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

Secured Agricultural Products Traceability System

A Thesis

Submitted to the Council of the College of Information Technology for Postgraduate Studies of University of Babylon in Partial Fulfillment of the Requirements for the Degree of Master in Information Technology -Information Networks

By

Shahad Saleem Khudair Karim

Supervised by

Asst. Prof. Dr. Ameer Kadhim Hadi

2021 A.D 1443 A.H

﴿قَالُوا سُبْحَانَكَ لَا عِلْمَ لَنَا إِلَّا مَا عَلَّمْتَنَا ۖ إِنَّكَ أَنتَ الْعَلِيمُ الْحَكِيمُ﴾

صدق الله العظيم

سورة البقرة – آية (32)

BICITS'21

1st Babylon International Conference on Information Technology and Science

CERTIFICATE OF ACCEPTANCE

This certificate is granted to

Shahad Salem, and Ameer Khadim Hadi

Certifies the acceptance of the research paper entitled:

A PROPOSED METHODOLOGY TO USE A BLOCK-CHAIN IN SUPPLY CHAIN TRACEABILITY

in

BICITS'21

Which will be held on 28-29 April, 2021 in Babylon, IRAQ, by College of Information Technology, University of Babylon and Technically Sponsored by IEEE represented by IEEE Iraq Section.

Prof. Dr. Hussain Attia
Dean of IT College, University of Babylon

Prof. Dr. Sattar B. Sadkhan
IT College, University of Babylon, IEEE Iraq Section

Declaration

I hereby declare that this dissertation entitled "**Secured Agricultural Products Traceability System**", submitted to University of Babylon in partial fulfilment of requirements for the degree of Master in Information Technology \ Information Network, 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 experts and summaries whose source are appropriately cited in the references.

Signature:

Name: **Shahad Saleem Khudair Karim**

Date: / / 2021

Supervisor Certification

I certify that this thesis was prepared under my supervision at the Department of Information Networks / College of Information Technology / University of Babylon, by **Shahad Saleem Khudair Karim** as a partial fulfillment of the requirements for the degree of **Master in Information Technology**.

Signature:
Name: **Asst. Prof. Dr. Ameer Kadhim Hadi**
Title: **Assistant Professor**
Date: / / 2021

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

Signature:
Name: **Prof. Dr. Saad Talib Hasson**
Title: **Professor**
Date: / / 2021

Certification of the Examination Committee

We hereby certify that we have studied the thesis (**Secured Agricultural Products Traceability System**) presented by the student (shahad saleem) and examined her in its content and what is related to it , and that, in our opinion ,it is adequate with (**Excellent**) standing as a thesis for the degree of Master in Information Technology-Information Networks.

Signature:
Name: Dr. Yossra HUSSIN Ali
Title: Assistant Professor
Date: / / 2021
(**Chairman**)

Signature:
Name: Dr. Saif M. KM.AL-Khalaf
Title: Assistant Professor
Date: / / 2021
(**Member**)

Signature:
Name: Dr. Nawfal Turki Obeis
Title: Lecturer
Date: / / 2021
(**Member**)

Signature:
Name: Dr. Ameer Kadhim Hadi
Title: Assistant Professor
Date: / /2021
(**Member and supervisor)**

Approved by the Dean of the College of Information Technology, University of Babylon

Signature:
Name: Dr.Hussein A. Lafta
Title: Professor
Date: / / 2021
(**Dean of Collage of Information Technology**)

Dedication

This thesis is dedicated to:

Imam Sahib Al-Zaman (may Allah hasten his reappearance),

to the Soul of my brother, Muhammad Ali.

Acknowledgments

First of all, I have to thank **my family** who helped and supported me throughout my life. Their enthusiasm and willingness to provide feedback made the completion of this research an enjoyable experience. Special thanks to my supervisor **Dr. Ameer Kadhim Hadi** for countless hours of reflection, reading, and encouragement despite the circumstances I have been through.

I would also extend my thanks and deep respect to **my college professors** for their advice, support, and encouragement.

Finally, I would like to thank **my friends** who have been most generous with their valuable experience.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Definition
3PL	third-party logistics
API	Application Programming Interface
D-Apps	decentralized apps
DC	Direct current
DCV	DEMAND CONTROLLED VENTILATION
DK	decryption keys
DLT	Distributed Ledger Technologies
DS	Digital signature
DSA	Digital Signature Algorithm
EK	encryption keys
EMR	enforcing business procedures
FIPS	Federal Information Processing Standard
FSCN	Food Supply Chain Networking
HMAC	Hash-based Message Authentication Code
ICOs	Initial Coin Offerings
IDR	Indonesia Rupiah
MIT	Massachusetts Institute of Technology
QR	Quick Response code
RFID	Radio-frequency identification
RSA	Rivest Shamir Adleman
SCI	Service Civil International
SDLC	System Development Life Cycle
SHA	Secure Hash Algorithm
SQL	Structured Query Language
VSM	Value Stream Mapping

Abstract

The supply chain is a series of procedures that involve making decisions and executing materials, money and information flow that with the intention to reach the eventual customer demands. This procedure goes through a number of supply chain phases. A supply chain represents the alignment of firms that brings products or services to market. One of the main challenges that face transferring the data over the network is how to keep the data intact while they are transferred from the source to destination, especially with existence of many intruders and hackers. One of the techniques to protect the data is by depending on the security Algos to provide integrity of authenticate algorithms to create signatures from the original data sent with it to the destination. When the data received at the destination the signature is checked. If they match, this mean that the data is received from authorized person. Otherwise, any difference in the signatures indicates that the data is received from unauthorized person. In this thesis, a supply chain traceability system is designed using some security methods such as HMAC (hash message authentication code), which comprises RSA and SHA512 implement data integrity. In such contracts, manufacturers define the composition of products and trace its origin to prevent it from manipulating. The results of the proposed model that have been obtained through the supply chain is evaluated in terms of time consumption, which is found to be relatively low (ranging between 0-9 sec). The security and precision are measured using the entropy. As for the accuracy and product security, the signature was used to ensure that no cases of manipulation occur throughout the phases of buying, selling, or transportation. The conclusion is drawn that using the supply chain, along with the HMAC and RSA algorithms within the Django environment as a single model does indeed provide the security and privacy. This combination creates

an effective framework in terms of saving time and scalability, providing high-accuracy and reliable results in less than a minute, in addition to the ease of dealing between parties. It also reduces efforts and costs, thereby representing a relatively less expensive alternative as compared to others in terms of transportation, agreements, and maintaining the security of product data.

Declaration Associated with this Thesis

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

(First Paper)

• **Name of Journal:** conference IEEE

• **Paper Title:** A proposed methodology to use a Block-chain in Supply Chain Traceability

• **Authors:** Ameer Kadhim Hadi**;** Shahad Saleem Kudair Karim

College of Information Technology, University of Babylon, Babil, Iraq

Chapter One

General Introduction

Chapter One

General Introduction

1.1 Introduction

Food safety is the main business for community these days. Some of the main issues found include food fraud, unlicensed productions and foodborne diseases in food supply chains. Such issues lead to the emergence of damage to consumers' health and failure in the food industry. In particular, several organizations tend to pay attention to the difficulties in food safety for which there are certain measures made in order to cope with them [1]. The ability to trace goods from source to retailer has increased in importance. Customers are more invested in utilizing goods which are in compliance with particular environmental and ethical criteria. Given the growing reproduction, deterioration, and use of unnecessary and dangerous chemicals, it has become necessary to trace the supply chains of products so as to overcome these issues. These systems enable users of verifying the consistency of products from farmers to retailers [2].

Supply chain traceability is the capacity to classify, track, and discover elements of a product or material as it moves along the supply chain from raw gains to finished goods, such as a food supply chain or oil supply chain. Today's supply chains are complicated system that include several stakeholders and make it difficult to verify. Several important criteria are to be considered, such as people of origin, planes in crop development, conformance to quality measures, and monitor harvests [3].

Furthermore, food information in the goods can directly affect allergy, diabetic and other health issues, which might have an effect on the patient's health if it is badly included. In addition, socially, the incorrect signs of Halal food in European countries leads to unacceptable behavior against Muslims people in case it is improperly included. In some cases, the validity date does not match the packaging, which might eventually hurt people somehow. Intermediate product tracking systems presented to intentional and accidental change, will lead to the exaggeration of information, all of which push to a proposed approach to solve these problems [4].

Supply chain is used to manage the flow of services and products, which starts from the origin of products, ending at the eventual consumers. The compromise of moving and storing for raw material are also part of the procedure. Supply chain management mainly aims towards monitoring and ensuring that the products are produced, distributed and shipped properly[5].

1.2 Related works

There are many supply chain systems that have been proposed or implemented in different fields. Below are some of recent literature reviews:

Erik-Oliver in 2010 [6] proposed a protocol to verify how genuine objects are using a Radio-frequency identification (RFID) based supply chains called Tracker. It provides security by identifying which legal path an object/tag takes throughout a supply chain. On the other hand, it provides a privacy whereas the adversary cannot learn details about an object’s path within supply chains. Both security and privacy of Tracker are determined by extensions of polynomial signature techniques to detect run-time faults by means of homo-morphic encryptions.

Mira Trebar in 2013 [7] proposed the temperature monitoring by using RFID technique for tracing fish supply chains. The data loggers of RFID are located on the box in order for measuring the ambient temperature of product, while it can be placed inside the box to measure the temperature of the product itself. The developed system is very effective through the stages of transporting and storing fish to improve the quality control. The sensor data will be checked by mobile RFID readers after which they are stored within the system database so as to be available for consumers and stakeholders.

Pranav, etal [8] presented a model which accounts for the basic cost components, pumping, and refinery expenses in the transportation network of the oil and gas industry. Given the necessity for reducing expenses and decreasing the environmental emissions, the different transport supply chain techniques offer a solution through the application of a linear program model. The model is optimized for creating a better understanding of the key factors required to update the supply-chain managements.

Although the limited researches in the field of pharmaceutical supply chains, the work in **Kapoor in 2018** [9] proposes a system for pharmaceutical companies which provides medicines in the acceptable quality and the accurate quantity, to the correct location and consumers within the set time-span and optimal costs. This is essential to meet the goals of health systems and at the same time to make benefits for its stockholders. The proposed system should decrease the risks in pharmaceutical companies, as it involves processes like optimizations, productivity augments and reducing business risks.

TOMY PERDANA in 2018 [10] propose another study which focuses on the improvement of performance for pepper supply chain using Value Stream Mapping (VSM). VSM is used to enhance the production efficiency and effectiveness, and to reduce the waste in production system. The study depends on operational coordination and analytical framework for dealing with logistics problems that occur in the chili pepper supply chain. The results show the effectivity of implementing VSM to resolve this issue.

Purwandoko et al. in 2019 [11] they proposed a smart IT based traceability system to solve the problems in rice supply chain in Indonesia using SDLC (System Development Life Cycle). This system was based on data flow diagrams, system architecture, and database designs. The elements that play a main role in this supply chain are: farmers, industries, distributors, and retailers. The developed system shows that the production activities meet the operational standards. Moreover, it facilitates the decision-making process in agricultural industries.

Lisitsa, Levina, and Lepekhin in 2019 [12] took into consideration the essential factors in supply chains needed for the reduction of expenses and increase of the company's overall profits in the oil industry. These include managing the demands, distributing petroleum products efficiently, better scheduled transportations, managing the warehouses, and the automation of the supply chain. The supply chain management is the main frame through which this framework in deployed.

Saing et al. in 2019 [13] they compared the features and performance rates of dry and wet cocoa bean supply chains. The supply chain performance is analyzed in a qualitative descriptive manner by means of the FSCN (Food

Supply Chain Networking) framework. The obtained results show that there are two cocoa bean supply chain models in East Luwu District: Dry Cocoa Bean Supply Chain and Wet Cocoa Bean Supply Chain. The first involves: farmers, collectors, wholesalers and exporters/processing industries, whereas the second involves farmers, collectors and purchasing units. The second chain performed more effectively and efficiently with a marketing margin of IDR 31,200 per kilogram and a farmer's share of 100%. It can therefore be used as a role model in the cocoa agribusiness activities in South Sulawesi.

Chilur Omkarappa in 2019 [14] this study made comparisons between sanitized and sanitized retail table eggs which originally come from commercial eggs (retailed with no form of cleaning, sanitization, or packaging) farms. About 1120 eggs obtained from retail markets have been analyzed for physico-chemical and microbial characteristics such as (shape, color, shell thickness, weight, yolk index, Haugh unit, albumen index, and pH), (yeast, mold counts, and total viable count), respectively. The result shows that eggs collected from retail markets are totally different in terms of physico-chemical features. Also, processed eggs have better microbial quality characteristics than unprocessed ones. Processed table eggs undergo healthy treatment and cold storage, so as to provide consumers with healthier eggs.

Shaniar Tahir Mohammed in 2020 [15] has suggested an electronic supply chain system for recording the transactions according to the block-chain technology. These recordings consist of three stages. First, all the parties are represented as clients with unique ID in the Block-chain network. Second, all the information on a certain type of drug is recorded within the transaction with a signature. Finally, all drug transactions are registered within blocks that have a unique identity each. Furthermore, some of the cryptography

mechanisms have been implemented such as RSA (Rivest Shamir Adleman) and SHA (Secure Hash Algorithm). The proposed system aims to protect the drugs from alterations and to ensure its reliability and trust, in addition to providing real-time tracking for the transactions of parties.

Table 1. 1: A summary of related works

Authors	Method	Dataset	Evaluation	The Proposed Work
Blass, Elkhiyaoui, and Molva [6]	RFID tracker	DB clone	▪ Security ▪ Determines the exact path ▪ Privacy-preserving	Sets of valid paths and valid states are presented for pharmaceutics or luxury objects supply chains datasets
Trebar, Lotric, Fonda, Pleteršek, and Kovalil [7]	RFID	Sensors database	▪ Quality control ▪ Efficient storage ▪ Ensures food safety for consumers	The temperature monitoring solution is presented at the box level in fish supply chains.
Joshi, Haghnegah Anika, and Singh [8]	RFID	RFID data	▪ Optimization ▪ Logistics	It reviews different supply-chain techniques currently within the petroleum industry.
Kapoor and Dadarwal [9]	RFID EPC	-	▪ Data accuracy ▪ Operation complexity reduction ▪ Supplier selection ▪ Ware housing ▪ Distributing	Limited research conducted on pharmaceutical supply chains is presented.
Perdana, Hermiatin, Pratiwi, and Ginanjar [10]	Value Stream Mapping (VSM)	Quantitative data	▪ Improved effectiveness ▪ Minimized risk in production, ▪ Eliminates waste ▪ Safety and responsive ▪ Improved production costs	It develops the chili pepper supply chain performance.

Purwando, Seminar, andSugiyanta [11]	SDLC	MySQL	▪ Ensures the quality and safety of food	The system architecture and traceability system design are developed using a data flow diagram(DFD).
Lisitsa, Levina, and Lepekhin [12]	SCM software	-	▪ Managing demands ▪ Distributing products efficiently ▪ Better scheduled transportations ▪ Up to date information via supply chain automation.	It investigated the need of supply-chain management in the oil industry.
Saing, Arsyad, Mahyuddin, Munizu, Nuddin, and Jamaludin [13]	FSCN analysis	Quantitative data	▪ Quality	The features and performance of dry and wet cocoa bean supply chains are compared
Omkarappa, Fairoze, Chakkoda, Bhave, And Karabasanavar [14]	Haugh unit (HU) based digital pH-meter analysis	Table egg samples	▪ Processing	The retail outlets eggs undergo physicochemical and microbial quality analysis.
Shaniar Tahir Mohammed, Jamal Ali Hussien [15]	RSA and secure hash algorithm SHA	Database system DBs	▪ Monitoring ▪ Reliability ▪ Traceability	An approach is used to protect drugs from counterfeiting.

1.3 Problem Statement

1. The problem in the current supply chain is the possibility of modifying the private database because it is central to security breaches or lack of credibility of the company manager.

2. The lack of information on the product origin and the inability to track its source within the supply chain may cause the product to be damaged in one way or another.
3. For example, patients who have allergies or are diabetic affected by inaccurate food information. Also, the validity date may not match the box and its cover.
4. Further, central tracking systems of products could be exposed to intentional and unintentional change, which lead to information of no accuracy.

1.4 Research Objectives

The main objective of this research is designing a supply chain traceability system by means of some security methods like HMAC, which comprises RSA and SHA512. These contracts enable manufacturers to present a definition of the product composition and trace its origin and so as to prevent it from manipulation. It is also another way to increase company's competition. It provides high transparency in product quality and integrity regarding working conditions. Moreover, it reduces the disqualification of fraud in larger packages, particularly critical material.

1.5 Thesis Structure

This thesis is organized as follows:

- It is a theoretical background about the research subject, the research methodology is explained, establishing the involved research model. It also involves the investigation of the research questions and outlines various methods of data collection.

- Chapter Three explores some of the key difficulties that occur and presents the proposed system. It illustrates the practical stages of the system, and explains the proposed chess supply chain method and a Secure Approach for process to explain each step in this work.
- Chapter Four introduces the results and evaluates the proposed system. It shows the practical section of the thesis and determine the expected results.
- Finally, the conclusion and future work are discussed in Chapter Five.

Chapter Two

THEORETICAL BACKGROUND

Chapter Two

Theoretical Background

2.1 Introduction

The previous chapter illustrates research introduction, problem statement, structure and related work. This chapter provides a theoretical background about supply chain. Furthermore, some encryption methods that can be used to secure and validate the data are presented.

2.2 Supply Chain

The latter involves each of the manufacturers, suppliers, logistic flow transporters, warehouses, retailers, and customers themselves. Supply chains are involved in a number of fields such as new product growth, marketing, administration, finance, and client service. These systems administrate the flow of products staring at the raw material stages and continuing all along to the final product's consumption. Supply chains mainly aim towards monitoring and reporting the details related to the different stages of production, delivery, and purchase of products and services [16]. Figure (2.1) represents a general supply chain in light of the total supply chain networks. Every firm is part of minimally one supply chain, as it often has more than one supplier and consumer. The common view on a supply chain is the cycle view, whereby every cycle performs at interfaces of two successive stages within supply chains. This implies the decoupling of cycles from others by means of indices to ensure their autonomous operation, eventually enhancing its overall performance [17].

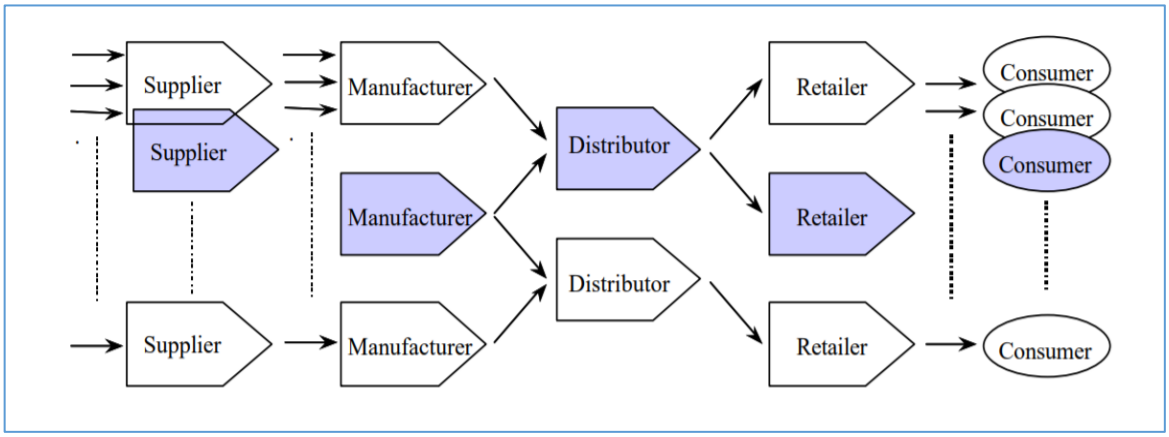

Figure 2. 1: Schematic diagram of supply chain network

2.2.1 Types of Supply Chain

The common uses of supply chain are in industrial companies. In traditional companies, the supply chain is more complicated because the items that provided are saved in warehouses and other locations. However, when the company uses another model like make to order, there is no need for storing completed products, but raw materials and elements should be stored. Therefore, it depends on the nature of the company [18]. The following are the common models of supply chain [19].

1- Integrated Make to Stock

This sort has the main focus on tracking the demands of customers in real-time in order to restock the completed products inventory in efficient way. Sometimes, this integration is achieved by using the fully integrated information such as enterprise systems. Consequently, the organizations develop and update schedules and production plans by receiving a real-time demand information. This type is exemplified by means of Starbucks Coffee (starbucks.com). The last makes use of multiple distribution channels because it deals with many businesses such as supermarkets, department stores, and

airlines. The Sale process is done through the Internet using direct mail. Here, the supply chain with multiple distribution channels must work with maximum effectiveness and reasonable cost. Furthermore, it requires accuracy in information flow and time about demand, storage capacity, inventories, and transportation scheduling. Therefore, hundreds of business partners should work with Starbucks.

2- Build to Order

The second type of model involves the company collecting the orders of customers as soon as the order is received. The delivery of needed supplies and the component inventories in this type requires a careful and accurate management along the supply chain. In order to resolve this potential problem, many common components should be utilized across several locations and several production lines. Among the key advantages of this type of supply chain is supporting the concept of mass customization whereas all customers rapidly receive their personalized products.

3- Continuous Replenishment

This type of supply chain model should be working closely with intermediaries/suppliers in order to constantly refill the inventory. However, if the process of refilling inventory has many shipments, the supply chain will collapse and the cost may be very high. Therefore, a strong integration is needed between production process and order-fulfillment process. In order to maintain the required replenishment levels and schedules, the information about demand changes should be provided at real-time in the production process. The environments which have a stable demand of patterns are the

most suitable and applicable to this model such as the distribution of prescription medicine.

4- Channel Assembly

The channel assembly model is an updated form of the order model. The product elements are collected and while the product itself is moved via the distributing channels with the help of 3PL (third-party logistics) firms. Sometimes, these services consist of either a collection of completed components or physical assembly of a product at 3PL facility for delivery to the customer.

2.2.2 Functional Attributes

The functional attributes of entities can be categorized into four types [20]:

- Procurement,
- Production,
- Distribution
- Sales type

1. Procurement

This is related to the number and nature of the product to be procured. It ranges from standard to very specific products which might require information, producing procedures, or equipment. This attribute is related to the type of sourcing, which may be wither single or multiple. The former is found whenever a unique supply needs to be produced for particular products. As for the double source, it involves two suppliers that fulfill portions of demands for the product procurement (60% by the main supplier and 40% by

the secondary). Another significant aspect is the supplier flexibility with regards to the amount of products to be supplied. These amounts can be either fixed or they may range between given minimum and maximum limits, based on the availability of the supplier contract. There is a close relationship between the supplier lead and reliability. The first sets the average time interval that separates the order of materials and their arrival time. A negative correlation exists between the lead and re reliability, as shorter lead times will lead to reliable promises of arrival dates. As for the life cycle, this affects the risk of obsolete inventories, as short cycles require the repetitious substitution of old materials.

2. Production

There are several attributes that determine the production types, particularly the way in which the production process is organized and the representation of operations. The way in which the product is organized, in addition to the flow lines are common characteristics of the production procedure.

3. Distribution

The products are distributed across the networks so as to bundle the shipment and at the same time decrease transportation expenses. Such networks often operate through external entities, and their types can be classified based on the designing issues involved from both perspectives (manufacturers and carriers).

4. Sales Type

This type of attributes deals with fulfillment, billing and cashing orders. Their optimization involves the automatization of order processing by means of EDI software and other technologies, for the direct capturing of order data. The reduction in time eliminates the need for the manual generation and sensing POs and invoices. Since no orders are taken down and processed manually, it also decreases the human error rates.

2.2.3 Examples of Supply Chain

1- Generic Supply Chain

Generic supply chains start by sourcing and extracting raw materials, which are later used by logistics providers to suppliers, so as to serve as wholesalers. The elements are taken to different manufacturers to improve and process them into a finished product. Ultimately, it is further sent to a seller who wholesales the finalized product to be presented to retailers. The retailers sell the goods in stores to customers. Whenever the customer buys the products, the cycle is completed. The demands of customers require more raw materials to be processes, so that the cycle resumes [21]. Figure 2.2 shows the generic supply chain cycle.

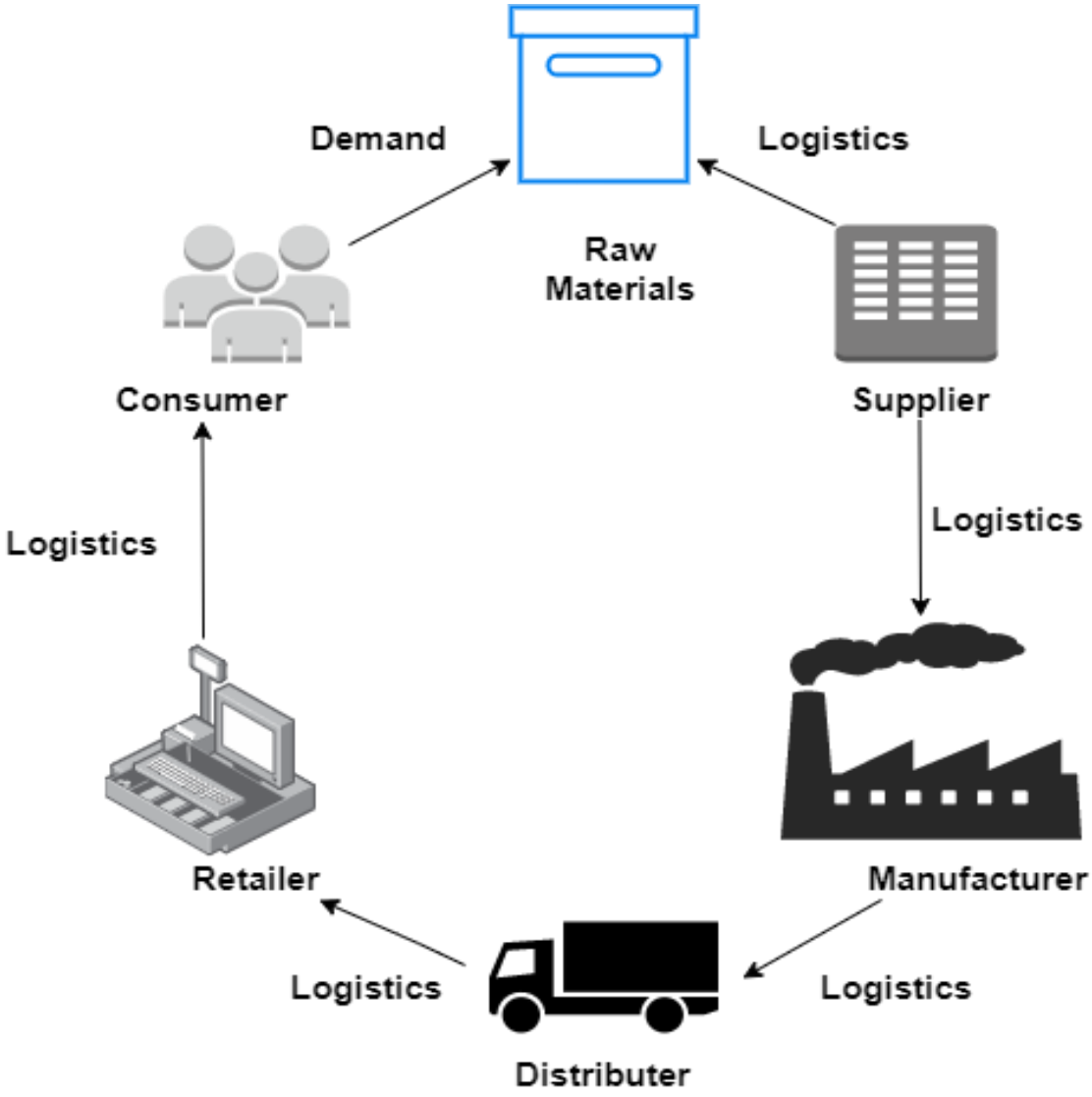

Figure 2. 2: Generic supply chain cycle

2- Supply Chain for an e-Commerce Company

For the purpose of explanation, the e-commerce company runs a website in which different products are sold. Consumers can place orders for different products, which are in turn prepared through a check-out cart, or a third-party such as Shopify. Next, the payment processors develop a cash transaction for the orders, thereby creating a new supply chain. Payment processors often involve the application of third parties like PayPal, Stripe, and banks. When goods orders are placed, the repository takes them and ensures that the

products are ready for dispatch. Warehousing companies could be in-house or third-party logistics providers. The order proceeds from the warehouses to the transportation companies, which also could be in-house or third-party. After shipping, the packages are delivered to the consumers, as shown in Figure 2.3 [22].

Figure 2. 3: Supply chain for e-commerce company

2.3 Supply Chain Scalability Through SCI

Alternatively, the scalability can be achieved by means of the integration of primary and secondary members within the supply chains. The collective collaboration and quick scale up are essential for meeting the demands. Scalability can be analyzed through SCI, which represents the highest level of relations shared by members with supply chains. Coordination is used for developing the theoretical framework. An essential part of the aforementioned activities in SCI is sharing of information, and they are

observed in the data on the Kenyan nutrition supply chain. Since SCI ensures the agility of humanitarian supply chains, it is a major contributor to scalability. The DCV Supply-chain integration is considered to be RC representing the ability to provide scalability and contribute to supply chain resilience [23].

2.4 Performance Metrics

There are three essential dimensions involved regarding the performance of supply chains:

- Service
- Assets
- Speed

Service is related to the ability to anticipation, capturing, and fulfilling of customers' demands using personalized products and punctual delivering times. **Assets** are related to the values of products commercially, especially inventory and cash. As for **speed**, it involves time-related metrics such as how responsive the chain is and how fast the procedures are executed. All supply chains require at least a single performance measure for each of the three aforementioned dimensions [24].

2.5 Cryptographic Algorithms

The Secure Hash Algorithm (SHA) can be defined as a cryptographic has function which is used in securing the date through its transformation into hash codes. It deploys a set of algorithms, including SHA1, SHA224, SHA256, and SHA512, which differ in sizes and length (bytes) [25]

As for the RSA cryptographic system, it is mainly of use in encrypting data followed by decrypting it through two keys (private and public). The private key belongs to the owner, whereas the public one can be accessed by the public. The RSA key size is over 1024 bits, whereby the public key encrypts the message and the private one decrypts it [15].

2.6 Cryptography Mechanisms

Cryptology is one of the fields that examine the ways of communicating safely. It involves several sub-branches, like cryptography and cryptanalysis. Cryptography mainly deals with the design of algorithms for encrypting and decrypting so as to ensure that the messages remain confidential and authentic. This branch does not only provide information security. In fact, its techniques can be considered as an art of maintaining secure communications. As for cryptanalysis, it mainly deals with the decryption of messages after encryption, also known as cipher text, to obtain or forge information to ensure its authenticity. Cryptography involves three fundamental aims [25]:

- **Confidentiality:** It secures the information from all with the exception of the users who are authorized to access it.
- **Data Integrity:** It secures unauthorized data changes by detecting any attempts of data manipulation such as inserting, deleting or substituting data.
- **Authentication**: It identifies whether the location to which the data is addressed is authentic.

The cryptographic system consists of three dimensions:

a) The method of transforming plain text onto cypher text. Encryption is determined by two fundamental principles: substitution and

transposition. The first maps the elements of the plain text along with other elements. The second rearranges the elements of the plain text. The majority of systems include several substituting and trans-positioning levels.

b) The type of key used determines the kind of system. Conventional encryption, also known as symmetric systems, involve the same key being used by the sender and the receiver. The public key encryption or asymmetric systems, on the other hand, uses a different key for each of the sender and receiver. It is also known as dual key encryption.

c) The plain text can be processed through two methods. In block ciphers, a single block input is processed and a single lock output is produced. The stream cipher involves the continuous input of elements after which a single element is produced.

There are two basic techniques for encrypting information:

- Asymmetric or public key cryptography
- Symmetric or secret key cryptography

When encrypting and decrypting messages, the key is necessary for maintaining that the algorithm operation remains confidential. Encryption algorithms are of two types:

1. In **symmetric algorithms**, the same key is used in the encryption and decryption process. It is also known as a one-key or secret key algorithm. From a mathematical point of view, this type of algorithms can be represented in the following way.

   E= Encryption

   K= secret key

D= Decryption

M= message

C= Cipher text

Encryption: **EK(M) = C** ……(2.1)

Decryption: **DK(C) = DK (EK (C)) = M** ……(2.2)

2. In **asymmetric algorithms**, a different key is used for each of the encrypting (public key) and decrypting (private key) processes. Since the key for encrypting is public, it has a public distribution. Meanwhile, the key for decrypting is private, and the overall validity and confidentiality are determined by how secure the private key is.

In comparison with symmetric algorithms, the asymmetric algorithms make use of loner keys that are of greater value. However, they tend to require more time and their efficiency appears only when smaller amounts of data are processed.

Public key cryptography, as follows:

- Public key encrypting: messages that undergo public encryption cannot be decrypted unless the private key users are submitted.
- Private key encrypting: messages that are marked using the private key may undergo verification by users that have the public key, so as to ensure that no alterations have been made to the content of the messages.

From a mathematical point of view, asymmetric encrypting and decrypting process algorithms can be represented in the following way [25]:

Encryption: **EK1(M) = C**

Decryption: **DK2(C) = DK2 (EK1 (C)) = M**

2.6.1 Hash function

Hash functions can be defined as tools for protecting that the information is authentic. Hash functions are found to be of use in building blocks for solving other security issues in tele-communication and computer networking. For example, it is used to detect un-authorized modifications to important messages by malicious users or computer viruses. Cryptographic hash functions perform deterministic procedures which turn arbitrary blocks of data into fixed-size bit strings. Usually, the encoded data is called message digest. Other applications of hash functions include digital signatures, message authenticating codes, pseudo-random functions, and data finger-printing [26].

2.6.2 Secure Hash Algorithm (SHA)

The Secure Hash Algorithm (SHA) can be defined as a cryptography hash function applied for digital certificates and data integrity. SHA represents a fingerprint with specific data developed by N.I.S.T. to be part of the U.S. Federal Information Processing Standard (FIPS). It mainly deals with messages of less than 264 bits in length. The message digest output is 160 bits (32 bits more than MD5) [27].

SHA deploys a set of algorithms, including SHA1, SHA224, SHA256, and SHA512, which differ in sizes and length (bytes) [25]

- **SHA1**

  SHA1 produces a 160-bit (20-byte) hash value, typically rendered as a hexadecimal number, 40 digits long. SHA1 is the most widely used of the

existing SHA hash functions, and is employed in several widely used applications and protocols. The SHA1 algorithm might not be secure enough for ongoing use. It is recommended not to use SHA1.

- **SHA224**

  SHA224 produces a 224-bit (28-byte) hash value, typically rendered as a hexadecimal number, 56 digits long.

- **SHA256**

  SHA256 produces a 256-bit (32-byte) hash value, typically rendered as a hexadecimal number, 64 digits long.

- **SHA384**

  SHA384 produces a 384-bit (48-byte) hash value, typically rendered as a hexadecimal number, 96 digits long.

- **SHA512**

  SHA512 produces a 512-bit (64-byte) hash value, typically rendered as a hexadecimal number, 128 digits long.

2.6.3 Rivest-Shamir-Adleman (RSA)

RSA can be described as the most commonly used asymmetric cryptographic algorithm applied in the encryption and decryption of messages through modern computers. It generally uses a public key algorithm, and it is most often found to be applied for enhancing the security of communicating channels and digital signatures. The algorithm of RSA includes both private

and public keys. The public key is known to anyone, as it is used for encrypting the messages from plain text to cipher text. These messages could only be decrypted using the corresponding private key. The security and reliability of the algorithms are determined by the process of generating keys, as it seems to be related to how complex they are in comparison with other cryptographic algorithms [25].

2.6.4 Hash-based Message Authentication Code (HMAC)

HMAC represents a cryptographic tool that is applied to verify transferred data between client and server by using a secret key for both sides, making it difficult to be attacked through common attacking methods. In HMAC, both clients and servers are provided with the private and public keys. The public key accessible to all, whereas the private key is given to the specific servers or clients. The client uses a HMAC for all requests by combining the hashing and request data together through a private key, after which it is transmitted as portion of a request to server. The server receives the request, and regenerates a unique HMAC [28].

The main equation of HMAC is defined as follows:

$$HMAC_K(m) = h\big(K^+ \oplus Ipad, h(K^+ \oplus Ipad, m)\big) \dots\dots (2.3)$$

HMAC could be obtained by means of the steps presented below:

1. The K^+ is obtained through padding zeros onto K's left side for increasing the length to b-bits.
2. S_i of b-bit length us calculated through XORing ipad with K^+.
3. S_i is concatenated with m in order to equal m' .
4. The message digest h(m') is calculated for m' through h.

5. S_0 of b-bit length is calculated through XORing opad with K^+.
6. h(m') is concatenated with S_0 so as to equal m''.
7. The message digest h(m'') is calculated for m' through h for obtaining the final results of HMAC.

2.7 RSA Digital Signature

Initially, the RSA algorithm was developed in 1977 at the Massachusetts Institute of Technology (MIT) by Rivest, Shamir and Adelman. The RSA concept depends on factorizing big numbers. This implies that larger number sequences will provide more protection. RSA cannot be broken by an adversary because of the fact that its keys are large and complex. RSAs are used for encrypting and decrypting data, as well as verifying packets. No specific hash function is required in RSA. Therefore, the type of hash function does determine the security of the signature to a particular extent. The security depends on the intractable complexity of a large composite integer n = p*q, whereby p and q require distinct large primes.

Being an asymmetric digital signature algorithm, RSA depends on the one-way trap-door function. This makes it easier to multiply prime numbers but difficult to factor. The multiplication can be computed in polynomial time. As for the factoring time, it increases through exponential proportions until it reaches the number size [30]. The algorithm can be described in the following way:

- **Key Generation**

- **Signature Generation**

The essential steps to generating signatures are as follows:

1. A message digest H (m) is created as an integer of information to be sent between 0 and n − 1.
2. The signature is computed through private key d as $s = H(m)^d \bmod n$
3. (s) represents the signature of the message m, which is sent along with the message m to recipient.

• Signature Verification:

The essential steps to verifying signatures are as follows:

1. Though the sender public key e, the integer $v = s^e \bmod n$ is computed. It represents the message digest obtained through the sender.
2. The message digest of the signed messages is computed in an independent manner.
3. The validity of the signatures depends on how identical both message digests are.

2.8 Conventional Digital Signature Schemes

Digital signatures (DS) are efficient techniques to ensure that the data is authentic, integral, and non-repudiate within open networks like the Internet. This type of verification methods demand the signature holder to hold two keys: a private one (signature key) to sign messages and a public one (verification key) to verify that the messages are authentic, as shown in Figure 2.4. DS mainly aims towards verifying that no modification occurs to the message while transmitted. It also ensures the receiver that the message is indeed sent by the expected party. With its initial introduction in 1976 by Diffie and Hellman, the first practical system was the RSA DS scheme proposed by Rivest et al. (1978). This was followed by the creation of other schemes like ElGamal and undeniable signatures.

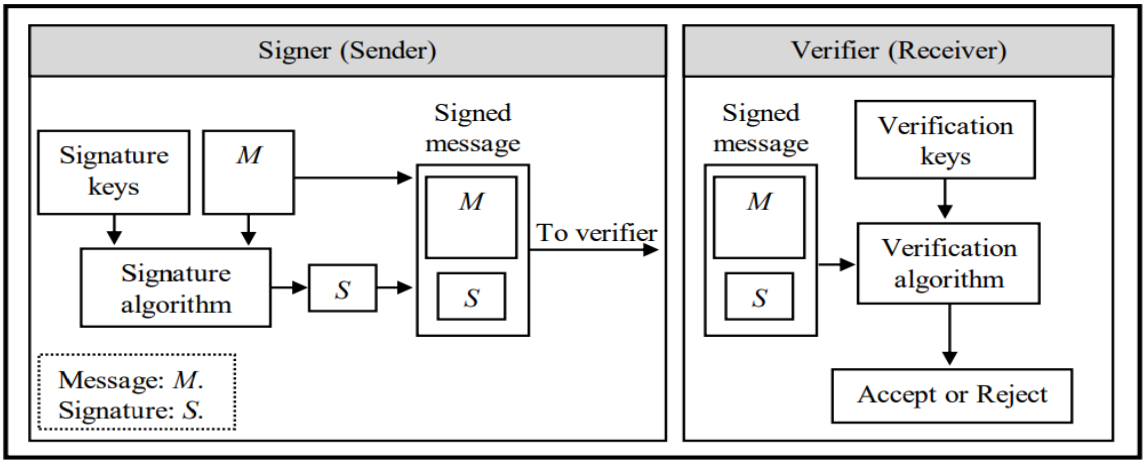

Figure 2. 4: The digital signature scheme

The majority of present day DS schemes depend on how difficult it is on a mathematical level. The most complex mathematical issue is the integer factorization (RSA DS scheme), and discrete logarithms (Digital Signature Algorithm - DSA) [31].

2.9 The RSA digital signature scheme

The majority of applications of RSA are found in key exchanging, encrypting, and digital signatures. The RSA-DSA makes use of a private key to sign original messages and a public key to verify them. Figure 2.5 illustrates the RSA DS scheme whereby signed messages are transferred to the receiver. The content of the received message is verified by computing new verifying values using the signed message plus the signer's public key. This is followed by comparing the verification values to the one of the received messages. In case both values are the same, this ensures the verification and authorization of the message originally sent. Otherwise, the signature is invalid. The RSA security is determined by how difficult the integer factorization is to be computed [31].

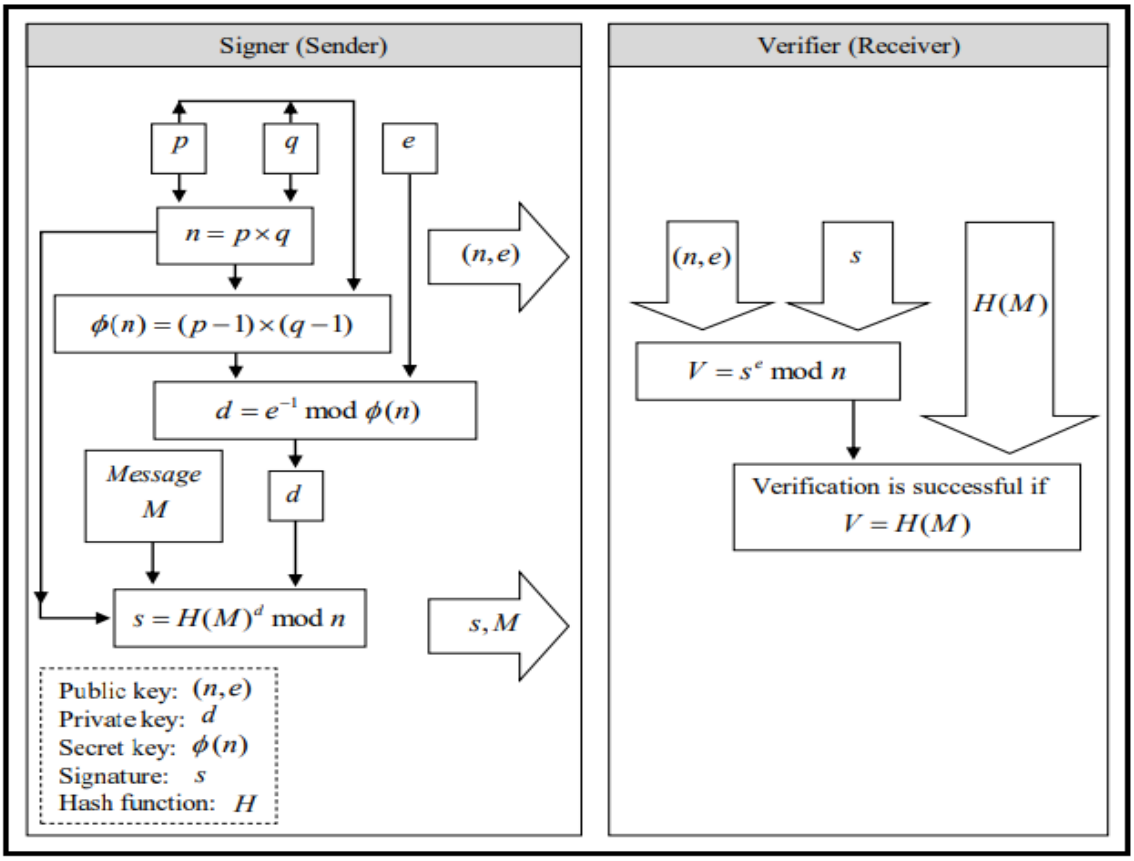

Figure 2. 5: RSA digital signature scheme

The signing of data is done using RSA-SHA1-1024 and HMAC.

2.10 Django

It is a framework for building and developing the Python web in a fast and high-end design. This framework was developed by professional developers in this field and it is available in a free and open source format. In this work the current framework is implemented to build a Python web and make it available to the end user by browser. Figure (2.6) shows the Django framework infrastructure [32].

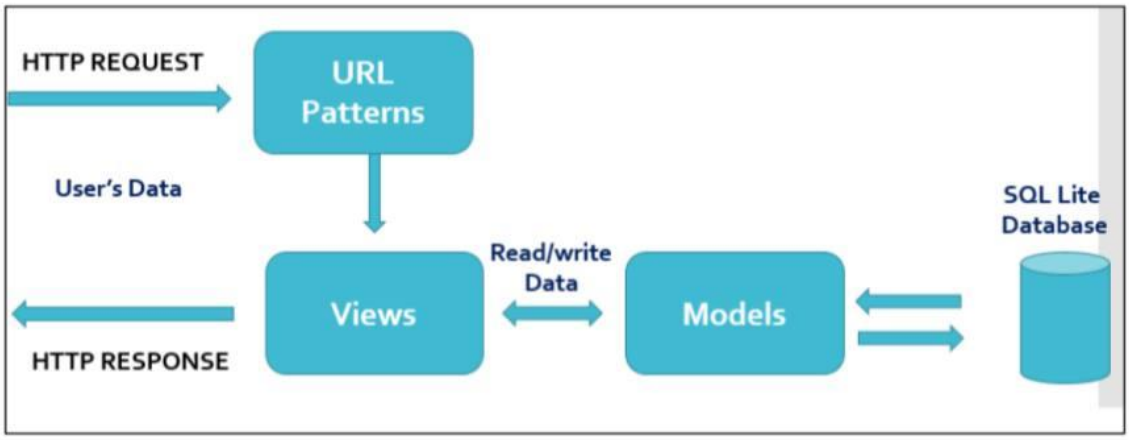

Figure 2. 6: Django framework infrastructure

2.11 Summary

This chapter described the theoretical background of the thesis as follows: First, an introduction is presented to clarify what subjects will be discussed. The second section provides a basic background about supply chain concept, types, and its applications. Then, some of security cryptography mechanisms is 0020xpresented. The next chapter discuss the practical part of the thesis which is represented by designing a traceability system for products based on supply chain technique.

Chapter Three

THE PROPOSED SYSTEM AND METHODOLOGY

Chapter Three

The Proposed System and Methodology

3.1 Introduction

This chapter present the main methodology for the proposed system by using supply chain for tracking the products with an authenticated approach where the proposed system consists of three stages: the first stage describe introduction to the topic The second stage illustrates the proposed system in details The third stage proposes the supply chain The fourth stage deals with the dataset and saved into a database with type of SQLite The fifth stage shows the using of some security cryptography methods. The final stage is the evaluation stage, user query, and conclusions. Then, implementing the same steps using JotForm platform and the role of DLT in sharing data cross multiple nodes.

3.2 Proposed System

The system is produced based on four central identities: farmer, factory, distributor, and marketer (retailer). Each identity is able to embed product information to supply chain stages. The farmer starts by inserting the product's central information when it enters the factory these data is updated with other data related to the product. Moreover, secure the product reaches the distributor, previous information updated over to have the product's information in this step secure the product reaches of distributor to marketer. Finally, the retailer would be able to present and obtain all preceding information. Every integrity has set of records building into a database then assembled to make distributed ledger. Indeed, what was mentioned represents the supply chain. Retailer would be able to view

product features and trace information. The following flowchart in Figure 3.1 explains the proposed system process.

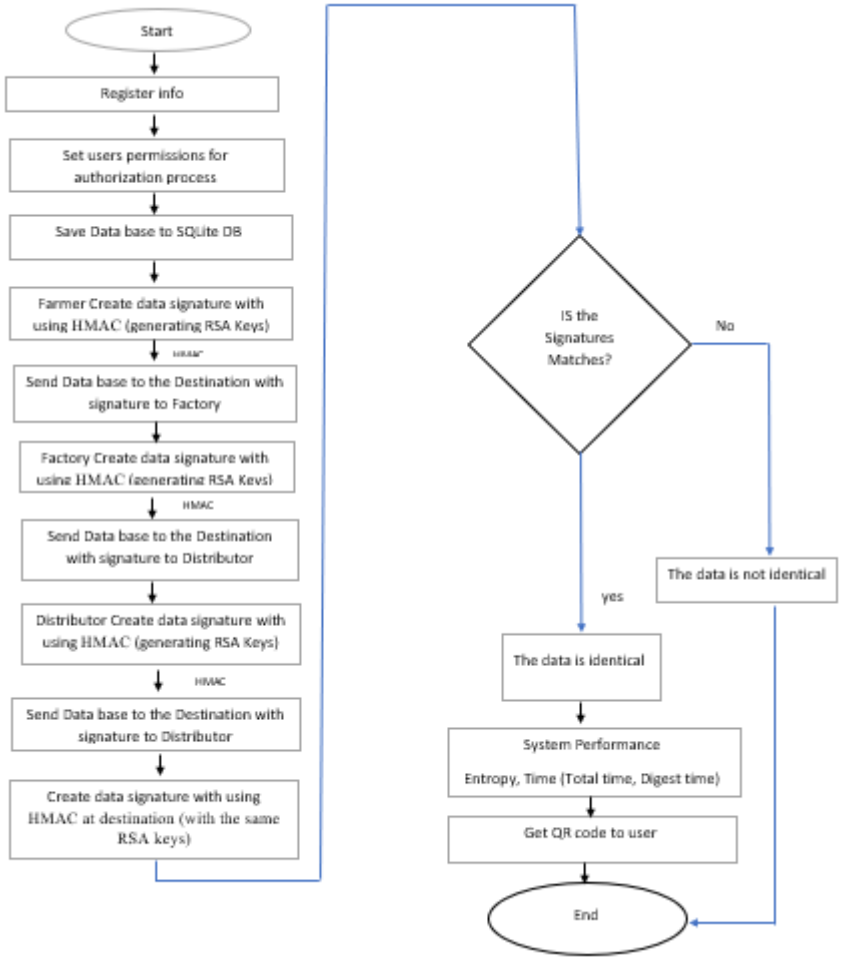

Figure 3. 1: Block diyan proposed work

3.3 General view of the Proposed System entities

When signing in using the Admin account, there are two interfaces, namely the main interface for the web service and the admin interface. The admin account is authorized with all the permissions. The current admin interface shows the control panel from which new users can be added and new accounts can be created by the admin. A new user account can be created by going to Activity, and then to Create New Account or Edit Account.

The Admin has permission to observe the activity of other users on the platform, as well as displaying all product with their full details (location, date, condition). There are four authorization groups that can be created by the Admin: Farmer, Factory, Distributer, Marketer. Each of these groups has a particular authorization. The Farmer groups represents the farmers, the Factory represents all the industrial members and factory owners. As for the Distributor, it involves all users who are in charge of distributing the products, and the Marketer is the group for the users who works on the product marketing. Table (3.1) shows the types of user's groups.

Table 3. 1: Group's Identification

Id	Name
1	Farmer
2	Factory
3	Distributor
4	Marketer

The foreign keys are assigned to the users so as to classify them into the four groups identified in Table (3.1). For example, users that are assigned

(permission 2) belong to the group of Factory, and those who are assigned (permission 3) will be part of the Distribution group.

Table 3. 2: Authentication group permission

Id	Name	permission
1	1	1
2	1	2
3	1	3
4	1	4

After categorizing the users into the predetermined groups, each user will have certain permission based on the group they belong to, whether they are part of the farmers, Factory, Distribution, or marketing groups.

Table 3. 3: The admin assigns permissions to the users

Id	permissions	Codename	Name
1	1	add_logentry	Can add log entry
2	1	change_logentry	Can change log entry
3	1	delete_logentry	Can delete log entry
4	1	view_logentry	Can view log entry
5	2	add permission	Can change permission
6	2	change permission	Can change permission
7	2	delete permission	Can delete permission
8	2	view permission	Can view permission
9	3	add group	Can add group
10	3	change group	Can change group
11	3	delete group	Can delete group
12	3	view group	Can view group
13	4	add user	Can add user

14	**4**	**change user**	**Can change user**
15	**4**	**delete user**	**Can delete user**
16	**4**	**view user**	**Can view user**
17	**5**	**Add content type**	**Can add content type**
18	**5**	**change_contenttype**	**Can change content type**
19	**5**	**delete_contenttype**	**Can delete content type**
20	**5**	**view_contenttype**	**Can view content type**
21	**6**	**add session**	**Can add session**
22	**6**	**change session**	**Can change session**
23	**6**	**delete session**	**Can delete session**
24	**6**	**view session**	**Can view session**
25	**7**	**add contract**	**Can add contract**
26	**7**	**change contract**	**Can change contract**
27	**7**	**delete contract**	**Can delete contract**
28	**7**	**view contract**	**Can view contract**
29	**8**	**add product**	**Can add product**
30	**8**	**change product**	**Can change product**
31	**8**	**delete product**	**Can delete product**
32	**8**	**view product**	**Can view product**
33	**9**	**add question**	**Can add question**
34	**9**	**change question**	**Can change question**
35	**9**	**delete question**	**Can delete question**
36	**9**	**view question**	**Can view question**
37	**10**	**add choice**	**Can add choice**
38	**10**	**change choice**	**Can change choice**
39	**10**	**delete choice**	**Can delete choice**
40	**10**	**view choice**	**Can view choice**

The Farmer is the only one which has the permission to add new products to the system, along with the related product details and conditions (temperature, humidity, etc.). The Factory group Can also add information related to the product condition, date of parking, time of processing, date of expiry, current temperature, and others.

In order to ensure that the product is safely transmitted from the farmers to the factory, the HMAC and RSA encryption algorithms are used generate a signature. This ensures that the product and/or product information has not been altered.

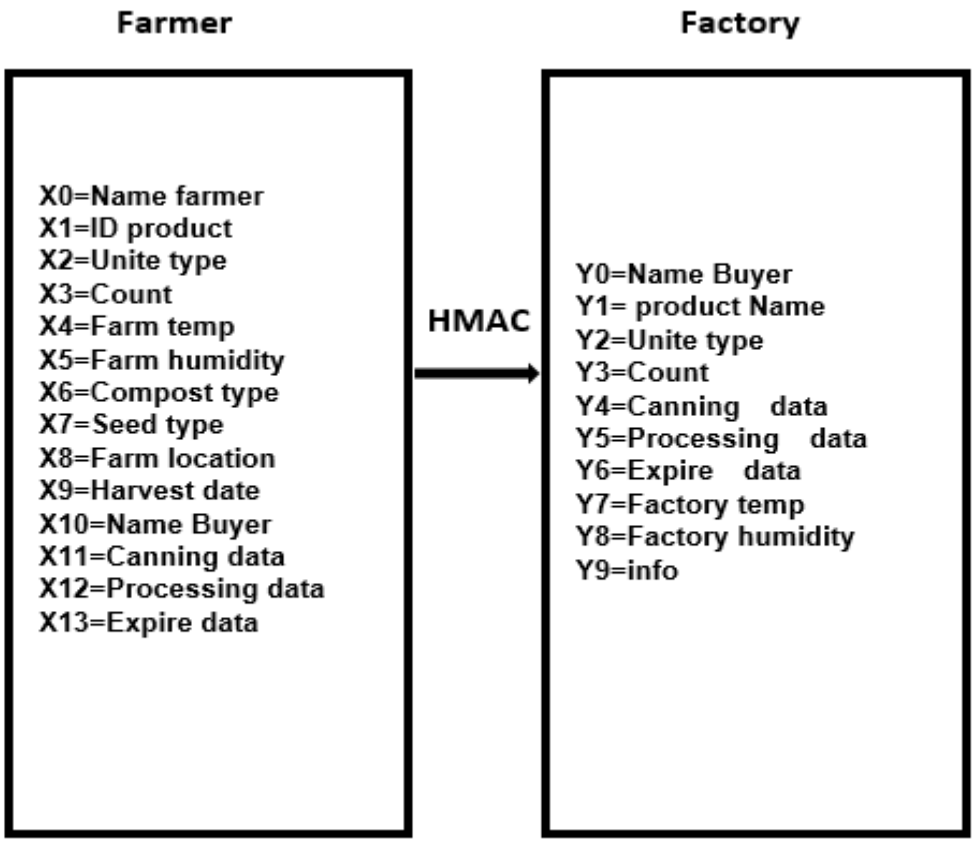

Figure 3. 2: Supply chain and secure to farmer to factory

The factory adds all the details and information related to the product itself as well as the conditions through which the product goes until it reaches the Distributor. The Distributor, in turn, adds the condition details that the product goes through when being distributed, such as the date of distribution. The encryption algorithms are applied to the factory-distributor stage to ensure that the product is transported safely and securely, with no chance of alteration.

All the information that the factory owner needs to share with the distributor are secured by means of a signature formed through the RSA and HMAC algorithms, until they reach the distributor.

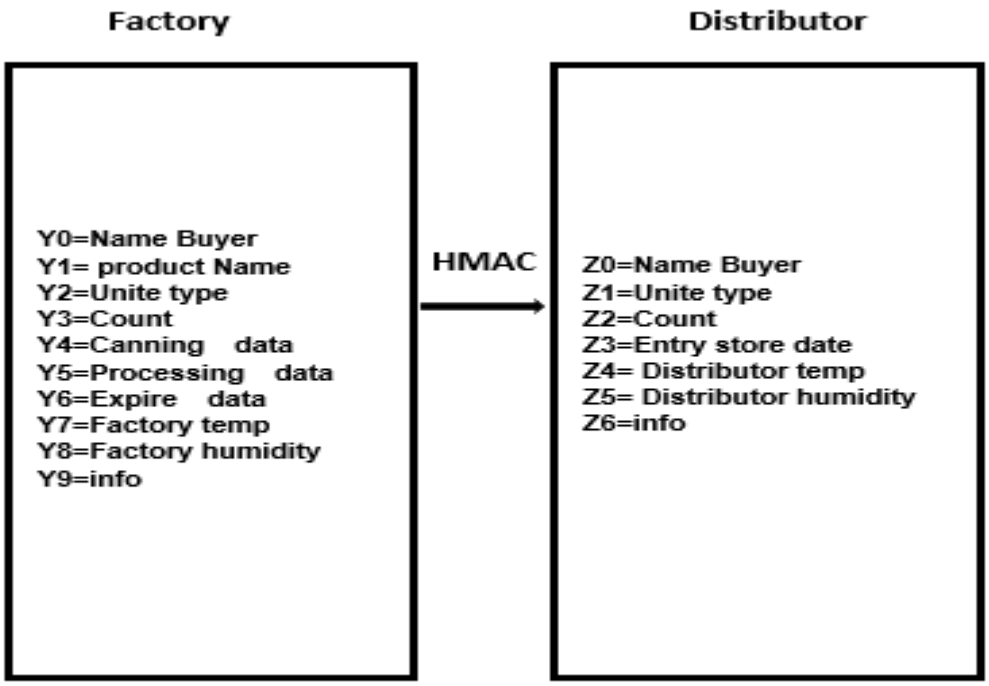

Figure 3. 3: Supply chain and secure to factory to distributor

The Distributor adds all the product details and information related to the process wherein it moves from distributor to marketer. These details include the distribution time, marketing entry date, and the sales date. Three safety algorithms are applied (HMAC, RSA, SHA512) to ensure that the product is transported securely with no chance of alteration.

Similarly, whenever the products are sold to the marketer, the latter can in turn add new product details related to their stage of supply, such as the product conditions and entry date. The Marketer further sells the products to

the customers again, a signature is created using the RSA algorithm to ensure the secure transport of the products to the customers.

An HMAC is generated for the public key and the private key of the data this results in the digestion of the data and it becomes ready for transport. Next, the message and signature are sent to the marketer along with the public key. The marketer receives them, counts the SHA512, and signs the signature. Here, a comparison is made between the hashes. In case the hashes are equal, this means that the message is intact and no alterations have been made to it.

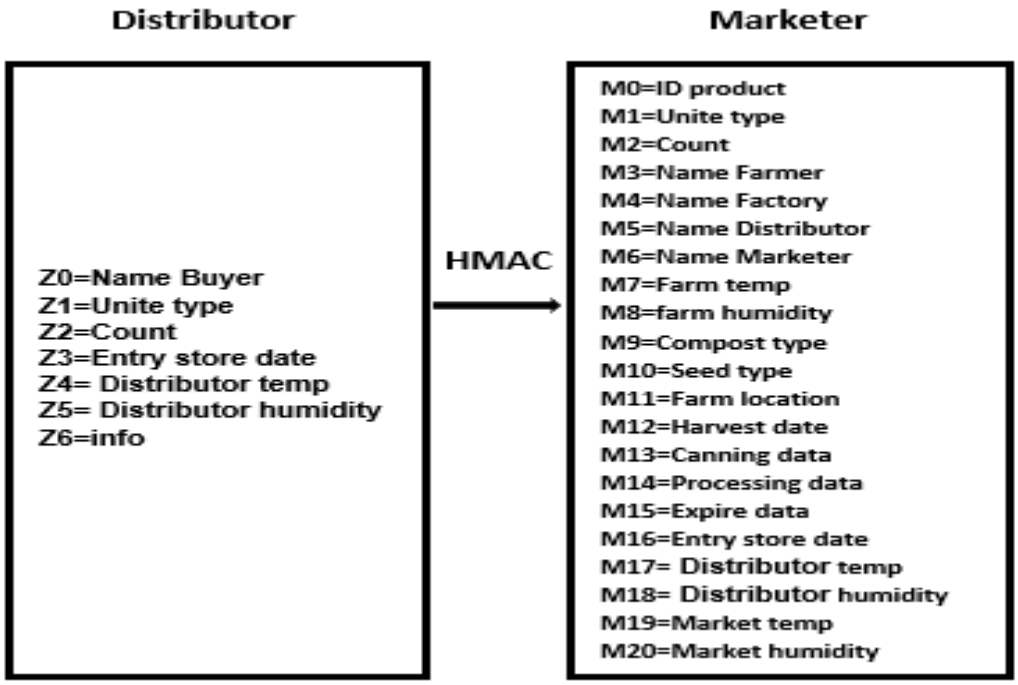

Figure 3. 4: Supply chain and secure to distributor to marketer

Sender:

HMAC = sign(sha512(message), privet key) …… (3.1)

Send data = public key, HMAC, message

Receiver:

Hash1 = sha512(message) …… (3.2)

Hash2= sign (HMAC, public key) …… (3.3)

If hash1 == hash2 then valid

Else not valid

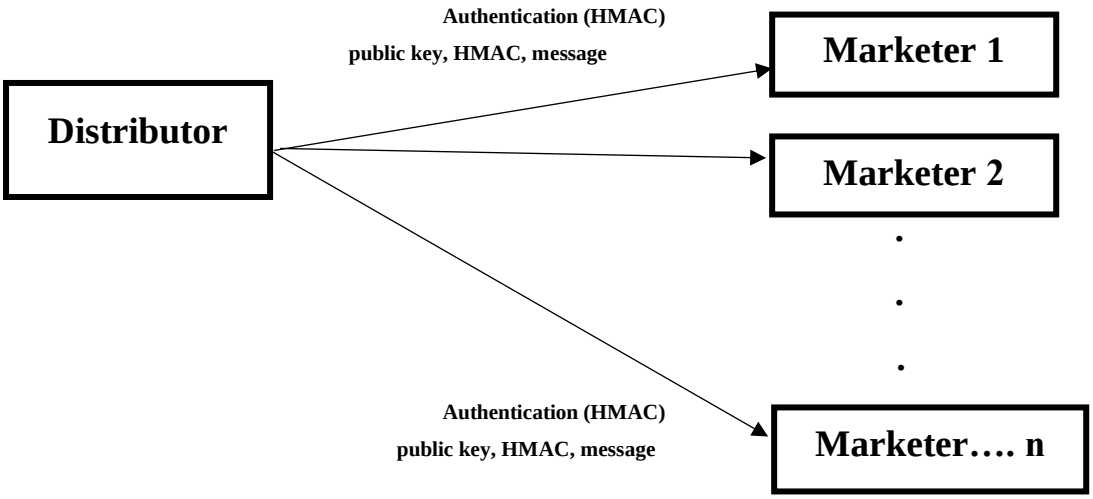

Figure 3. 5: Authentication between distributor and marketer

Database saves and stores all the system data in order to be dealt with.

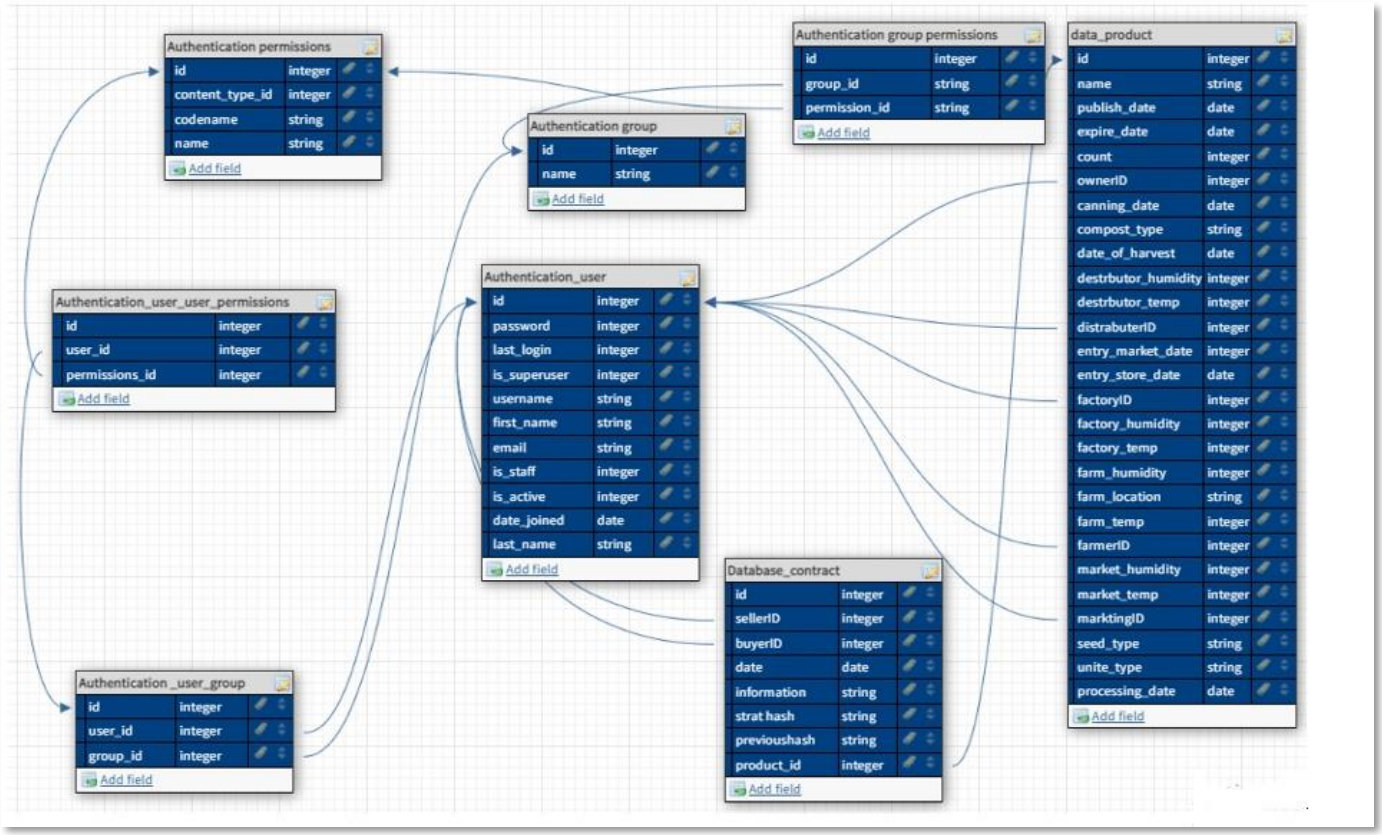

Figure 3. 6: System database

The e-contract is a contract that cannot be altered in any form. The transaction shown in the Table Database contract illustrates the buying and selling process where all the relevant product data is collected within a single table in order to be encrypted using a SHA512 algorithm.

Table 3. 4: Database contract

id	Seller ID	Buyer ID	date	Info	current Hash	Previous Hash	Product _id
40	4	5	2021-07-05		573f7f25b7b1eb79a4ec6ba896debefd	('',)	16
41	5	6	2021-07-05		55a0ce8200cf39c3028ebc66f356bf7e	573f7f25b7b1eb79a4ec6ba896debefd	16

It shows all the details of the supply gene to trace the product to its breeder, the product at the farmer stage, the factory stage, the distributor stage, and the market stage.

The farmer grows it or makes dairy products, the farmer inserts it into the insured supply gene system and adds the product information such as the name and all the climatic conditions .The product is going through, the quantities of the product, location of the farm and all the dates of its production, as well as when the product is sold to the factory, The factory owner adds the dates of his entry to the factory and the degrees of climatic conditions to the product goes through. Also, when the product is sold to the distributor, the owner or the person responsible for the distribution adds the dates of the date it entered the distribution phase and the degrees of climatic conditions the product is going through the phase of distribution entered into the safety algorithms

In order to maintain product integrity and reliability, the product does not have any forgery, and we add reliability algorithms between the factory stage and the distribution stage of the market, as well as when the product is sold to the market, the owner of the market adds the date of entering the market and the degrees of climatic conditions that the product is going through each person in the system is able to see the products page and the conditions that the product went through the products page during the buying and selling stages, can sell all or part of the product.

Table 3. 5: Product database

id	name	pub_date	expire_date	count	ownerID	canning_date
1	Tomato Paste	2021-07-05 00:00:00	2022-07-30 00:00:00	100	6	2021-07-01 00:00:00
compost_type	date_of_harvest	destrbutor_humidity	destrbutor_temp	distrabuterID	entry_market_date	entry_store_date
organic	2021-07-05 00:00:00	9	6	6	2021-07-08 00:00:00	2021-07-07 00:00:00
factoryID	factory_humidity	factory_temp	farm_humidity	farm_location	farm_temp	farmer ID
5	19	10	30	بابل- النيل	10	4
market_humidity	market_temp	marktingID	seed_type	unite_type	processing_date	
9	4	0	seed tomato	Box	2021-07-05 00:00:00	

The QR code is an effective information transmission medium, which is widely used in product traceability.

The product page is available in firm of a QR code which can be scanned by any user using the camera of any smart device. When scanning, a link will appear that leads to the product page, and this enables possible customers to buy the products or collect information about them. Such a procedure enables anyone to access the relevant information without the need to have an account.

In order to access this information, the scanning of the QR code leads dividing the URL routing. This URL is restricted to a particular page, and the server receives and responds to them. Otherwise, the request will be denied.

Figure 3. 7: QR code of product

3.4 System Functionality

The main goal of the proposed system is to trace products, keep it secure, and out of modification. Therefore, it has been designed to:

- **First,** ask customers to register their information to the system. The registration form has their personal details and some other information about login process. An authentication process shows on registration to make sure customers details keep save.
- **Second,** set different permissions to the registered users. Each pass to different form with different fields. In case the user is farmer, so, the products information sets into a farmer form. It contains product ID, farmer name, QR code and more other details as it shows in figure 3.3. The same process followed with the other three users.

- **Third,** the inserted data from all users is saved into a database with type of SQLite.
- **Four,** using some security cryptography methods like HMAC which includes RSA and SHA512. The last need to verify the public and private keys of RSA. Algorithm (3.1) and (3.2) shows hashing schemas.
- **Five,** depending on some parameters related to product, the proposed system tracks product's information using supply chain mechanism and hence the reliability ensured

The main steps of a Supply-chain traceability with signature based on a secure approach described in algorithm 3.1 below:

Algorithm 3.1: A **supply-chain traceability**

Input: the source message
Output: the signature, RSA Public and private keys

Begin

- Enter the data by user
- Switch ($userRol)
  Step1: Set_permission =Farmer
  Step2: Set_permission = Factory
  Step3: Set_permission = Distributor
  Step4: Set_permission = Retailer
  Step5: Update User Information based on user Roles
  Step6 : create RSA Private and public keys
  Step7: create signature in HMAC

End

Algorithm (3.2) illustrates the steps of implementing authentication on the data log.

Algorithm 3.2: Authentication Process

Input Message , signature , public key

Output Identical/ not identical massage

Begin
Step1 : Product data sent from the sender to the receiver.
Step2 : Sender hashes the input into a 1024-bit integer using the SHA512 hash algorithm.
Step3: Sender signs the 1024bit number with private key, converting it into a Digital Signature. The data, Digital Signature, and public key are sent to the receiver.

Step4 : Receiver decrypts the Digital Signature using the public key received to obtain a 1024-bit number.
Step5: Receiver then applies the SHA512 hash to the received data to get a 1024-bit integer.
Step6: The receiver then compares the two 1024-bit values to ensure they are equal.
If false → someone has tampered with the contents or provided a public key that does not match the sender's private key.
→ If true case, the recipient knows the data is safe to use.
End

Algorithm (3.2) shows the steps of encryption process using RSA.

Algorithm 3.2: RSA Algorithm

Input RSA public key (n,e), Pure text m ∈[0,n-1]
Output Cipher text c

Begin
Step1 : Randomly generate: 2 primes P and Q of length K / 2 bit

Step2: The public key calculated;
publicKey = P * Q;
(public key's length is k-bit)

Step3: Random encryption generated;
key keyE, 2 <= keyE <= < φ(n) - 1,
keyE * keyD mod φ(n)=1,
φ(n) is known as the Euler function of n,
the value is φ(n) = (P-1) * (Q-l);

Step4: where GCD(keyE, φ(n)) = 1;
The decryption key is calculated,
keyD = keyE - 1 mod(n),
keyE - 1 is inverse for the decrypt key keyD. The formula of the original equation is keyE * keyD mod φ(n) = 1;

End

In the same way but without using previous signature methods, the above steps have been implemented online platform for building forms, applications, collecting various information, etc. Four forms have been created as follows: farmer, factory member, distributer, and retailer to insert product's information and repass them to the second user in the system. Worthy to mention that the data is stored into Google Sheet service. Farmer will give information about the product before sending it to the next stage, which is the factory. At this point, product information should be updated to

have factory information. On the distributer form, the same information should be filled but what is related to this stage particularly. Finally, all information is shown to the retailer under the same product ID. It important to mention that the collection of restored information is linked using with Distributed Ledger using API. The distributed ledger is the result of product information, which shared by network user and make customers, trace their goods information and current position. Peer-to-peer nodes are connected and able to access data in the distributes ledger. Each node has individual information such that they can communicate with each other. Figure 3.9 illustrates the role of distributed ledger in the implementation of supply chain using JotForm platform.

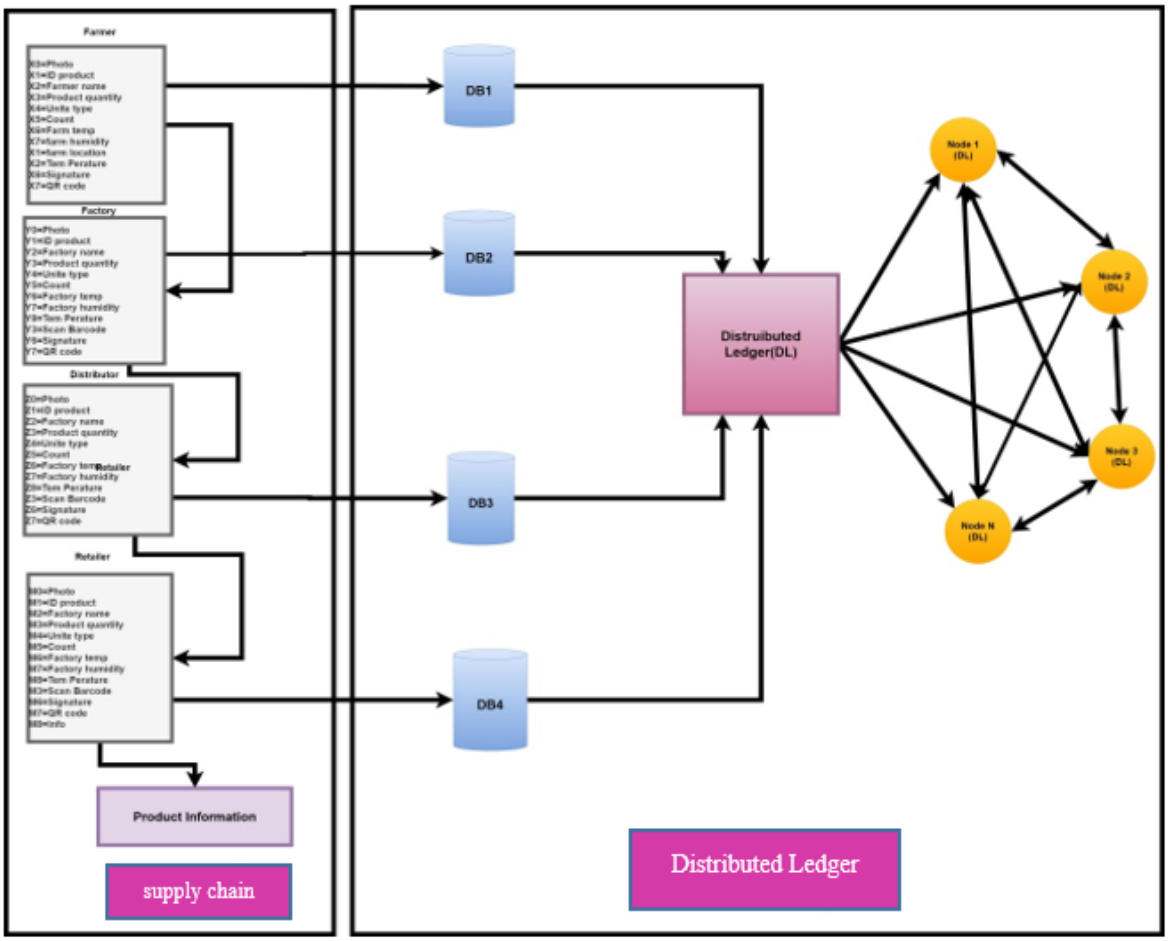

Figure 3. 8: The design of supply chain & DLT using JotForm

The main goal of the proposed system is to trace products, keep it secure, and out of modification. Therefore, it has been designed to:

1. Inserted data from all users will be each saved into a separate database and them stored together to make product information.
2. Distributed ledger is the result of product information, which shared by network user and make customers, trace their goods information and current position.
3. Peer-to-peer nodes are connected and able to access data in the distributes ledger. Each node has individual information such that they can communicate with each other.

For more details, Appendix (A) provides a full explanation about the implementation of this mechanism.

3.5 Summary

This chapter presented the designing of the proposed system which was about tracking products using supply chain technique based on secure approach represented by implementation some of hashing methods to ensure reliability. Similarly, another supply chain system has been designed using online platform called JotForm. Here, the concept of distributed ledger had implemented to share the information of product cross the nodes in the network.

Chapter Four

System Implementation and Results

Chapter Four

System Implementation and Results

4.1 Introduction

The following sections illustrate the system implementation and results, in addition to the evaluation and comparisons between the obtained results and other similar systems. The proposed system is a web-based application built using python programming language within the Django framework, and it is executed on a platform with processor Intel (R) Core i7 2.40 GHz and 8 GB RAM running Win10 64-bit.

4.2 Django

The application has two types of users: **admin and customer**. Each one has different permissions. The Admin user is able to add new users, and view all inserted products and details. On the other hand, Customers have different privileges. Firstly, the admin account should enter the login information in order to be redirected to the control panel according to their permissions.

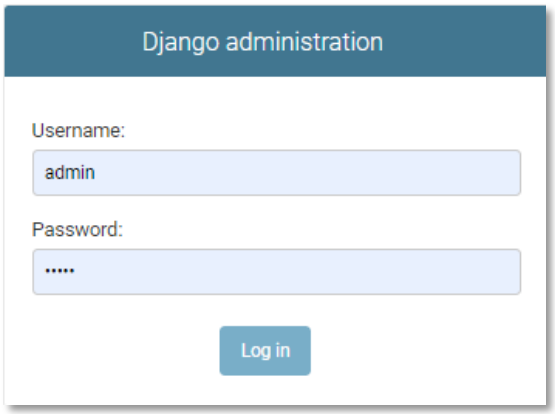

Figure 4. 1: Django login form of the system

4.3 Admin Permissions

This interface allows the Admin to create groups in order to assign users to them. Four groups have been created as follows: Farmer, Factory, Distributers and Retailer.

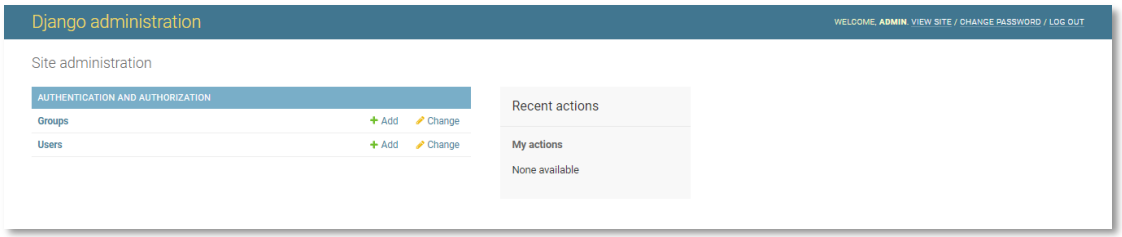

Figure 4. 2: Admin page of the system

The figure 4.3 below illustrates the process of asigning permissions for each group.

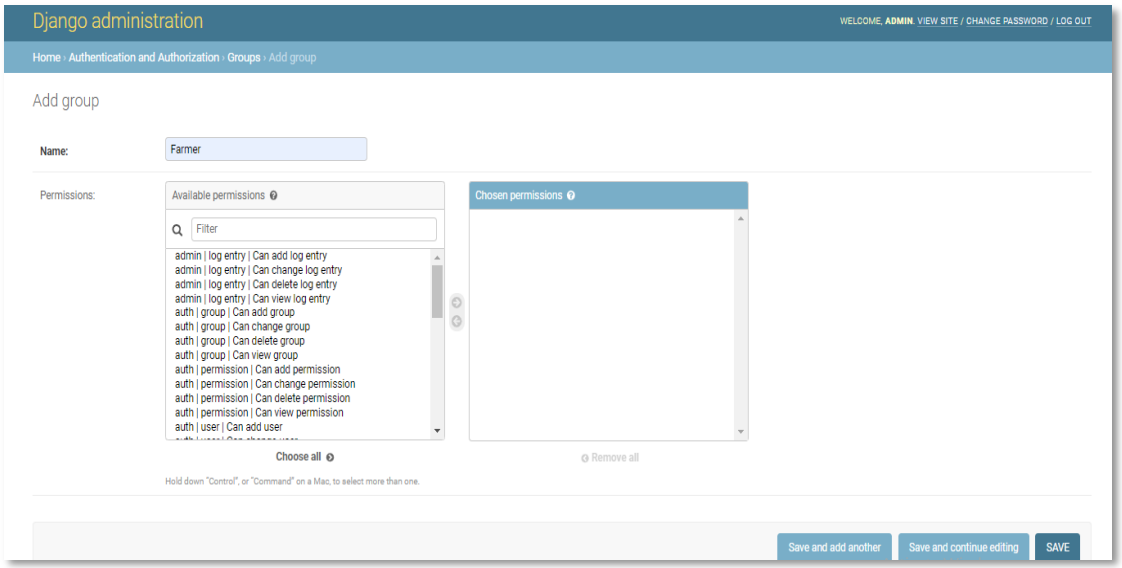

Figure 4. 3: Farmer's dashboard

Moreover, the Admin has a permission to add many users through the “add” button.

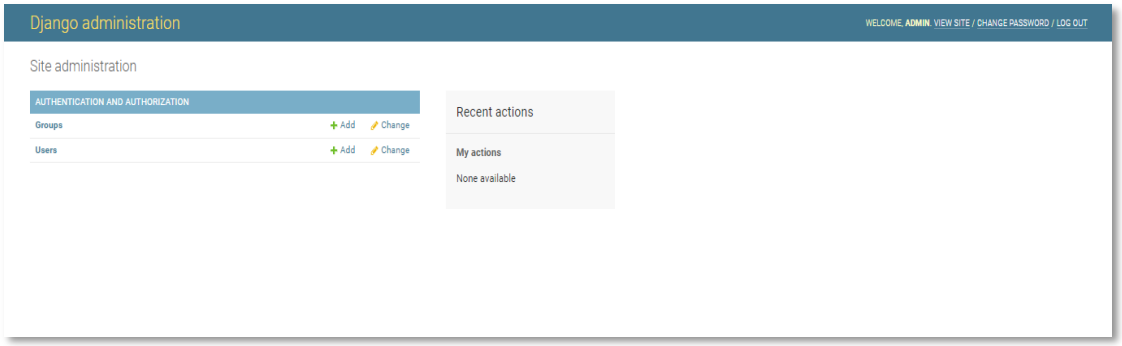

Figure 4. 4: New users are added to the farmer type user

A new page with several required fields, asking the user to enter login information such as a username and password.

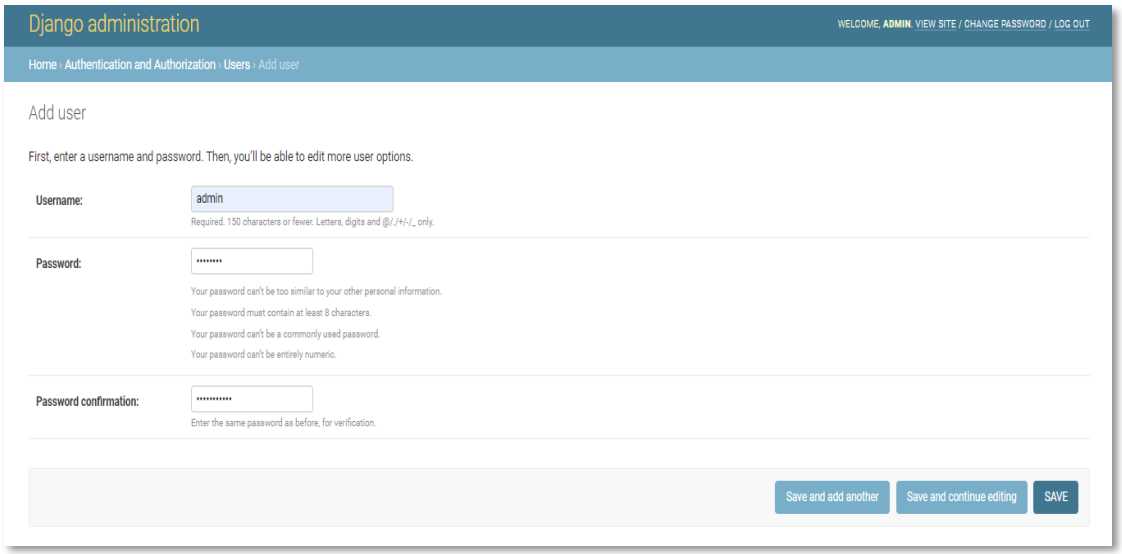

Figure 4. 5: Set registration/login details to new users

Some options should be selected in order to activate the account, as shown in the figure 4.6.

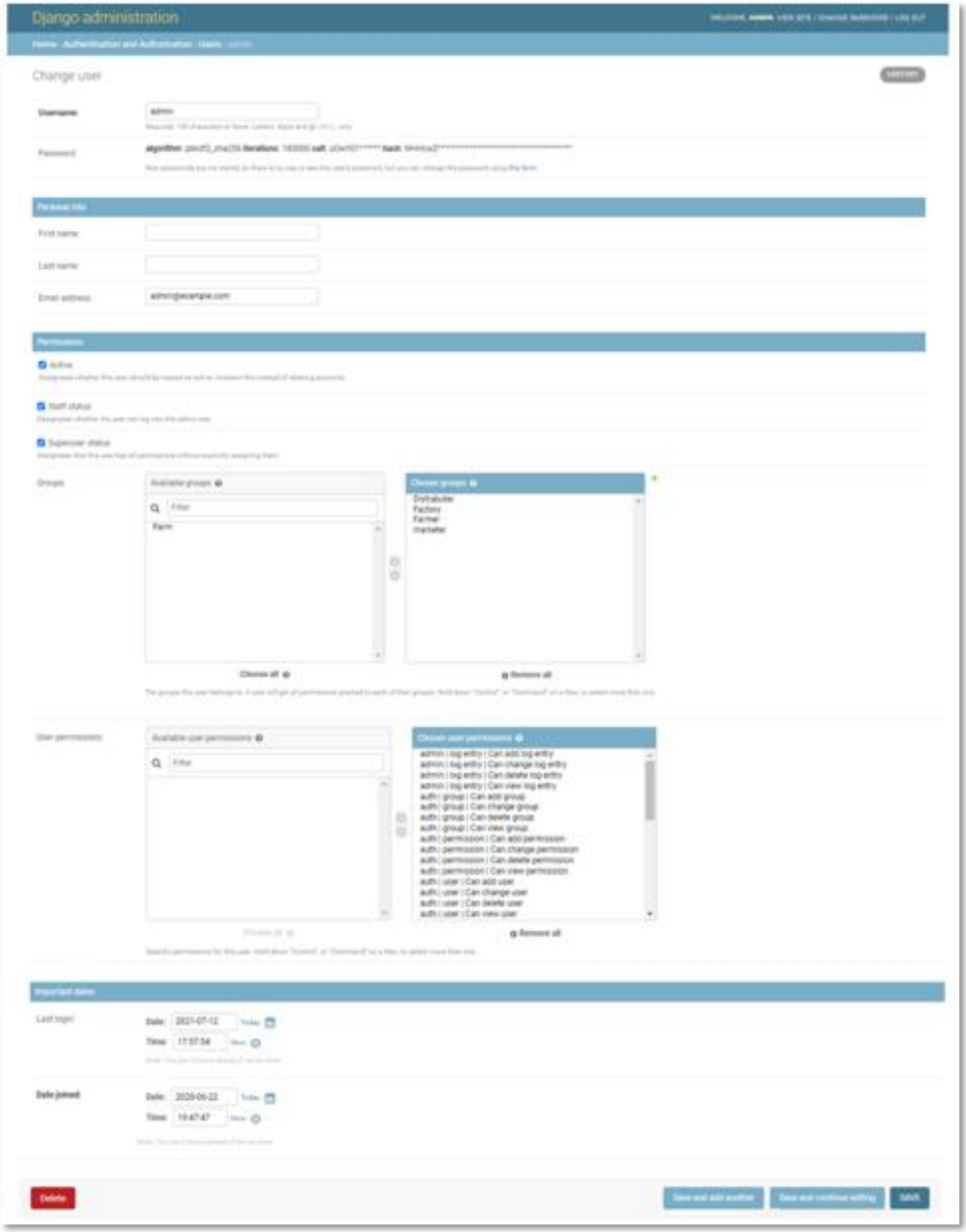

Figure 4. 6: Activating the new account

The user accounts are created, after which the permissions are assigned.

Table 4. 1: Authentication of users

Id	password	Last log	Is sparser	username	First _name	Email	is _staff	is _active	date joined	Last_ name
1	pbkdf2_sha256$180000$uOwY0l15DgxJ$M+HcwZQorXbVdsWk1pbFsYzGIFINU3MsLe0ONOywxDg=		1	admin		admin@example.com	1	1	2020-06-22 19:47:47	
2	pbkdf2_sha256$180000$ZNCmNSwUOC8J$xX/evshWu6qjRx74WT25gaFPwKHpGk5H9uPfGu8Ncn0=		0	Farmer			1	1	2021-04-09 14:52:18	
3	pbkdf2_sha256$180000$zyacNbtPXMKr$bfaGXShZsCV7AVx/jgnpMl9r5XrdWAibgd14CH4zJKg=		0	Factory			1	1	2021-04-09 14:56:17	
4	pbkdf2_sha256$180000$ymx4k90MIepI$Odao2+CsgUDvUzShPTNZ1fWt+8SolZY3hKKNi11lewI=		0	Distributor			1	1	2021-04-09 15:00:10	
5	pbkdf2_sha256$180000$GAgQ3j2m53w3$vGkt9is6ZAU8sV1nc9FGF0/IIUa6HHeS3U6oQHgDY7U=		0	Marketer			1	1	2021-04-09 15:02:26	

4.4 Farmer Permissions

The Farmer is the first user used in the system, and their main role is adding new products to the system. The following screenshot shows the required details of the product that should be added to the system.

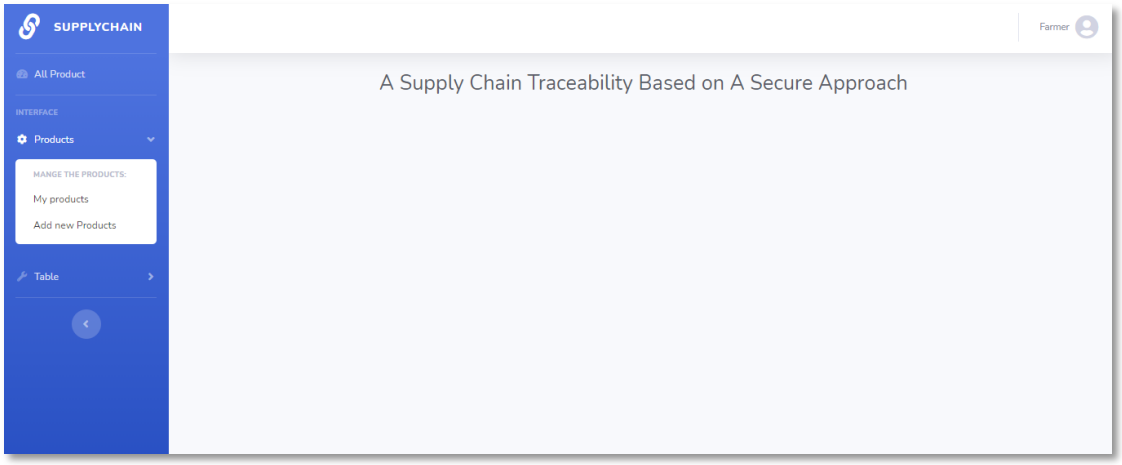

Figure 4. 7: Farmer add new products to lists

The farmer is the only user that can add new products to the system.

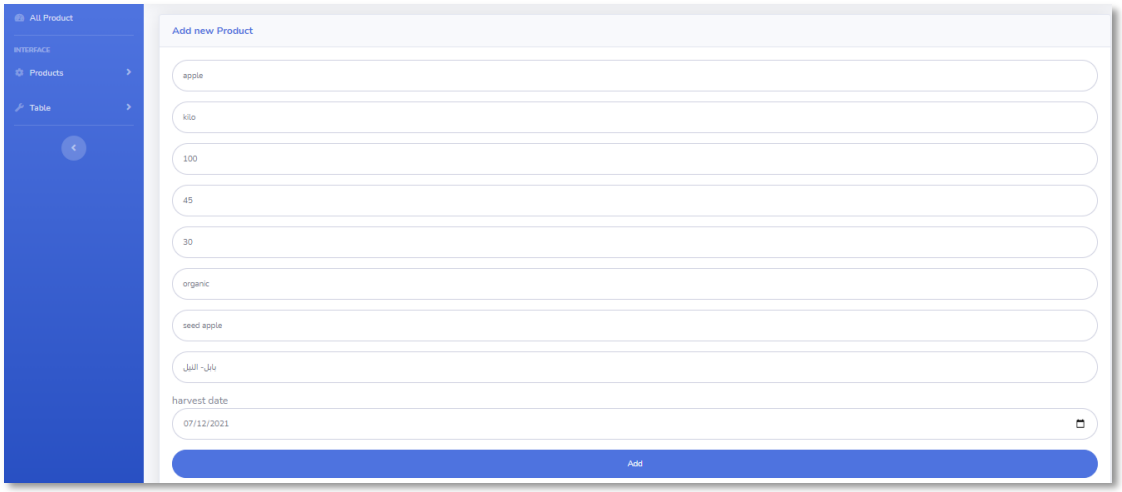

Figure 4. 8: Adding new product by farmer

After adding the product to the system, all its details are shown to the user as presented , and they are added to "my product list". In addition, there are some details that have not been filled in, because the product still in its initial stage of process. Such information includes canning date, and the time required to input the product data by the Farmer. More details about product can be seen by clicking on it.

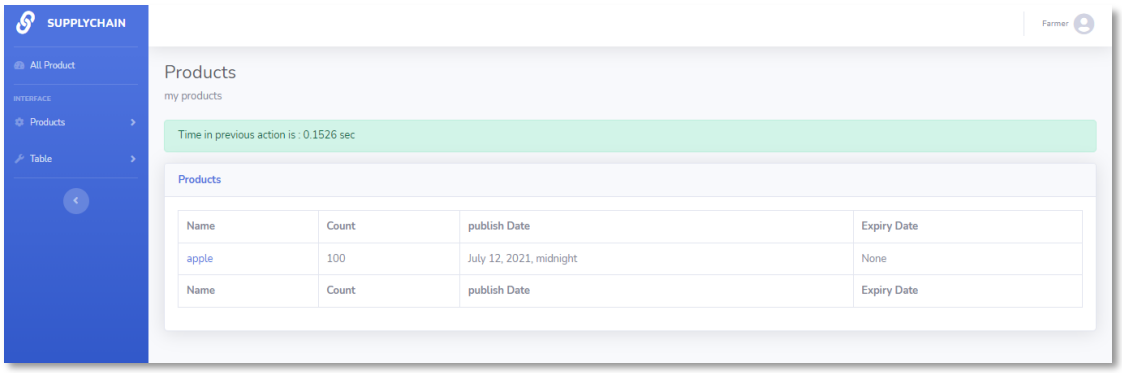

Figure 4. 9: History of products and time required to create products

When clicking on the product (which is in this case "apple"), the following details will be shown.

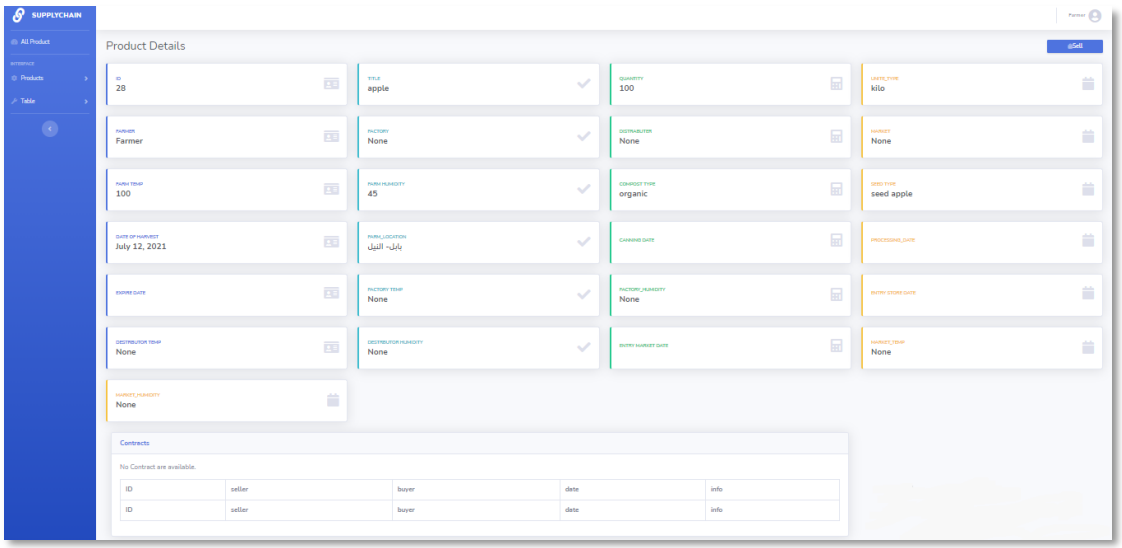

Figure 4. 10: Products details

The Farmer is able to sell product to the factory. By clicking on the sell button, a new tab shows with the required information as illustrated. The farmer can choose which user wants to sell product. The remaining fields should be filled in as well. Finally, the submit button si clicked.

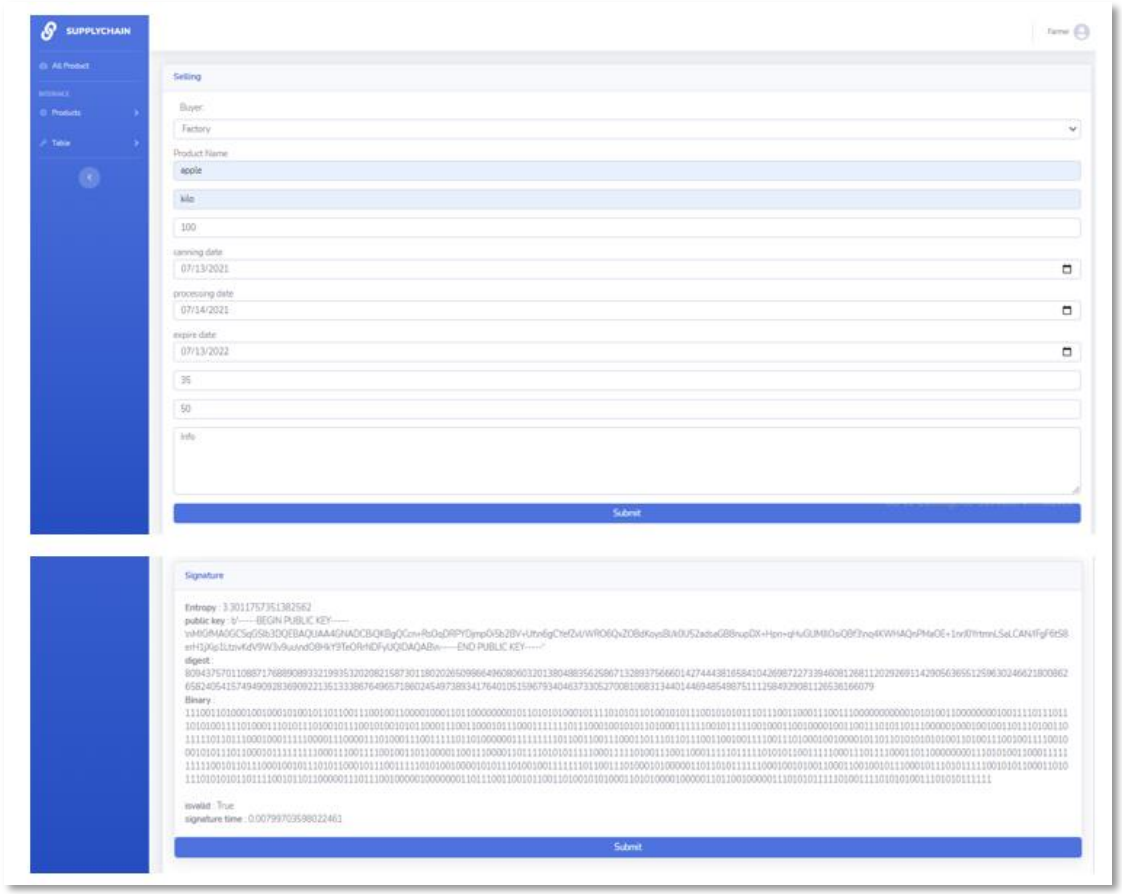

Figure 4. 11: Set seller data

When selling a lot of product quantities, it may be sold out and in this case the product will be removed from product list, based on the time required to sell the products from the farmers to the factories.

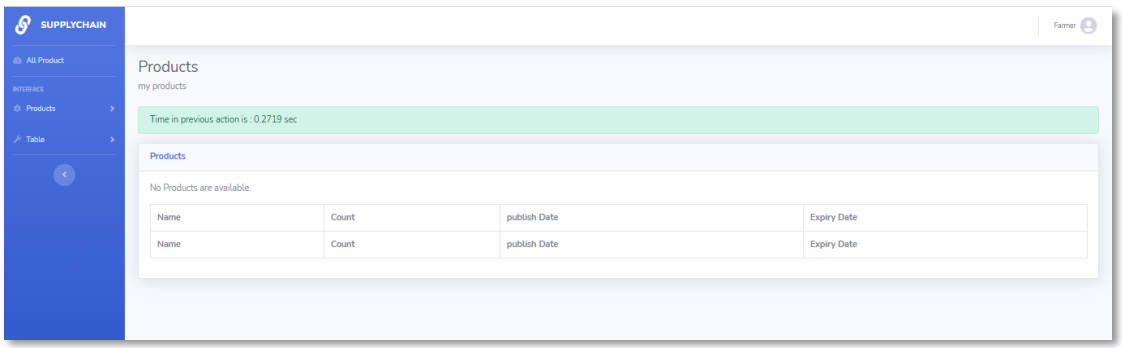

Figure 4. 12: No items to sell into farmer list

4.5 Factory Permissions

Factory users are the second level user in terms of authorization permissions.

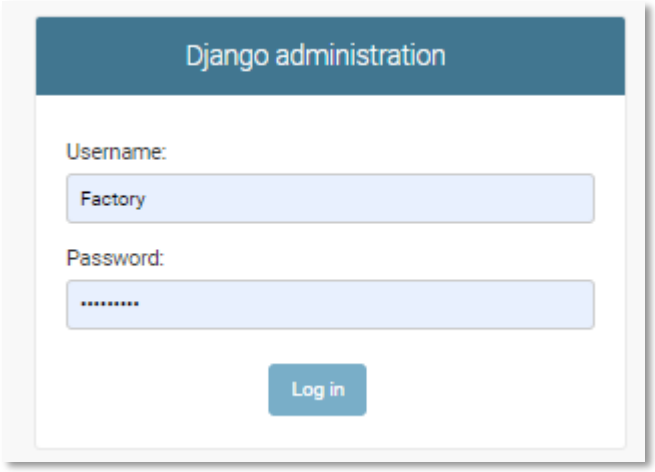

Figure 4. 13: Factory user's login interface

By logging in with factory user login information and navigating through the submenu of products, the products list that are bought from the farmer will be listed as Figure 4. 14.

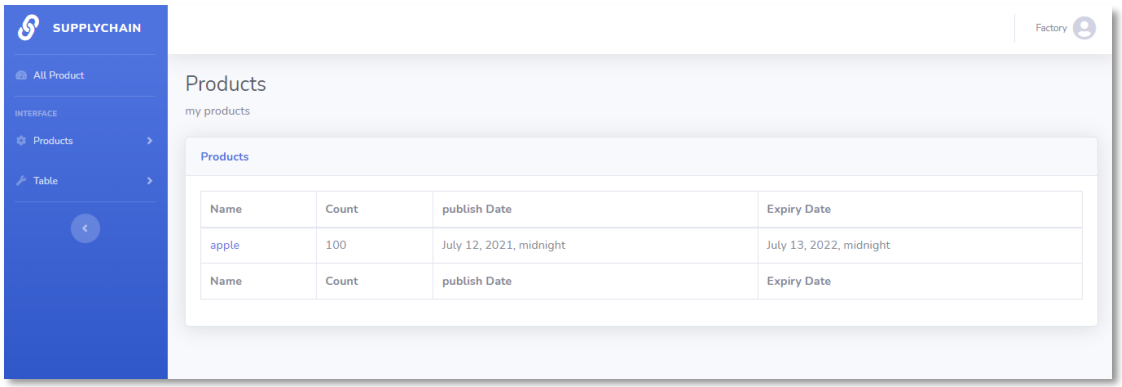

Figure 4. 14: Products list on factory dashboard

By clicking on particular products within the previous list, the details will be viewed. It can be noticed that the factory data has been added to product as it shows below, under the sections of canning date, factory humidity, and the e-contract signed to trade the product.

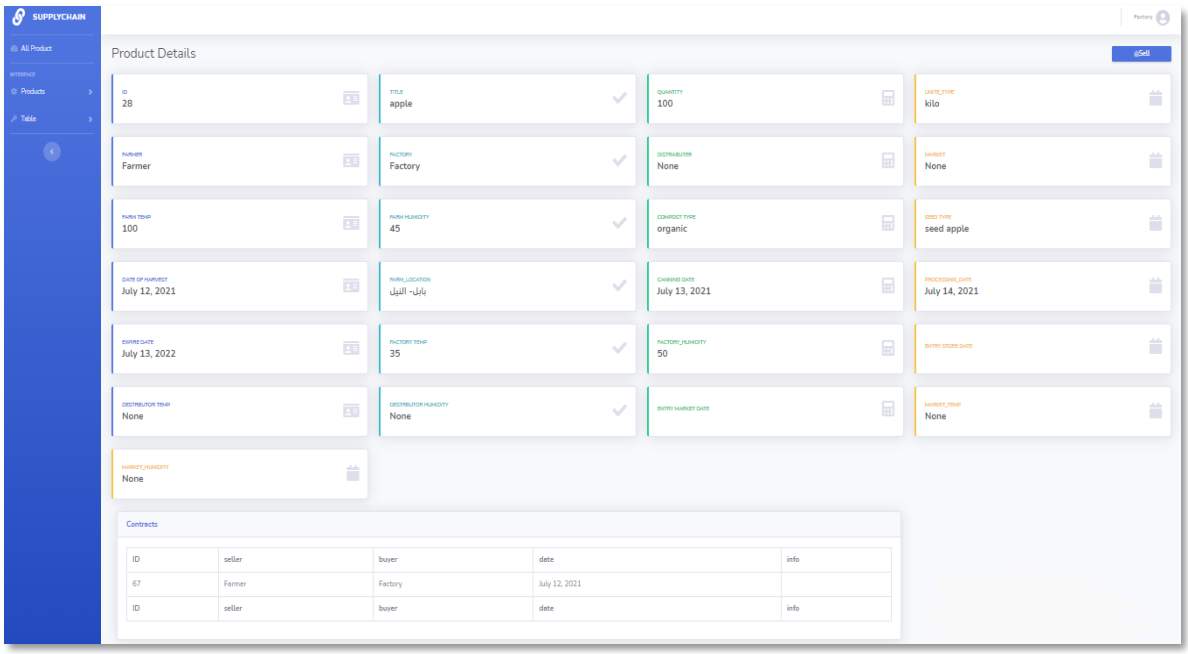

Figure 4. 15: Products details on factory dashboard

The factory will sell the products to another user called distributor which is already registered in system. The following screenshot shows the required details that the factory should fill to sell their product to the distributer.

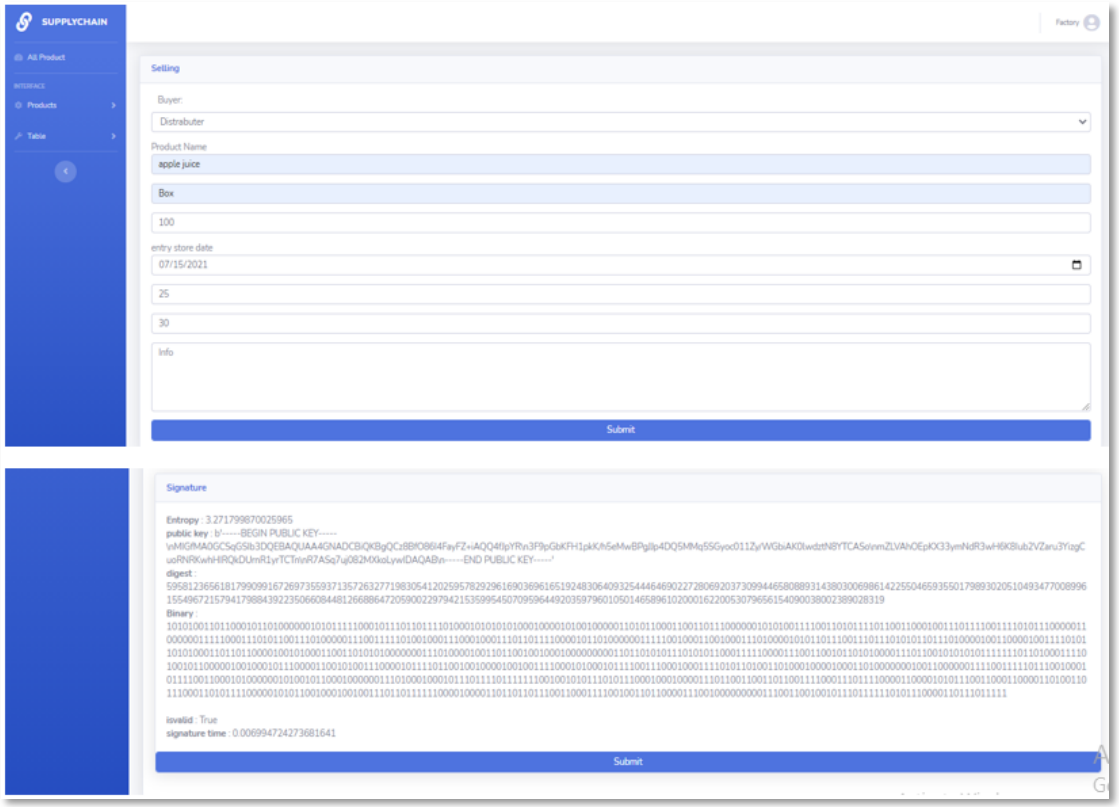

Figure 4. 16: Factory selling items to distributer

After submitting, 100 items have been sold and in this case this product will be sold out and disappear from the factory product list.

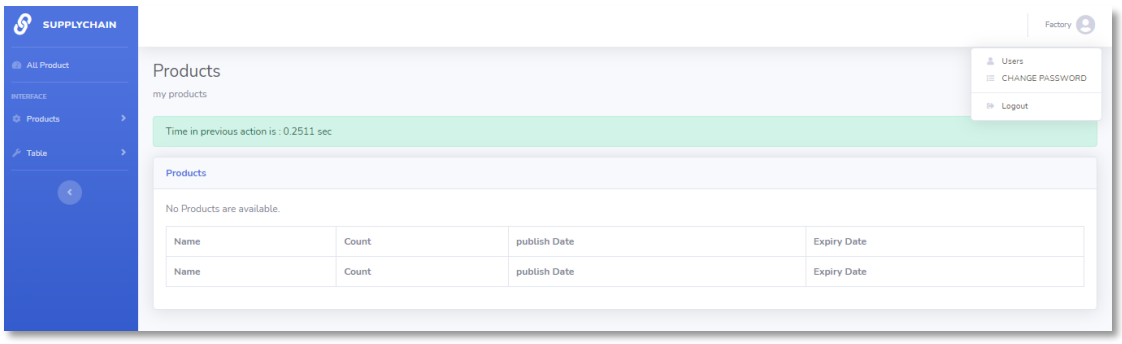

Figure 4. 17: Products sold out

4.6 Distributer Permissions

The distributor sells products to the markets, and it is possible to sell all the product and the quantity runs out, or sell part of it according to the buyer's request, the owner of the market. Here the product is divided into two parts. If all the product is sold, it be an electronic contract between the seller and the buyer of the product, and if part of the product is sold, there be two electronic contracts for part of the product to be sold for the market and contains all the details of the product and the second electronic contract for the part of the product that does not belong to the market remains with the distributor.

In the distribution stage, apply reliability using cryptographic algorithms HMAC and RSA on products to ensure the safety of products from counterfeiting or tampering and protect the access of the product from distributors to the market without forgery or manipulation of the product by using the hacker algorithms and the time taken in the sales process and the security is very little and by measuring the entropy of the algorithms used in the security and a large random value appeared that proved the strength of the algorithms used to protect the product during the transportation process and proved the accuracy system high through the Message digest. It can be noticed that Hash1 at distributors is matching Hash2 in the markets which mean that the message digest is valid. Otherwise, it is not valid, may be fraud or manipulation happened during the operations of selling and transferring the product.

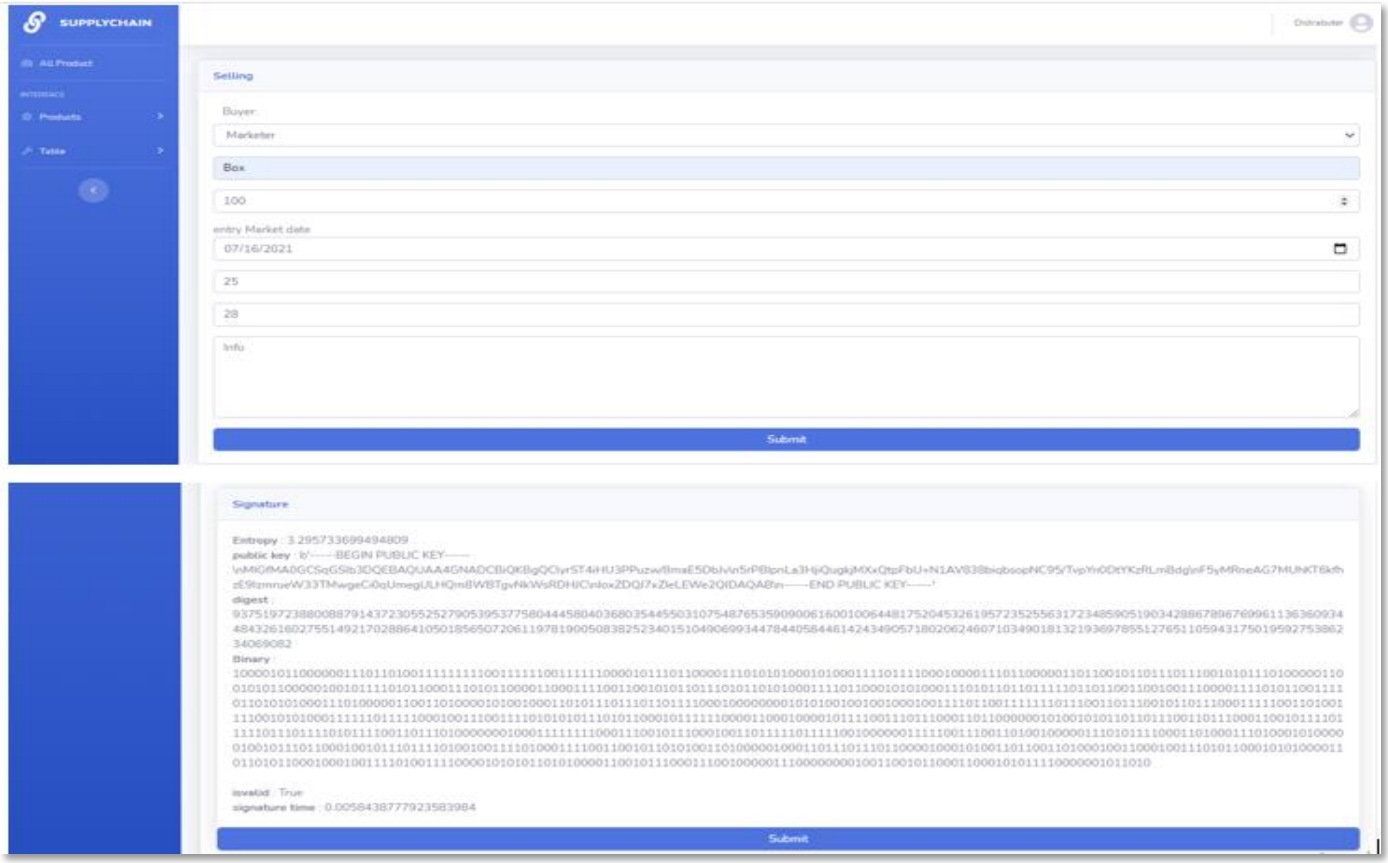

Figure 4. 18: Product details on the distributor dashboard

4.7 Marketer Permissions

The marketer (retailer) is the last destination of the sold product. After logging in with the marketer account, the last can browse the list of products that are bought from distributer by clicking the “My products” button. In this example, the product is “apple juice” as shown in the figure below.

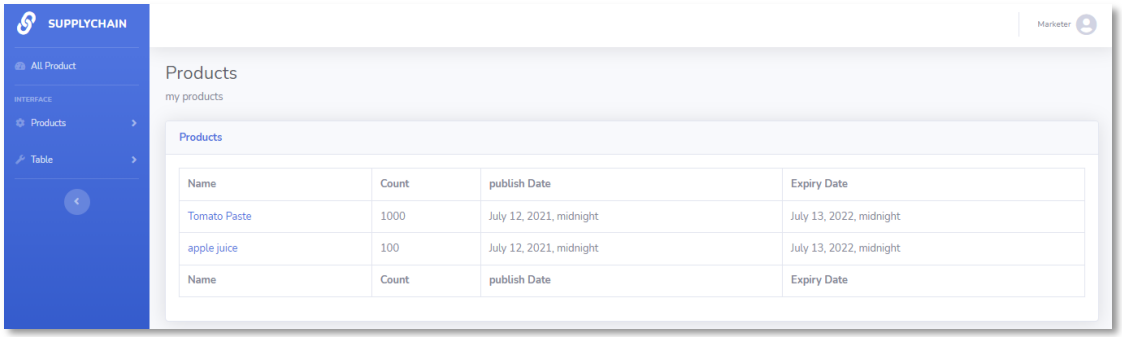

Figure 4. 19: Retailer's list of products

When clicking on the product, all details that are stored in the system and have been inserted by (farmer, factory and distributor) will be viewed, in addition to other details inserted by the marketer.

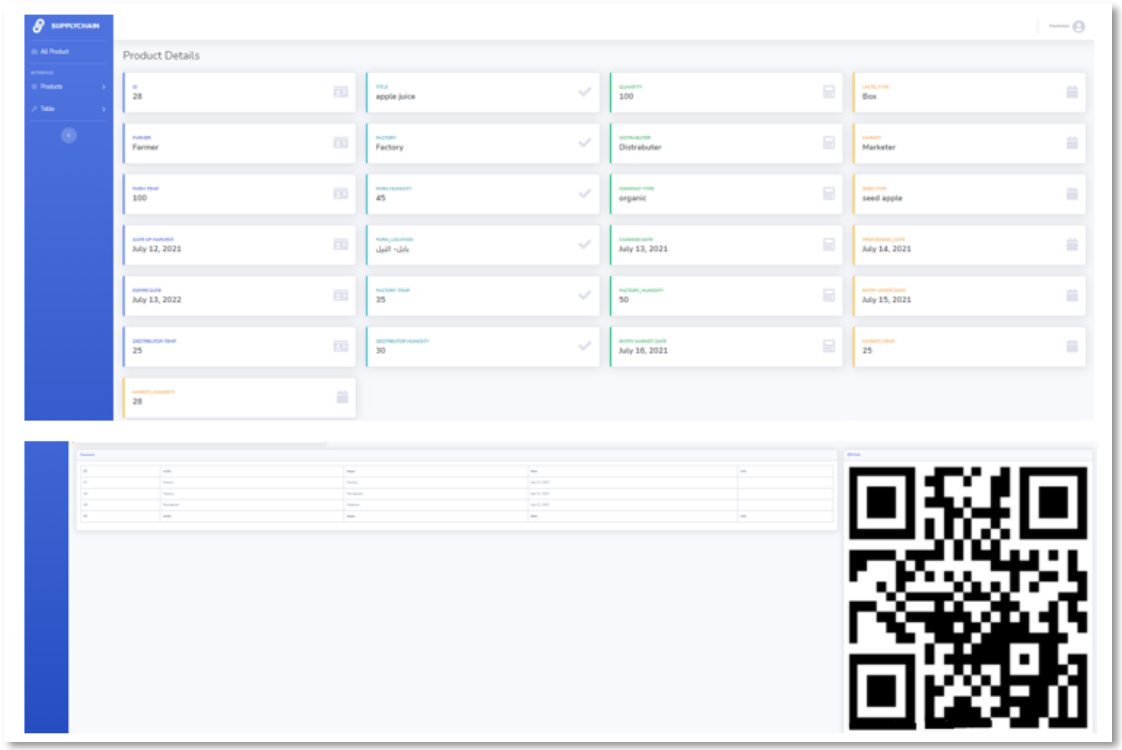

Figure 4. 20: Product details on retailer dashboard

Moreover, the contract list displays all details of the seller and buyer. After this step, the QR code be set up to access products information easily.

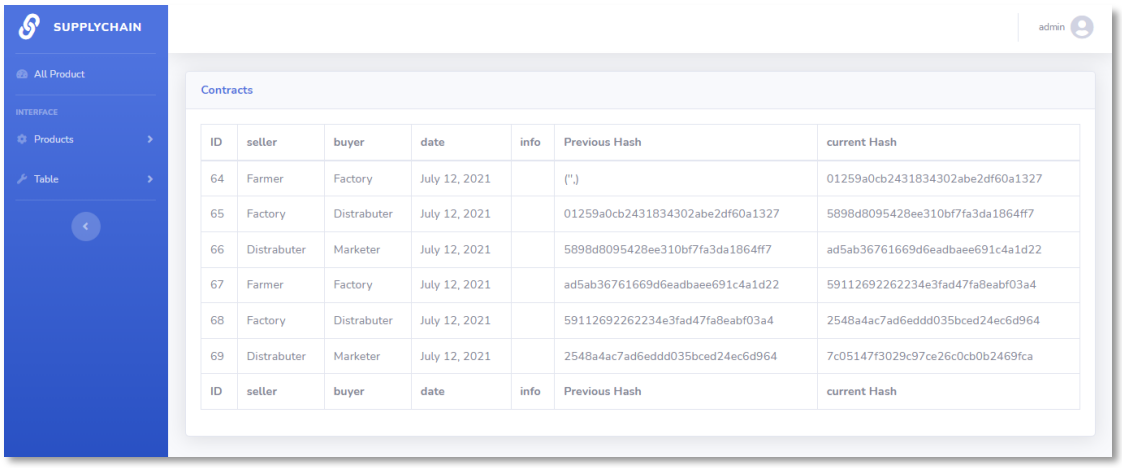

Figure 4. 21: Contract

One of the aspects that have been added to the proposed system is the use of a QR code to read product information by scanning it. As a result, the market user be able to scan the code and view all details related to hashed signature, as illustrated in Figure 4.21. By hovering the phone's camera over the QR code, all the products details will be shown from its origin to retailer, including the different environmental aspects that it passes through (such as temperature and humidity), and also other details regarding canning date, expiry date. In addition, all sell-buy contracts will be listed.

Figure 4. 22: QR code sample

Table 4.2 shows the requirements of marketing and their results in the proposed system.

Table 4. 2: Results of the proposed system

Marketing Requirements	Properties of system	Simple interface	Backup plan	Easy to maintain	Protected using authentication	Reliable	Fast
		√	√	√	√	√	√
Accurate information	√	×	×	×	×	√	×
Easy to use	√	√	×	√	×	×	√
Fast response	√	√	×	×	×	×	√
Durable system	√	×	×	√	×	√	×
Secure system	√	√	×	×	√	√	×
Tracking	√	×	×	×	×	×	×
Targets for Marketing requirements		Python Language	Daily	×	HMAC RSA	SQL lite	QR

The time has been calculated regarding the process of entering the product information into the system by the farmer, the time of selling the product from the farmer to the factory, the time taken to sell the product from the factory to the distributors, the time taken to sell the product from the distributors to the market, and the total time taken for the system as well. Further, the digest time for each stage of the selling and purchasing of the product that takes place between farmers and factory owners, between factory owners and distribution owners, between distribution owners and market owners, and the total time for Digest time. Finally, the percentage of signature time in all operations from the original time of the system has been calculated.

Table 4. 3: Total time of system

	Create the product	Sell product from farmer to factory	Sell product factory to distributor	Sell product from distributor to market	Total time to system
Execute time	0.2449 sec	0.2088 sec	0.2518 sec	0.2823 sec	0.9878 sec
Digest time	-	0.00499 sec	0.00499 sec	0.00499 sec	0.01497 sec
This is the signature time for all transactions from the original time	-	-	-	-	0.01%

Entropy is a physical feature that can be measured scientifically, and its most common association is with states of disorder and randomness. The equation below shown how its value can be obtained.

$$S = -k_{\mathrm{B}} \sum_i p_i \log p_i \qquad \ldots\ldots (4.1) \qquad [45]$$

One of the algorithms applies Optimization Such as Genetics This is a future work has been calculated Supply chain to ensure the accuracy and security of the product, and there is no fraud or manipulation of the product during the stage of buying, selling and transferring. In the Supply chain the product is based on the Message digest as shown in the table .

Table 4. 4: Product accuracy

Signature	**Sell product from farmer to factory**	**Sell product from Factory to distributor**	**Sell product from distributor to market**
	isvalid : True	isvalid : True	isvalid : True

4.8 Evaluation of the Proposed System

When evaluating the role of suppliers within supply chains, there are a number of attributes that are taken into consideration. These may include its efficiency, flow, integration, responsiveness and customer satisfaction. Being a form of collaboration between buyers and sellers, there are certain aspects which require special attention in order to avoid any complaints made by customers, such as how efficient the purchase-to-order time cycle is, the way in which the product quality is assured, and the extent to which the capacity is flexible.

Each of HMAC, RSA and SHA-512 are algorithms applied to ensure the secure cryptography criteria, which are in turn determined by the sizes of keys, time required in computation, and the amount of power being consumed.

- Because of the evolution of cryptanalysis and the expansion of computational abilities that are provided to adversaries, it is necessary that the encrypting keys increase in size over time in order to ensure sufficient security for a fixed protection life duration.
- RSA is distinguished by its combination of low verifying expenses and rather high sign operation expenses.
- As for the encryption time, it is found to be more favorable in RSA than in other algorithms.

For the aforementioned reasons, the HMAC has been used as part of the proposed system, along with the use of the RSA cryptography function to get acceptable results in securing plain message send over the internet between sender and receiver. The product’s data encrypted on the sender side and decrypted on the receiver side using the private key. In case the

keys are identical, this means that the message is secured. Otherwise, it is an indicator that the message has been altered by a third part. The proposed system is evaluated by means of drawing a comparison between the implementation results of the proposed system to those that have been obtained in other related works.

It has been found that the time required for the product to get from the farm to the market is (0.9878 sec) in the paper of Ahmed Iftekhal, whereby the supply chain is used [46]. The data presented in Table 4.6 shows the time to market for fresh vegetables in Meena Bazar (3). The standards of facilities and handling was considered as weakest performance in terms of rating in this analysis.

Table 4. 5: Time of selling product from farmer to market

Execute time	**Create the product**	**Sell product from farmer to factory**	**Sell product factory to distributor**	**Sell product from distributor to market**	**Total time**
	0.2449 sec	**0.2088 sec**	**0.2518 sec**	**0.2823 sec**	**0.9878 sec**

Table 4. 6: Time of retail storage to market

Time to Market	**Retail storage**
	Fresh vegetables in Meena Bazar
	3

Chapter Five

Conclusions and Future Works

Chapter Five

Conclusions and Future Works

5.1 Conclusions

Overall, the main goal of this thesis is to provide a food traceability system to follow products from their resource to the retailer using supply chain technology. The proposed system traces products in different stages, each of which has information inserted to the system under the same product ID. Therefore, retailer is able to follow the product from the moment it leaves the farm. The main findings can be concluded as follows:

1. Accurate information: the contracts and all the details and details have been added to the database through the Distributor himself, so the information is accurate and reliable and there is no any manipulation on product's data.
2. Easy to use: the interfaces are very simple and easy to use. Everyone who is upset takes an account from the admin. This account is given by the admin, each person according to his occupation, whether he belongs to the group of farmers, the group of factories, the group of distributors, or the group of marketers.
3. Fast response: the fast response will reduce the time, and everyone (the farmers, factory owners, distribution owners and market owners) will have a system to communicate between each other, so the program will be light and reliable, meaning there will be no delay in the response. Moreover, system timing is very accurate.
4. Easy to maintain: the maintenance time is very short.

5. Security: our system uses encryption algorithms such as HMAC, RSA to ensure the security and reliability of data.
6. Simple interface: the fewer the complications that exist in the interfaces, it will reduce the errors that occur to me in a system, thus reducing the gaps that occur to me in a system, and therefore it will give me more strength and protection for the multi-system.
7. Tracking: our system implements tracking operations in supply chain.
8. SQLite: SQLite database has been used due to strong data protection and easy penetration fast.
9. QR Code: Here the user gets the product information. This information is given to the user in full, from harvesting the product or obtaining the product until it reaches the market.

Another interesting conclusion about implementing similar system using Jotform platform can be summarized as follows:

1. In Jotform platform, there are four forms that have been created (farmer, factory, distributer, and retailer) to insert the product information. Each form represents a phase through which the product passes within the supply chain system.
2. Peer-to-peer nodes represents people who want to assets the system and trace inserted information such as government, national security and taxes. They are connected with the system through the distributed ledger, which is the block-chain technology. Therefore, its data will be inclusive to trace goods from its origin to the retailers.
3. The collection of the restored information will be linked by the Distributed Ledger using API.

Finally, proposed approach provides a secure product traceability system for comprehensible production information and prevents manipulation, increases reproduction, deterioration, and use of unnecessary and dangerous chemicals. It has been concluded that the proposed system is more convenient to be applied, as it decreases the amount of efforts and costs needed to transport the products, as well as the contracts and meetings by providing a higher security for the product data.

5.2 Future Works

The proposed work motivates to think about some future works:

1. Building supply chain system based on block-chain technology. In other words, the current system will be implemented on multiple nodes so that the data will be replicated on multiple sites in network.
2. Developing the system by adding IoT capabilities. For example, a real time tracking is important for high value products. IoT devices can track these products from source location to current location providing up to date information such as temperature, humidity, etc.
3. In order to obtain more accurate entropy rates, the optimization or genetics algorithm can be applied to the entropy results that have been obtained.
4. Propose system can be implemented on a cloud platform and then promoted in the marketplace.

References

[1] A. D. J. S. Lenny Koh, "Blockchain in Transport and Logistics - Paradigms and Transitions," International Journal of Production Research Special Issue, p. 15, 2019.

[2] Prashanth Joshi A, Han Meng and Wang Y," A survey on security and privacy issues of blockchain technology," Mathematical Foundations of Computing, 2018, 121147,1(2).

[3] P. K. L. H. a. N. D. PETER GONCZOL, "Blockchain Implementations and Use Cases for Supply Chains – A Survey," IEEE Acess, vol. 4, p. 16, 2016.

[4] AcharjamayumI , PatgiriR and Devi D, "Blockchain: A Tale of Peer to Peer Security," Proceedings of the 2018 IEEE Symposium Series on Computational Intelligence, SSCI 2018, 2019, 609-617.

[5] t. point, "Supply Chain Management i," tutorial point, 2016.

[6] Blass E,ElkhiyaouiK and Molva R, "Tracker: Security and Privacy for RFID-based Supply Chains," Sophia Antipolis, France, 2010.

[7] Trebar M ,Lotrič M , FondaI,Pleteršek A and KovačičK , "RFID Data Loggers in Fish Supply Chain Traceability," International Journal of Antennas and Propagation, pp. 1-11, 2013.

[8] L. H. A. Pranav S. Joshi, "Supply Chain Innovations in the Oil and Gas Industry," in Industrial and Systems Engineering Conference, 2017.

[9] V. R. a. D. D. Kapoor D1*, "An Overview on Pharmaceutical Supply Chain: A Next Step towards Good Manufacturing Practice," Drug Designing & Intellectual Properties international journal, vol. 10, no. 11, 2018.

[10] F. R. H. TOMY PERDANA1, "Lean Production on Chili Pepper Supply Chain Using Value Stream Mapping," MIMBAR, vol. 4, no. 2, 2018.

[11] K. B. S. 1. S. 1. a. S. 2. Pradeka Brilyan Purwandoko 1, "Development of a Smart Traceability System for the Rice Agroindustry Supply Chain in Indonesia," MDPI, vol. 10, no. 3, 2019.

[12] Lisitsa S,Levina A and Lepekhin A,"Supply-chain management in the oil industry," E3S Web of Conferences, 2019.

[13] Saing, M. M, Arsyad, M, Asrul L et al . "Supply chain analysis of dry and wet cocoa beans," IOP Conference Series: Earth and Environmental Science, 2019.

[14] M. N. F. Vinayananda CHILUR OMKARAPPA*, "Study of retail egg supply chain for quality in relation to level of sanitization and farm of origin," Turkish Journal of Veterinary and Animal Sciences, vol. 10, no. 1, 2019.

[15] J. A. H. Shaniar Tahir Mohammed*, "A Traceable and Reliable Electronic Supply Chain System Based on Blockchain Technology," ORIGINAL RESEARCH ARTICLE UHD JOURNAL OF SCIENCE AND TECHNOLOGY, vol. 4, no. 1, 2020.

[16] Zhang J, "Deploying Blockchain Technology in the Supply Chain," Computer Security Threats, 2020.

[17] Van Der Vorst J and Van Der Vorst J ,G A J, "Supply Chain Management: theory and practices Qpork-chains View project Supply Chain Management: theory and practices," IEEEAccess, p. 20, 2018.

[18] S. Manyathi1, "An Analysis of Various Types of Supply Chain Management Systems: Case of Global Public Sector versus Private Sector Procurement," Asian Journal of Social Sciences and Management Studies, vol. 4, no. 1, 2017.

[19] Types of Supply Chains." [Online]. https://www.selecthub.com/supply-chain-management/13-essential-supply-chain-management-tools/. [Accessed: 2020].

[20] Meyr H and Stadtler H, "3 Types of Supply Chains," in an overview of Supply Chains.

[21] Hofmann E and Knébel S, "Supply Chain Differentiation: Background, Concept and Examples," Journal of Service Science and Management, 2016,160-174,09(02).

[22] A. Holmberg, "Blockchain technology in food supply chains," Karlestad University, 2018.

[23] T. tubklar, scalability and resilience in humanitarian supply chain tunca tabaklar, 2017.

[24] HausmanW, "Supply Chain Performance Metrics," The Practice of Supply Chain Management: Where Theory and Application Converge ,2005,61-73.

[25] Liestyowati D, "Public Key Cryptography," Journal of Physics: Conference Series, 2020.

[26] G. Rajeev Sobti, "Cryptographic Hash Functions: A Review," IJCSI International Journal of Computer Science Issues,Vol. 9, no. Issue 2, No 2, March 2012 .

[27] S. K. Piyush Gupta, "A Comparative Analysis of SHA and MD5 Algorithm," International Journal of Computer Science and Information Technologies, vol. 5, no. 3, 2014.

[28] Bellovin S and Rescorla E, "Deploying a New Hash Algorithm," In a presentation delivered at the Rump Session of CRYPTO, 2005.

[29] M. E. a. F. M. Christoph Dobraunig, "Analysis of SHA-512/224 and SHA-512/256," ASIACRYPT, 2015.

[30] A. H. Mansour*, "Analysis of RSA Digital Signature Key Generation using Strong Prime," International Journal of Computer (IJC) , vol. 24, no. 1, pp. 28-36, 2017.

[31] A. M. J. a. A. Samsudin, "Visual Digital Signature Scheme: A New Approach," IAENG International Journal of Computer Science, vol. 37, no. 4, 2020.

[32] djangoproject." [Online]. Available: https://www.djangoproject.com/. [Accessed: 16-Sep- 2020].

[33] Bruyn A , "Blockchain an introduction Research paper,"Amasterdam University, 2017.

[34] K. G. Buck Endemann, "TECHNOLOGY FACTSHEET SERIES BLOCKCHAIN," Technology and Purpose Project | Belfer Center for Science and International Affairs, 2020.

[35] M. Crosby, "BlockChain Technology," Sutardja Center for Entrepreneurship & Technology Technical Report, 2015.

[36] J. R. Varma, "Blockchain in Finance," The Journal for Decision Makers, vol. 44, no. 1, 2019.

[37] N. O. Sadiku M,G. Eze K and M. Musa S, "Block chain Technology in Healthcare," International Journal of Advances in Scientific Research and Engineering, 2018, 154-159, 4(5).

[38] T. Alam, "Blockchain and its Role in the Internet of Things (IoT)," International Journal of Scientific Research in Computer Science Engineering and Information Technology, vol. 10.32628/CSEIT195137, 2019.

[39] Litke A , Anagnostopoulos D and Varvarigou T, "Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment," Logistics, 2019,5,3(1).

[40] K. G. E. S. M. M. Matthew N. O. Sadiku, "Smart Contracts: A Primer," Journal of Scientific and Engineering Research, 2018.

[41] Zheng Z, Xie S, Dai H et al , "An Overview on Smart Contracts: Challenges, Advances and Platforms," Future genetation computer systems, vol. 105, 2020.

[42] Y. Hu, "Blockchain-based Smart Contracts -Applications and Challenges," 18 06 2019. [Online]. Available: https://www.researchgate.net/publication/328230865_Blockchain-based_Smart_Contracts_-_Applications_and_Challenges. [Accessed 08 07 2021].

[43] Masood F and Faridi, A, "An Overview of Distributed Ledger Technology and its Applications," International Journal of Computer Sciences and Engineering, 2018, 422-427, 6(10).

[44] S. Kadam, "Review of Distributed Ledgers: The technological Advances behind cryptocurrency," in International Conference Advances in Computer Technology and Management (ICACTM), 2018.

[45] Entropy"[Online]. Available: https://en.wikipedia.org/wiki/Entropy. [Accessed: 25 July 2021].

[46] D. I. J. v. d. Vorst, "Supply Chain Management: theory and practices," IEEEAccess, p. 20, 2018.

Appendix A / (System Implemation using Google Sheets DB)

A.1. Block chain Implementation

In this section, explain implementation. First, we provide an overview of our system main needs. Second, move into detail for each of the core component the database and distributed ledger. Finally, discuss our final implementation outcome into a conclusion. Briefly, database implementation summaries in main two steps: utilizing google sheet and Jotform forms. On the Jotform side every member has a form to fill connected via email address to google document. On google sheet, have a various database fields to store product data on its different phases. System four members (farmer, factory, distributer and retailer) each has an email address on the Jotform platform linked to other users emails. This make product data available and accessible to recent members. The following screenshots illustrates various users' forms. Figure A.7 shows Jotform interface. It has five various forms (registration form, farmer form, factory form, distributer form and finally retailer form).

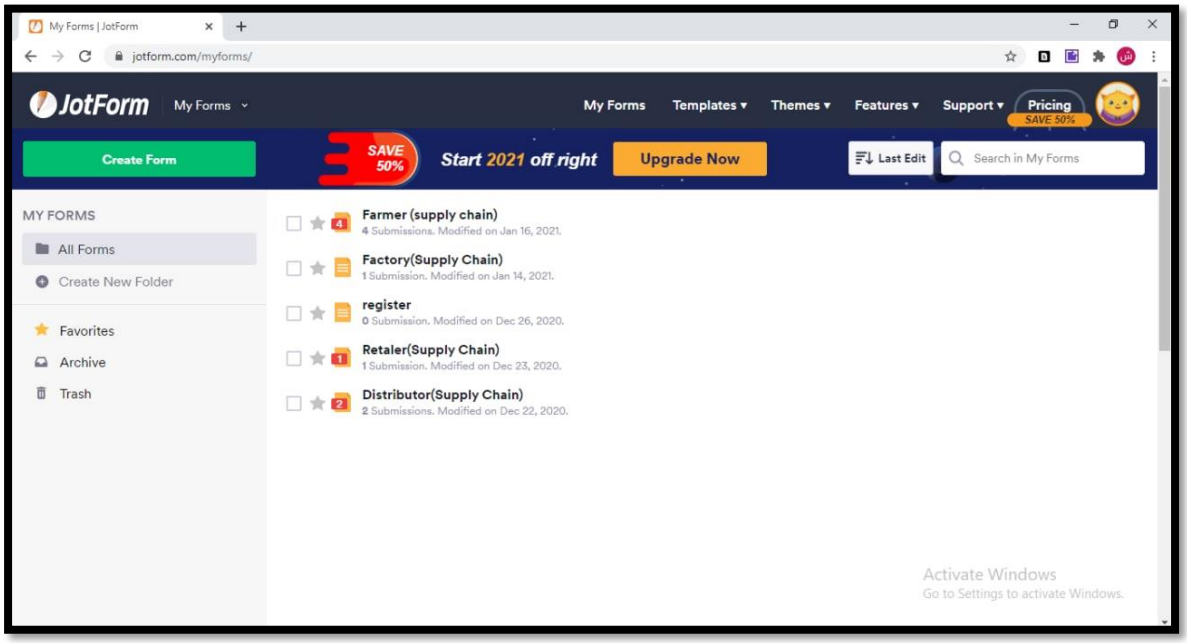

Figure A. 1: Jotform interface

In this section, are going to propose system implementation in steps.

1. After registering all users and authentication completed. System members can have fully access to jotform interface and able to fill individuals' form. The farmer is firstly filled form details and then submitit. These data are stored to a google sheet as it shows below. Every field of the form has an column in the sheet to store its data.

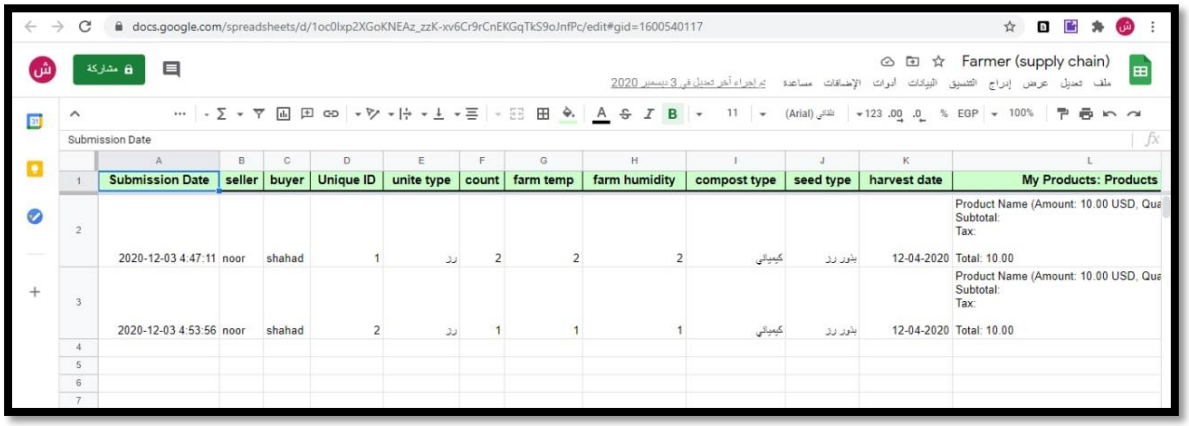

Figure A. 2: Database on google sheet

Once data stored successfully to the system and passed to the next form a thank you message shows to the users as it shows below.

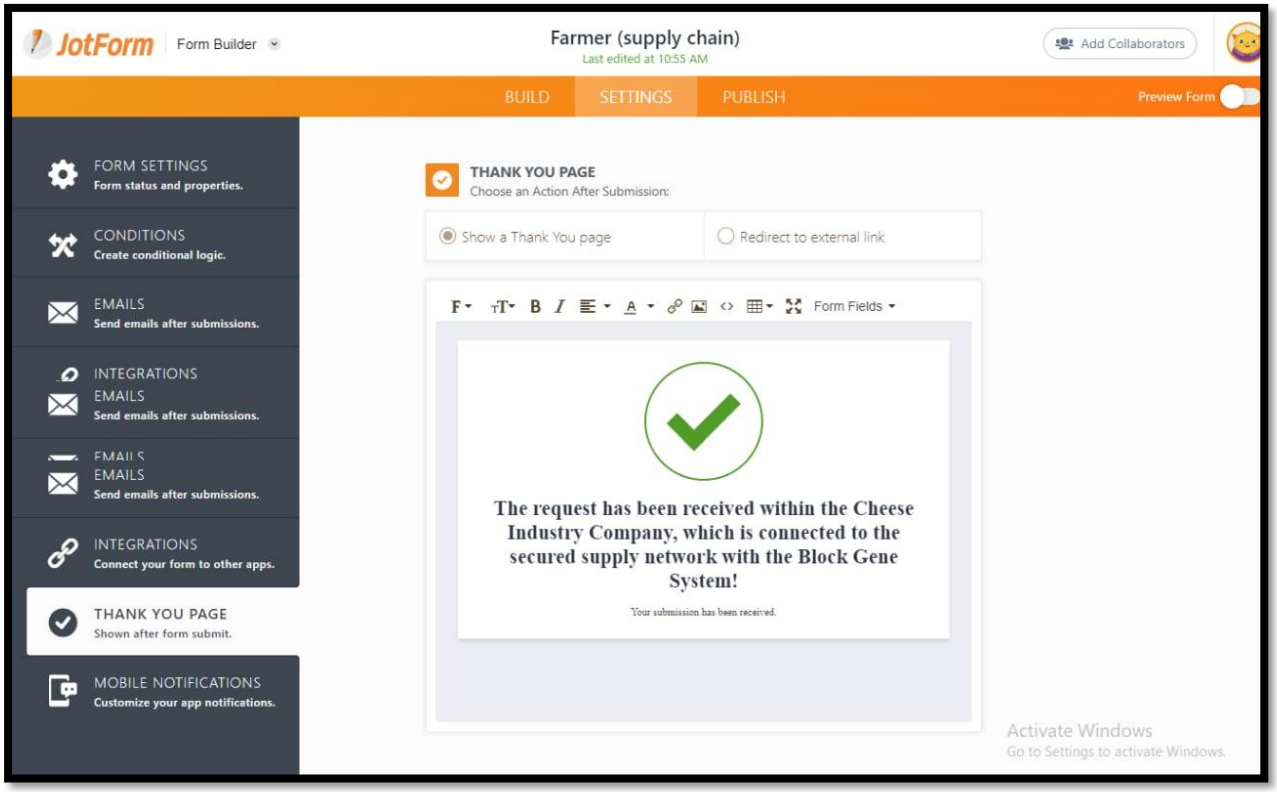

Figure A. 3: Thankyou message shows to the user once form submitted correctly

1. Farmer form will already have related records to the product significantly, it's ID that will be the same in all supply chain phases. Afterthought, the same strategy followed with distributer and retailer. They be able to view the previous information and insert the new updates to their accessed form.
2. Every member of the system has an email address to be access the database and get a notification once a new information received.
3. Finally, all previous sheets which are represented the database are collected to a distributed ledger.

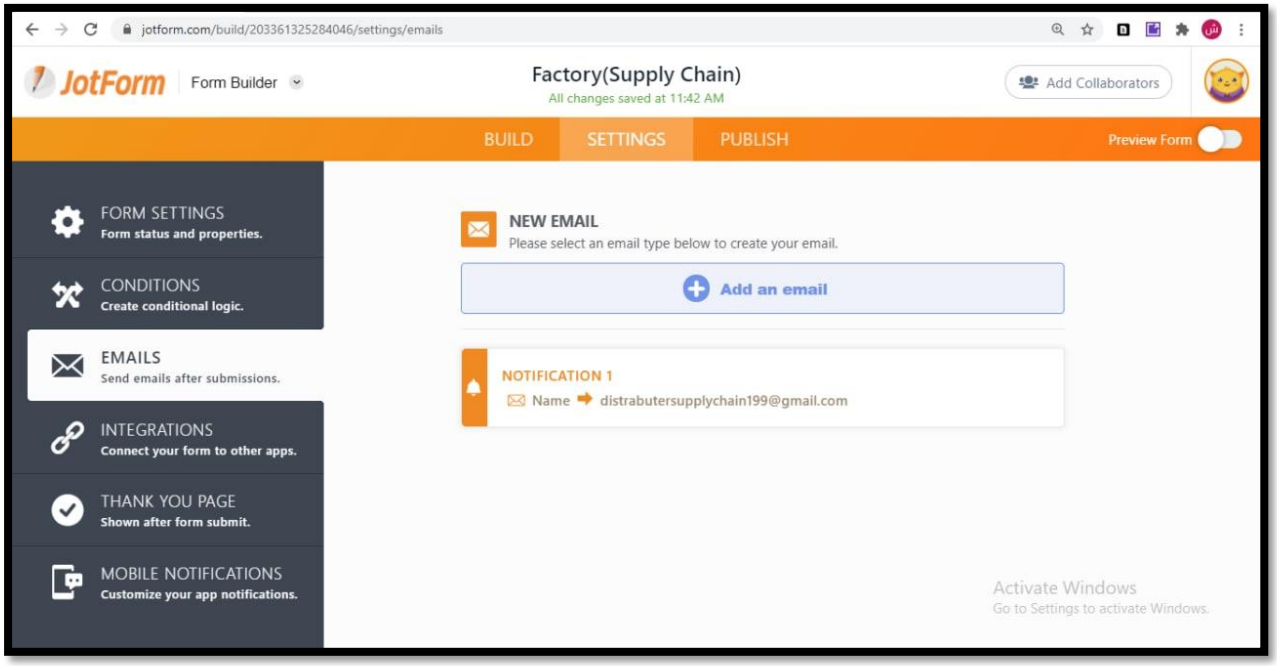

Figure A. 4: Factory has a new email send to alert user on new data updated on from the previous form

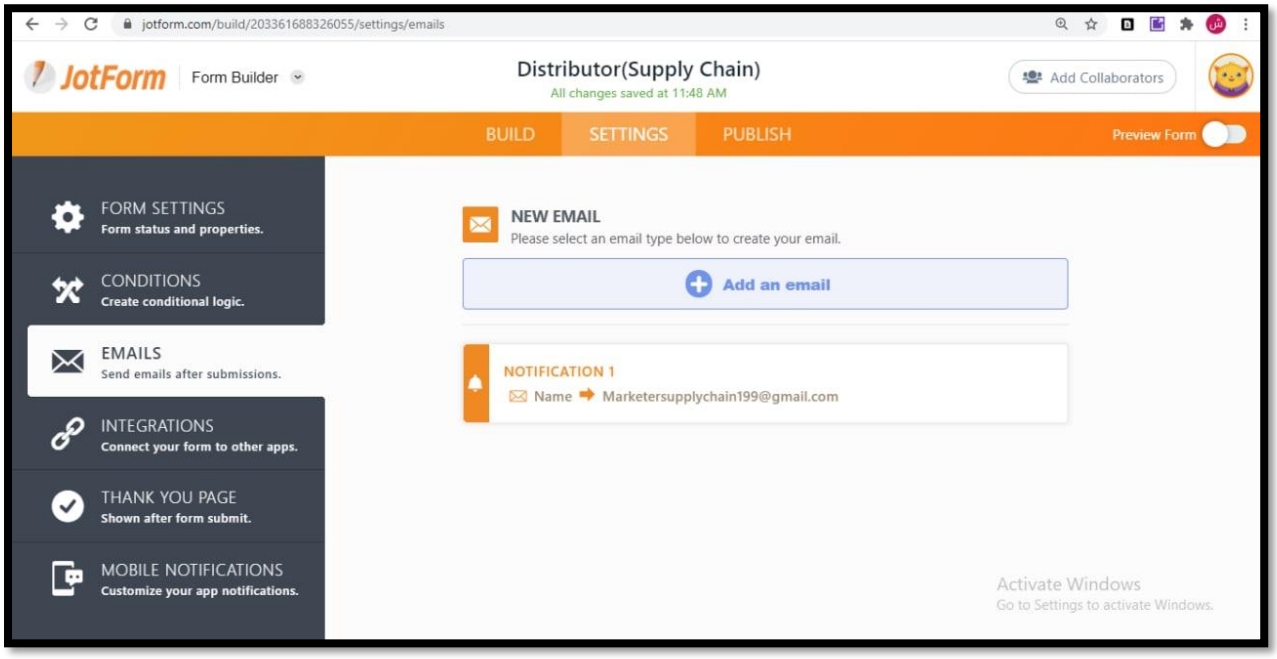

Figure A. 5: distributer has a new email send to alert user on new data updated on from the previous form

In order to describe the efficiency and feasibility of the presented system, a case study has been proposed. Typically, the food traceability system is performed in insignificant appropriate product version. The proposed system is designed and managed under the Hyperledger Fabric. It is designed as a framework for developing applications or solutions with a modular architecture. The system depends on the data inserted by the farmer, which includes the general product information. This data is stored inside a ledger in the Jotform server. Next, an update is shared by the factory. After that, the distributor enters the next update to the product's information. Finally, it reaches the retailer. Using the product ID, the retailer will be able to view product information. For data setup, three nodes are deployed to evaluate the system. Each node represents a known organization that uses the distributed ledger information to trace food. The following figures illustrate the graphic representation of the inserted ledgers and the results that are obtained.

Distributor

The distributed ledger is the result of product information, which shared by network user and make customers, trace their goods information and current position. Finally, the peer-to-peer nodes represent the Ministries of Agriculture and Trade, which are connected and able to access data in the distributes ledger. Each node has individual information such that they can communicate with each other.

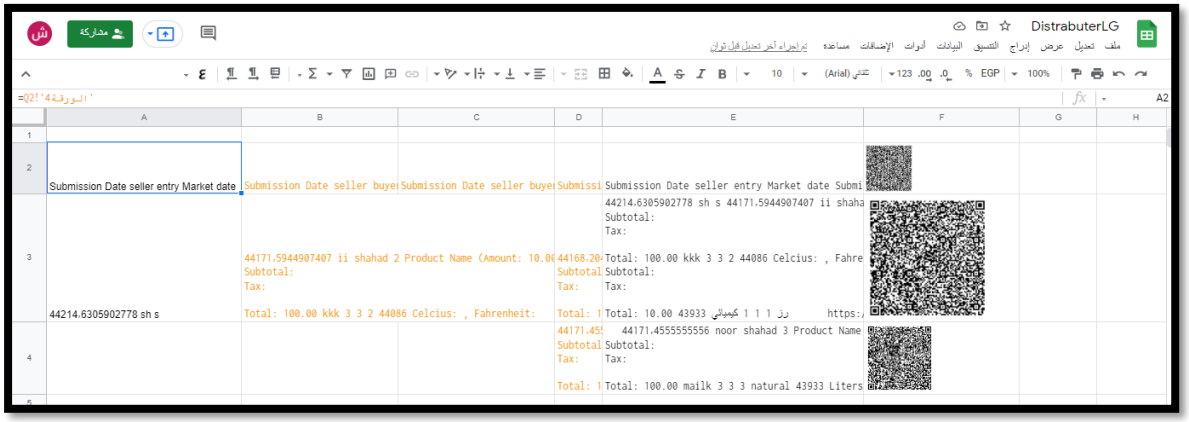

Figure A. 6: Supply chain and distributed leger

As a result, a number of advantages have been observed with the proposed system. First, it is a reliable system that leads all participating nodes to directly inform when a product's information changed. Therefore, it prevents data manipulation and product stealing. Second, it is a model that links system entities to a supply chain network and stores these entries in a register distributed by many nodes. This large number of nodes involved in the block chain enables the end user to track the stages and origins of each product in the chain.

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة بابل كلية تكنولوجيا المعلومات
قسم شبكات المعلومات

نظام التتبع الامن للمنتجات الزراعية

رسالة

مقدمة إلى مجلس كلية تكنولوجيا المعلومات في جامعة بابل كجزء من متطلبات
الحصول على درجة الماجستير في تكنولوجيا المعلومات / شبكات المعلومات

من قبل
شهد سليم خضير كريم

بإشراف
أ. م. د. أمير كاظم هادي

1443هـ 2021 م

الخلاصة

سلسلة التوريد عبارة عن سلسلة من الإجراءات التي تتضمن اتخاذ القرارات وتنفيذ المواد والأموال وتدفق المعلومات بهدف الوصول إلى متطلبات العملاء النهائية. يمر هذا الإجراء بعدد من مراحل سلسلة التوريد المختلفة. تمثل سلسلة التوريد محاذاة الشركات التي تقدم المنتجات أو الخدمات إلى السوق. تتمثل إحدى التحديات الرئيسية التي تواجه نقل البيانات عبر الشبكة في كيفية الحفاظ على البيانات سليمة أثناء نقلها من المصدر إلى الواجهة، خاصة مع وجود العديد من المتسللين والهكرز. تتمثل إحدى تقنيات حماية البيانات في الاعتماد على خوارزميات التشفير والتجزئة لإنشاء توقيعات من البيانات الأصلية المرسلة معها إلى الوجهة. عند وصول البيانات إلى الواجهة، يتم إعادة إنشاء نفس التوقيع باستخدام نفس الخوارزميات ويتم مقارنة التوقيعين. إذا كانت متطابقة، فهذا يعني أن البيانات لم تمس. خلاف ذلك، يشير أي اختلاف في التوقيعات إلى تعديل البيانات.

في هذه الأطروحة، تم تصميم نظام تتبع سلسلة التوريد باستخدام بعض الأساليب الأمنية مثل HMAC والتي تضم RSA و SHA512 والعقود الذكية لإنشاء التوقيعات لإرسالها مع البيانات. في مثل هذه العقود، يحدد المصنعون تكوين المنتجات ويتتبعون مصدرها لمنعها من التلاعب. يتم تقييم نتائج النموذج المقترح التي تم الحصول عليها من خلال سلسلة التوريد وخوارزميات HMAC و RSA من حيث استهلاك الوقت ، والذي وجد أنه منخفض نسبيًا (يتراوح بين 0-9 ثوانٍ). يتم قياس الكفاءة والدقة باستخدام الانتروبي. فيما يتعلق بالدقة وأمن المنتج، تم استخدام التوقيع لضمان عدم حدوث حالات تلاعب خلال مراحل الشراء أو البيع أو النقل.

تم التوصل إلى نتيجة أن استخدام سلسلة التوريد، جنبًا إلى جنب مع خوارزميات HMAC و RSA داخل بيئة Django كنموذج واحد، يوفر بالفعل الأمان والخصوصية. يخلق هذا المزيج إطار عمل فعال من حيث توفير الوقت وقابلية التوسع، وتوفير نتائج عالية الدقة وموثوقة في أقل من دقيقة، بالإضافة إلى سهولة التعامل بين الأطراف. كما أنه يقلل من الجهود والتكاليف، وبالتالي يمثل بديلاً أقل تكلفة نسبيًا مقارنة بالآخرين من حيث النقل والاتفاقيات والحفاظ على أمان بيانات المنتج.