. "Document forgery detection using source printer identification: A comparative study of text-dependent versus text-independent analysis.*", Expert Systems , 2022.*

[19] S. Omar, O. Ghazali, and M. Rana. "Blockchain based framework for educational certificates verification." *Journal of critical reviews* 7.03,79-84, 2020.

[20] GoChain, Retrieved March 10, 2021 from https://www.unic.ac.cy/university-of-nicosia-iff-joins-gochain-network-as-a-signing-node/#

[21] Z. Aaber, G. Willsa. and R. Crowder. "Protecting document outside enterprise network: A confirmed framework. In International Workshop on Enterprise Security. " (pp. 259-275). Springer, Cham, 2015.

[22] https://www.blockcerts.org/ [retrieved: August 16,2018]

[23] W. Gräther, S. Kolvenbach, R. Ruland, J. Schütte, C. Torres and F. Wendland. Blockchain for education: lifelong learning passport. in *Proceedings of 1st ERCIM Blockchain workshop 2018*. European Society for Socially Embedded Technologies (EUSSET), 2018.

[24] N. Nizamuddin, H. Hasan, K. Salah and R. Iqbal. "Blockchain-based framework for protecting author royalty of digital assets." *Arabian Journal for Science and Engineering*, 44(4), 3849-3866, 31.12.2018.

[25] S. Mthethwa, N. Dlamini, and G. Barbour. "Proposing a blockchain-based solution to verify the integrity of hardcopy documents." *In 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC) (pp. 1-5). IEEE.* 2018.

References

[26] C. Brunner, F. Knirsch and D. Engel. “SPROOF: A Platform for Issuing and Verifying Documents in a Public Blockchain.” In ICISSP (pp. 15-25),2019.

[27] V. Yatskiv, N. Yatskiv, and O. Bandrivskyi. “Proof of Video Integrity Based on Blockchain.” *In International Conference on Advanced Computer Information Technologies* (ACIT) (pp. 431-434). IEEE. 2019

[28] I. Permatasari, M. Essaid, H. Kim and H. Ju.”Blockchain implementation to verify archives integrity on cilegon E-archive.” *Applied Sciences*, 2621, 10(7) 2020.

[29] R. Dharmalingam, H. Ugail, A. Shivasankarappa, and V. Dharmalingam, “Framework for Digitally Managing Academic Records Using Blockchain Technology.” I*n Mobile Computing and Sustainable Informatics (pp. 633-645). Springer, Singapore*. 2022

[30] W. Negasa and D. Prasad Sharma. "A Blockchain-Enabled Digital Document Locker and Verification Model for Ethiopia." *IUP Journal of Knowledge Management* 18.2 2020.

[31] Britt, M. Anne, Jean-Francois Rouet, and Jason LG Braasch. "Documents as entities: Extending the situation model theory of comprehension." Reading-from words to multiple texts. *Routledge*, 2012. 174-193.

[32] O. Beth. *Forging the Past: Invented Histories in Counter-Reformation Spain*. Yale University Press, 2015.

[33] J. Reis, M. Amorim, N. Melão and P. Matos.” Digital transformation: a literature review and guidelines for future research.” In *World conference on information systems and technologies* (pp. 411-421). Springer, Cham, 2018.

[34] A. Tanenbaum and D. Wetherall, "**Computer Networks**", book, 5th ed., 2011.

[35] E. Daniel and F. Tschorsch. "Ipfs and friends: A qualitative comparison of next generation peer-to-peer data networks." *IEEE Communications Surveys & Tutorials* (2022).

[36] C. N. Academy, "**Network Basics Companion Guide**", book, 1st ed., Cisco Press 800 East 96th Street, 2013.

[37] S. Rüdiger. "A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications." *Proceedings First International Conference on Peer-to-Peer Computing*. IEEE, 2001.

[38] V. Gomes, G. Queiroz, and K. Ferreira."An overview of platforms for big earth observation data management and analysis." *Remote Sensing* 12, no. 8, 1253, 2020.

[39] S. Zeebaree, H. Shukur, L.Haji, R. Zebari, K. Jacksi, S. Abas. “Characteristics and analysis of hadoop distributed systems.” *Technology Reports of Kansai University*, *62*(4), 1555-1564, April 2020.

References

[40] S. Sharma,and Y. Gupta. “Study on cryptography and techniques.” *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* 2(1), 2017.

[41] M. Rogobete and O. Tarabuta. “Hashing and Message Authentication Code Implementation. An Embedded Approach.” *Scientific Bulletin Mircea cel Batran Naval Academy,* p. 296A-304, 22(2)2019.

[42] S. Singh, P. Sharma, and D. Arora,. “Data Integrity Check in Cloud Computing using Hash Function.” *International Journal of Advanced Research in Computer Science8(5), 2017.*

[43] A. Qadi and N. Varol.” A Review Paper on Cryptography.” *International Symposium on Digital Forensics and Security (ISDFS)*. IEEE. 2019.

[44] S. Ramakrishnan , *Cryptographic and Information Security Approaches for Images and Videos*. CRC Press, 2018.

[45] S. Hong. "Efficient digital signatures from RSA without random oracles." *Information Sciences* 512 471-480, 2020

[46] G. Abdullah, Q. Mehmood and C. Ahmad Khan"Authentication of symmetric cryptosystem using anti-aging controller-based true random number generator." *Applied Nanoscience* 1-10,2021

[47] V. Shetty, R. Anusha, M. Dileep Kumar and P.Hegde.” A survey on performance analysis of block cipher algorithms.”*International Conference on Inventive Computation Technologies (ICICT)* (pp. 167-174). IEEE, 2020.

[48] L. Jiao, Y. Hao, and D. Feng. "Stream cipher designs: a review." *Science China Information Sciences* 63.31-25, 2020.

[49] M. Dworkin. “SHA-3 standard: Permutation-based hash and extendable-output functions.” *National Institute of Standards and Technology*

Gaithersburg, MD 20899-8900, 2015.

[50] D. Bhattacharjee, V. Pudi, and A. Chattopadhyay. “SHA-3implementation using ReRAM based in-memory computing architecture.” *International Symposium* on Quality Electronic Design (ISQED). IEEE, in 2017 18th

[51] Z. Jawad, and H. Hoomod. "A hybrid modified lightweight algorithm combined of two cryptography algorithms PRESENT and Salsa20 using chaotic system." *International Conference of Computer and Applied Sciences (CAS). IEEE*, 2019.

References

[52] M. Ali, and W. Bhaya. "Blockchain technology's applications and challenges: An overview." *AIP Conference Proceedings*. Vol. 2290. No. 1. AIP Publishing LLC, 2020.

[53] Javaid, M., Haleem, A., Singh, R. P., Khan, S., & Suman, R. "Blockchain technology applications for Industry 4.0: A literature-based review Blockchain*." Research and Applications*, 100027, 2021.

[54] T. Tasatanattakool and C. Techapanupreeda. "Blockchain: Challenges and applications." *2018 International Conference on Information Networking (ICOIN)*. IEEE, 2018.

[55] A. Antonopoulos. "Mastering Bitcoin: unlocking digital cryptocurrencies. O'Reilly Media, Inc, 2014.

[56] M. Swan. "Blockchain: Blueprint for a new economy. " *O'Reilly Media, Inc*, 2015.

[57] B. Hill, S. Chopra, and P. Valencourt. *Blockchain Quick Reference: A guide to exploring decentralized blockchain application development*. Packt Publishing Ltd, 2018.

[58] D. Puthal, N. Malik, S.Mohanty, E. Kougianos, and C. Yang "The blockchain as a decentralized security framework" [future directions]. *IEEE Consumer Electronics Magazine*, *7*(2), 18-21, 2018.

[59]M.l Crosby, Nachiappan, P. Pattanayak, S. Verma and V. Kalyanaraman. "BlockChain Technology:Bitcoin, Beyond." *Tech. Rep. 2015*.

[60] K. Sultan, U. Ruhi and R. Lakhani. "Conceptualizing blockchains: Characteristics & applications." *arXiv preprint arXiv:1806.03693*, 2018.

[61] Y. Wanga and A. Kogan. "Designing confidentiality-preserving Blockchain-based transaction processing systems." *International Journal of Accounting Information Systems* 30 1-18, 2018.

[62] D. Kraft. "Difficulty control for blockchain-based consensus systems." *Peer-to-peer Networking and Applications* 9.2 397-413, 2016.

[63] A. Antonopoulos and G. Wood."Mastering ethereum: building smart contracts and dapps." *O'reilly Media,* 2018.

[64] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels and B. Amaba."Blockchain technology innovations." *2017 IEEE technology & engineering management conference (TEMSCON)*. IEEE, 2017.

[65] S. Nakamoto, and A. Bitcoin. "A peer-to-peer electronic cash system." *Bitcoin. –URL: https://bitcoin. org/bitcoin. pdf* 4, 2008.

References

[66] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang. "An overview of blockchain technology: Architecture, consensus, and future trends." *2017 IEEE international congress on big data (BigData congress)*. Ieee, 2017.

[67]G. Nguyen and K. Kim. "A survey about consensus algorithms used in blockchain." *Journal of Information processing systems* 14.1101-128, 2018.

[68]L. Mihaljevic and M. Zagar. "Comparative analysis of blockchain consensus algorithms." *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. Ieee, 2018.

[69] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang "An overview of blockchain technology: Architecture, consensus, and future trends." *2017 IEEE international congress on big data (BigData congress)*. Ieee, 2017.

[70] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, “A Review on Consensus Algorithm of Blockchain Du,” *IEEE Trans. Human-Machine Syst*., vol. 47, no. 2, pp. 304–304, 2017, doi: 10.1109/thms.2017.2671618.

[71] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, “PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain,” *CEUR Workshop Proc*., vol. 2058, pp. 1–11, 2018.

[72] M. Pilkington, “*Blockchain technology: Principles and applications*,” Res. Handbooks Digit. Transform., pp. 225–253, 2016, doi: 10.4337/9781784717766.00019.

[73] H. Hellani, A. E. Samhat, M. Chamoun, H. El Ghor, and A. Serhrouchni, “On BlockChain Technology: Overview of Bitcoin and Future Insights,” *2018 IEEE Int Multidiscip. Conf. Eng. Technol. IMCET 2018*, pp. 1–8, 2019, doi: 10.1109/IMCET.2018.8603029.

[74] D. Vujičić, D. Jagodić, and S. Randić, “Blockchain technology, bitcoin, and Ethereum: A brief overview,” *2018 17th Int. Symp. INFOTEH-JAHORINA, INFOTEH 2018* - Proc., vol. 2018-January, no. March, pp. 1–6, 2018, doi: 10.1109/INFOTEH.2018.8345547.

[75] C. Wright, “Bitcoin: A Peer-to-Peer Electronic Cash System [Bitcoin: un sistema de efectivo electrónico de igual a igual],” SSRN Electron. J., pp. 1–9, 2008, [Online]. Available: https://www.ssrn.com/abstract=3440802.

[76] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, “Presence of prostaglandin E in lung tumors from normocalcemic patients,” *Am. J. Med., vol. 72, no. 5, p. A29*, 2017, doi: 10.1016/0002-9343(82)90530-7.

[77] V. Buterin, “A next-generation smart contract and decentralized application platform,” Etherum, no. January, pp. 1–36, 2014, [Online]. Available: http://buyxpr.com/build/pdfs/EthereumWhitePaper.pdf.

[78] V. Dhillon, D. Metcalf, and M. Hooper, The Hyperledger Project. 2017.

References

[79] A. Dorri, S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things: Challenges and Solutions,” *Univ. New South Wales, vol. 45, no. 2 PART 1, pp. 129–137*, 2016, doi: 10.1016/0168-0072(89)90057-2.

[80] Feng Tian, “An information System for Food Safety Monitoring in Supply Chains based on HACCP, Blockchain and Internet of Things,” *WU Vienna Univ. Econ. Bus., no. March*, 2018, [Online]. Available: http://epub.wu.ac.at/.

[81] D. Dujak and D. Sajter, “Blockchain Applications in Supply Chain,” *Springer Int. Publ. AG*, pp. 21–46, 2019, doi: 10.1007/978-3-319-91668-2_2.

[82] S. Chang and Y. Chen, “When blockchain meets supply chain: A systematic literature review on current development and potential applications,” *IEEE Access, vol. 8, pp. 62478–62494*, 2020, doi: 10.1109/ACCESS.2020.2983601.

[83] R. Azzi, R. Kilany, and M. Sokhn, “The power of a blockchain-based supply chain,” *Comput. Ind. Eng., vol. 135, no. June, pp. 582–592*, 2019, doi: 10.1016/j.cie.2019.06.042.

[84] S. Dey, S. Saha, A. Singh, and K. McDonald-Maier, “FoodSQRBlock: Digitizing food production and the supply chain with blockchain and QR code in the cloud,” *Sustain., vol. 13, no. 6, pp. 1–11*, 2021, doi: 10.3390/su13063486..

[85] Y. Ma, Y. Sun, Y. Lei, N. Qin, and J. Lu, “A survey of blockchain technology on security, privacy, and trust in crowdsourcing services,” *Springer, vol. 23, no. 1, pp. 393–419*, 2019, doi: 10.1007/s11280-019-00735-4.

[86] B. Bhushan, P. Sinha, K. Sagayam, and A. J, “Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions,” *Comput. Electr. Eng., vol. 90, no. July 2019, p. 106897*, 2020, doi: 10.1016/j.compeleceng.2020.106897.

[87] F. Khan, M. Asif, A. Ahmad, M. Alharbi, and H. Aljuaid, “Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development,” *vol. 55. Elsevier B.V.*, 2020.

[88] D. Valdeolmillos, Y. Mezquita, A. González-Briones, J. Prieto, and J. M. Corchado, “Blockchain technology: A review of the current challenges of cryptocurrency,” *Springer Nat. Switz. AG, vol. 1010, pp. 153–160*, 2020, doi: 10.1007/978-3-030-23813-1_19.

[89] I. Lin and T. Liao, “A survey of blockchain security issues and challenges,” *Int. J. Netw. Secur., vol. 19, no. 5, pp. 653–659*, 2017, doi: 10.6633/IJNS.201709.19(5).01.

[90] M.Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang and D. Mohaisen, “Exploring the Attack Surface of Blockchain: A Comprehensive Survey,” I*EEE Commun. Surv. Tutorials, vol. 22, no. 3, pp. 1977–2008*, 2020, doi: 10.1109/TPDS.2015.2488629.

References

[91] M.Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang and D. Mohaisen "Overview of attack surfaces in blockchain." *Blockchain for distributed systems security* (2019): 51-66.

[92] Y. Chen and U. Volz, “Scaling up sustainable investment through blockchain-based project bonds,” Dev. Policy Rev., vol. 40, no. 3, pp. 1–15, 2022, doi: 10.1111/dpr.12582.

[93] M. Ali and W. Bhaya, “Higher Education’s Certificates Model based on Blockchain Technology,” *J. Phys. Conf. Ser., vol. 1879, no. 2*, 2021, doi: 10.1088/1742-6596/1879/2/022091.

[94] M. Kaur and S. Gupta, “Blockchain Technology for Convergence: An Overview, Applications, and Challenges,” *IGI Glob., no. June, pp. 1–17*, 2021, doi: 10.4018/978-1-7998-6694-7.ch001.

[95] Kaal, Wulf A. "Blockchain solutions for agency problems in corporate governance." *Information for Efficient Decision Making: Big Data, Blockchain and Relevance*. 2021. 313-329.

[96] M. Wani, F. Bhat, S. Afzal, and A. Khan, *Advances in Deep Learning*. Springer, 2020.

[97] M. Coskun, A. Ucar, O. Yildirim, and Y. Demir, “Face Recognition Based on Convolutional Neural Network,” *IEEE, vol. 54, no. 5, pp. 376–379*, 2017, doi: 10.13810/j.cnki.issn.1000-7210.2019.05.024.

[98] Z. Zhang, “Derivation of Backpropagation in Convolutional Neural Network (CNN),” *Univ. Tennessee, Knoxville, TN, pp. 1–7*, 2016.

[99] A. Al-Bayati, “Enhancing Performance of Hybrid AES, RSA and Quantum Encryption Algorithm,” *Anglia Ruskin University Enhancing,* 2021.

[100] L. Zhang, Y. Liu, C. Wang, J. Zhou, Y. Zhang, and G. Chen, “Improved known-plaintext attack to permutation-only multimedia ciphers,” *Inf. Sci. (Ny)., vol. 430–431, pp. 228–239*, 2018, doi: 10.1016/j.ins.2017.11.021.

[101] S. Jiao, Y. Gao, T. Lei, and X. Yuan, “Known-plaintext attack to optical encryption systems with space and polarization encoding,” *Opt. Express, vol. 28, no. 6, pp. 8085–8097*, 2020, doi: 10.1364/oe.387505.

[102] D. Siva Kumar and P. Santhi Thilagam, “Approaches and challenges of privacy preserving search over encrypted data,” *Inf. Syst., vol. 81, pp. 63–81*, 2018, doi: 10.1016/j.is.2018.11.004.

[103] R.Deepthi, “A Survey Paper on Playfair Cipher and its Variants,” Int. Res. J. *Eng. Technol., vol. 4, no. 4, pp. 2607–2610*, 2017, [Online]. Available: https://www.irjet.net/archives/V4/i4/IRJET-V4I4642.pdf.

References

[104] Muthavhine, K.D. and M. Sumbwanyambe. An analysis and a comparative study of cryptographic algorithms used on the Internet of Things (IoT) based on avalanche effect. in 2018 International Conference on Information and Communications Technology (ICOIACT). 2018. IEEE.

[105] S. Zhu and C. Zhu, “Image encryption algorithm with an avalanche effect based on a six-dimensional discrete chaotic system,” *Multimed. Tools Appl., vol. 77, no. 21, pp. 29119–29142*, 2018, doi: 10.1007/s11042-018-6078-2.

[106] R. Miranda-Quintana, D. Bajusz, A. Rácz, and K. Héberger, “Extended similarity indices: the benefits of comparing more than two objects simultaneously. Part 1: Theory and characteristics†,” *J. Cheminform., vol. 13, no. 1, pp. 1–18*, 2021, doi: 10.1186/s13321-021-00505-3..

[107] R.Andrew, S. Juan, N.James, S. Miles, B. Elaine, L. Stefan, L. Mark, V. Mark, B. David, H. Alan, D. James, V. San, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,” *Nist Spec. Publ.*, vol. 22, no. April, pp. 1-1-G-1, 2010, [Online]. Available: http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf.

الخلاصة

ان تطور الأنظمة الالكترونية الموزعة والامنة أصبحت موضوعا هاما تماشيا مع التطور الحاصل في العالم الرقمي، وخصوصا بعد جائحة كورونا فان الاعتماد على الأجهزة والأنظمة الالكترونية أصبح واسع الانتشار في مختلف مفاصل الحياة اليومية. وقد فضلت هذه الأنظمة لما لها من الخواص المميزة كالشفافية والثقة وعدم المركزية وسجل البيانات غير القابل للتعديل.

يستخدم التحقق الالكتروني لتسهيل واتمتة بعض العمليات وكذلك بإمكان المستخدم انجاز التحقق الالكتروني على الفور. فضلا عن ذلك ان بالإمكان مشاركة الملفات بسهولة وامان. وتستخدم أدوات مناسبة مثل التحقق من خلال موقع الويب دون انشاء قاعدة بيانات مركزية لضمان خصوصية البيانات. وهذه التقنية يتم تشغيلها ضمن شهادة رقمية وتسهل التحقق التلقائي من قبل طرف ثالث دون الحاجة الى مؤسسة المصدر.

من جانب اخر تعاني انظمة الحضر من مشاكل التفضيل بين الامن والكفاءة. في المقابل لوحظت عدة عوامل تؤثر على فاعلية أنظمة الحضر مثل هجوم الأغلبية وقابيله التوسيع ومشاكل أخرى تتعلق بالتعقيد. لذلك تم تقديم نموذج تحليل الأنظمة المستندات قائم على سلسلة الحضر وكذلك سي ان للهندسة العمارية، التي توفر سلامة المستندات الالكترونية والمصادقة عليها للحفاظ على الشفافية والثقة مع الأطراف غير الموثوقة للتخلص من مشاكل النظام المركزي. يضمن تكامل المستند عدم وجود أي تغيير في أجزاء المعلومات المشتركة ويتم توفير نفس المستند لجميع الأطراف. تثبت المصادقة المالكين الشرعيين والهويات لجميع الأطراف الأخرى. فقد جدت الدراسة تحقق هذا الامر من خلال استخدام تلك التقنيات.

يعد الاتصال الامن بين الأطراف امر بالغ الأهمية اثناء نقل البيانات بين الأطراف ورفض عم الأطراف غير الموثوق فيها. يتم تعريف خوارزميات التشفير والتوافق كحلول امنة لهذه المتطلبات. بالإضافة الى ذلك فانه يوفر الخصوصية والثقة والشفافية. كما انه يتخلص من الخروقات الأمنية التي تهدد الانظمة الحالية، حيث تقوم الجهات الخارجية بجمع البيانات الهامة والتحكم فيها.

يتم تحليل ومراجعة الخوارزميات المقترحة بناء على اختبارات معرفية في هذا المجال مثل اختبارات مجموعة الاختبار الإحصائي (NIST) وتأثير الانهيار الجليدي. وان نتائج التجربة أظهرت ان الخوارزميات المقترحة أفضل من الخوارزميات الحالية من حيث العشوائية ووقت التنفيذ. علاوة على ذلك تم تطبيق اختبارات مختلفة كالمسافة المطروقة والانهيار الجليدي للتحقق من عمل الخوارزمية المقترحة ضد الهجمات التفاضلية.

ان تأثير اختبارات المسافة المؤثرة والانهيار الجليدي لخوارزمية التوقيع الرقمي المنحنى الإهليلجي (ECDSA) المقترحة كانت مؤثرة جدا بنسبة 5%. تم تطبيق أربع شبكات عصبية عميقة لشبكة (CNN) لتعليم بنية التعليم مثل Inception, ResNet,VGGNet-16, VGGNet-19, للتعرف على الصور داخل المستند تتألف العينة من مجموعة بيانات ما بين 22000 الى 10000 مع معلمات مفرطة مختلفة وتعديلات معمارية. اظهرت التجارب دقة بلغت 72%, 80%, 82% و91%. يجب ان تهتم الاعمال المستقبلية بتنفيذ سلسلة الكتل والتعليم العميق كتطبيقات اللامركزية في العديد من البيئات الحقيقة والواقعية واستكشاف خصائص وفوائد هذه التطبيقات.