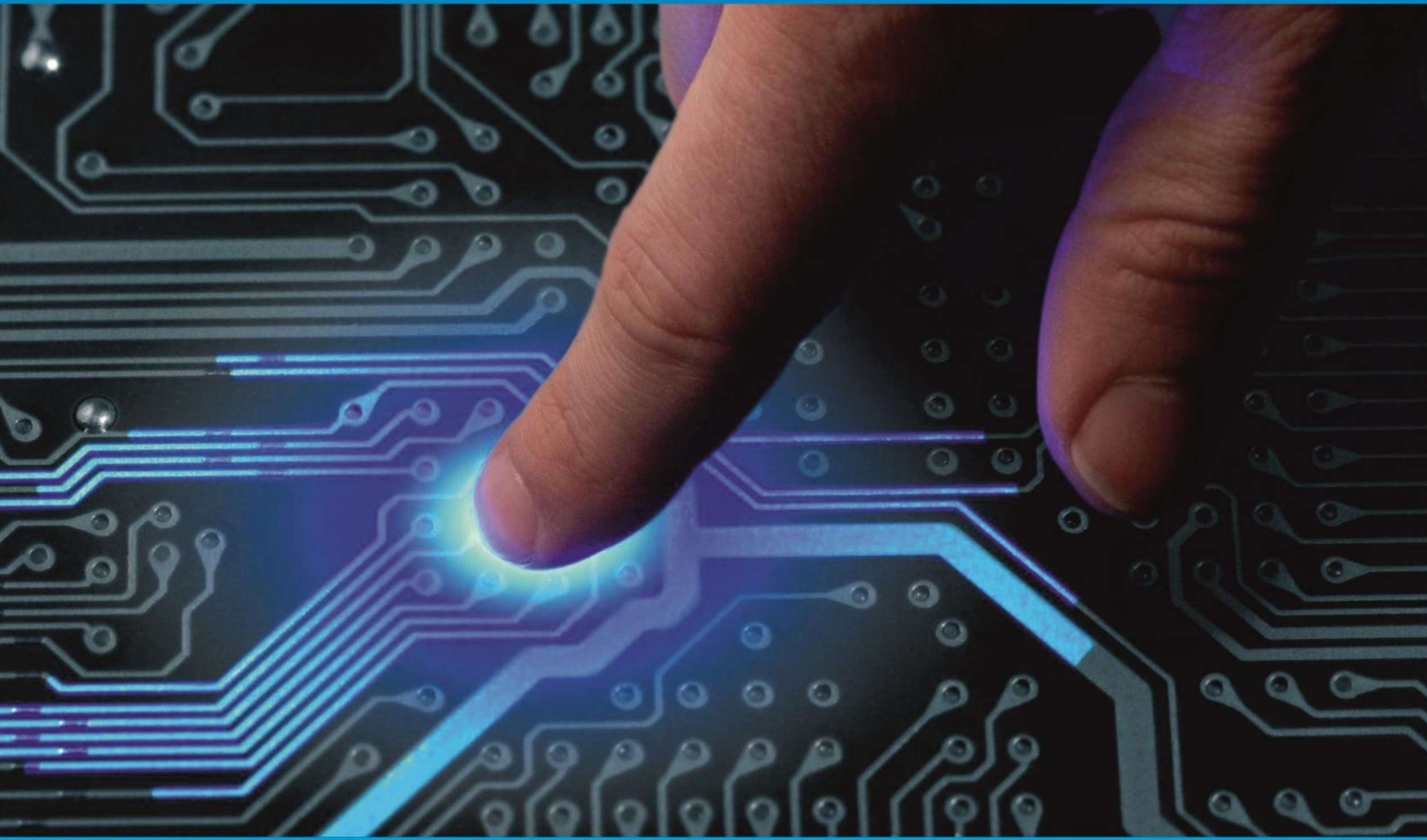
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 4, April 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904092 |

Cryptography Based Support Commodity Distribution System

Shardul Rajeev Mulay[1], Advait Vinay Naik[2], Ajay Rajendra Pandit[3], Prof. Keerti D. Kharatmol[4]

BE Student, Department of Computer, KC College of Engineering & Management Studies & Research, Thane (E), Maharashtra, India[1]

BE Student, Department of Computer, KC College of Engineering & Management Studies & Research, Thane (E), Maharashtra, India[2]

BE Student, Department of Computer, KC College of Engineering & Management Studies & Research, Thane (E), Maharashtra, India[3]

Assistant Professor, Department of Computer, KC College of Engineering & Management Studies & Research, Thane (E), Maharashtra, India[4]

ABSTRACT: In developing countries, there are several commodities and services which are financially supported by the government as financial aid to their citizens. This Distribution of Commodities like grains, cooking gas, and others follow a very archaic manual distribution process. This typical and manual process is time and effort consuming for the government and also at the same time is weak in terms of control and monitoring. The middle non-governmental entities involved in the process can smuggle these commodities outside the legal channels for double profit-seeking or intentional political reasons. When scenarios like these arise, public money gets wasted and the people who were supposed to be the beneficiaries are left with dissatisfaction. This paper introduces a model for solving this problem by increasing the control of the whole process and thus decreasing the smuggling and wasting rates. The proposed model defines a centralized entity that is primarily responsible for the accounting of the flow of the distribution chain, which is in turn authenticated and monitored by another trusted third-party entity. This monitoring and accounting are enabled by using various cryptographic algorithms.

KEYWORDS: Cryptography, Public Distribution System, Elliptic Curve Cryptography, Digital Signature, Encryption, Improved Public Distribution System

I.INTRODUCTION

Everyone is aware of the drawbacks of the manual systems for commodity distribution. Because of their decentralized structure and involvement of several intermediaries, they are vulnerable to leakages and unaccountability. The proposed model is supposed to solve these problems. To mitigate and avoid unfortunate illegal activities in the Distribution procedure the governments in the developing world can make use of Digital Distribution Systems. With the emergence of cheap smartphones and Internet connections, it is now possible to make use of cryptography-based online applications to provide these services. Many countries in the world use the old distribution process. India is also one of those countries and the introduction of the proposed model can bring better control and reduce the leakages in the system. The paper starts by providing a general idea about the contemporary distribution procedure in India and then goes onto highlighting its various drawbacks. Then it shows how the proposed model can be used to solve the issues pertaining to the old model. The paper goes into the details of the motivation behind the model and its working.

The rest of this paper is organized as follows. Section II showcases the literature review. In Section III, we introduce the current public distribution system (PDS). In Section IV, we introduce the various cryptographic techniques used in the model. Section V goes into the details of the actual structure and working of the model. Section VI showcases the advantages of the proposed model over the older model. Section VII highlights the Future Scope of the model i.e., improvements that can be made to the project.

II. LITERATURE REVIEW

1) Mohammed A. Hassouna "A Secure Governmental Supported Service Distribution Model Using Identity-based Cryptography", International Journal of Computer Science and Information Security (IJCSIS), Vol. 18, No. 5, May 2020.

This paper uses a different approach to achieve the goals intended to be solved by our model. This paper was the inspiration behind the proposed system.

2) D.Lavanya Kumari, Prof. K. Santha Kumari "Public Distribution System in India: An Overview", Indian journal of applied research, May 2015
This paper describes the importance of the Public Distribution System in India. It also goes on to highlight the weaknesses of the system. The proposed model is intended to address these issues in the contemporary PDS.

3) Neal Koblitz "Elliptic Curve Cryptosystems", Mathematics of Computation, January 1987.
This paper describes the Elliptic Curve Cryptography (ECC) technique that we are using in the proposed model. This paper explains the mathematical theory behind Elliptic Curve Cryptography. It highlights the advantages of ECC over other older crypto techniques.

4) AbdessalemAbidi, BelgacemBouallegue, Fatma Kahri. "Implementation of Elliptic Curve Digital Signature Algorithm"
This paper explains the Digital signature application of ECC i.e., ECDSA. ECDSA is a variant of DSA which uses ECC for asymmetric cryptography. This paper describes the theory and implementation of the ECDSA algorithm. The paper also points out the advantages of using ECDSA over RSA based digital signatures.

5) Joan Daemen, Vincent Rijmen "AES Proposal: Rijndael", International Carnahan Conference on Security Technology, September 1999
This paper describes the AES symmetric cryptography algorithm used in the model. The paper goes into the details of AES's implementation and the mathematical theory behind it. The AES Encryption algorithm replaced the older vulnerable DES algorithm. This is the proposal of the same.

III. CURRENT PUBLIC DISTRIBUTION SYSTEM

The central and state governments share the responsibility of regulating the PDS. While the central government is responsible for procurement, storage, transportation, and bulk allocation of food grains, state governments hold the responsibility for distributing the same to the consumers through the established network of fair price shops (FPSs). State governments are also responsible for operational responsibilities including allocation and identification of families below the poverty line, issue of ration cards, and supervision and monitoring the functioning of FPSs.[2][3]

A public distribution shop, also known as a fair price shop (FPS), is a part of India's public system established by the Government of India which distributes rations at a subsidized price to the poor [7]. Locally these are known as ration shops and public distribution shops, and chiefly sell wheat, rice, and sugar at a price lower than the market price called Issue Price. Other essential commodities may also be sold. To buy items one must have a ration card. These shops are operated throughout the country by joint assistance of the central and state government. The items from these shops are much cheaper but are of average quality. Ration shops are now present in most localities, villages, towns, and cities. India has more than 5.5 lakh (0.55 million) shops, constituting the largest distribution network in the world.

Shortcomings of the current model:

- Illicit fair price shop owners have been found to create a large number of bogus cards to sell food grains in the open market.
- Many FPS dealers resort to malpractice, illegal diversions of commodities, holding, and black marketing due to the minimum salary received by them.
- Rogue dealers swap good supplies received from the Food Corporation of India (FCI) with inferior stock and sell the good quality FCI stock to private shopkeepers.

The information mentioned above was taken from [2],

The current Distribution system is mostly undigitized. It highly depends on manual accounting. The shortcoming mentioned above can be easily dealt with by the introduction of the proposed model.

IV. CRYPTOGRAPHIC TECHNIQUES USED IN THE MODEL

- Elliptic Curve Cryptography Digital Signature (ECDSA)

Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC allows smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security.[4]

Elliptic curves are applicable for key agreements, digital signatures, pseudorandom generators, and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme. The proposed model uses the Digital Signature Scheme called ECDSA from this family of cryptographic techniques.

The main advantage of choosing this scheme over any other old scheme like RSA is that this scheme requires comparatively smaller keys. It also provides more security for the same length of key than that might be provided in RSA [5].

We are using this scheme to digitally sign the transactions which would be stored in the primary server responsible for accounting, while the keys for it would be present on the Trusted Third Party (TTP) Server.

- Advanced Encryption Scheme (AES)

The Advanced Encryption Standard (AES), also known by its original name Rijndael is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

AES is a subset of the Rijndael block cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192, and 256 bits [6].

AES has been adopted by the U.S. government. It supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

We are using this algorithm to securely encrypt the previously stated ECDSA keys on the TTP. Encryption of these keys through AES provides better security and confidentiality to the system.

- Secure Hash Algorithm (SHA 2 - 256)

SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA) and first published in 2001.They are built using the Merkle–Damgård construction, from a one-way compression function itself built using the Davies–Meyer structure from a specialized block cipher.

SHA-2 includes significant changes from its predecessor, SHA-1. The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. SHA-256 and SHA-512 are novel hash functions computed with eight 32-bit and 64-bit words, respectively. They use different shift amounts and additive constants, but their structures are otherwise virtually identical, differing only in the number of rounds. SHA-224 and SHA-384 are truncated versions of SHA-256 and SHA-512 respectively, computed with different initial values. SHA-512/224 and SHA-512/256 are also truncated versions of SHA-512, but the initial values are generated using the method described in Federal Information Processing Standards (FIPS) PUB 180-4.

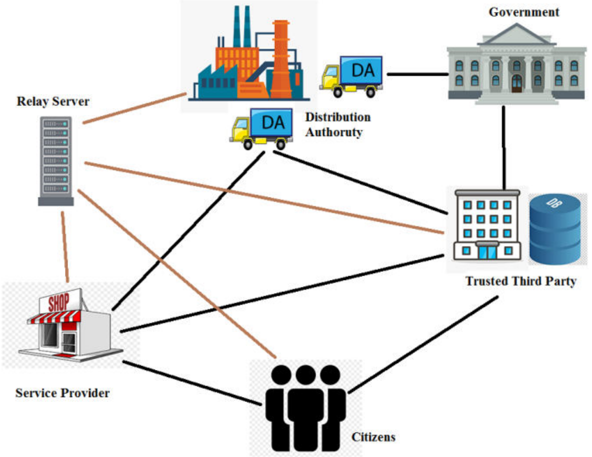
SHA-2 was first published by the National Institute of Standards and Technology (NIST) as a U.S. federal standard (FIPS). The SHA-2 family of algorithms is patented in US patent 6829355. The United States has released the patent under a royalty-free license.

We are using SHA-2, particularly SHA256, an algorithm for generating hashes for digital signature. A transaction's digital signature would be its SHA256 hash signed with ECDSA private key.

V. THE PROPOSED SYSTEM FOR COMMODITIES DISTRIBUTION

In this section, we introduce the proposed model/system for distributing commodities to their deserved consumers/citizens through a systematic process.

A. General overview of the proposed model



entities present in the system.

We’re going to start by first defining various entities (Servers, Consumers & Intermediaries) in the system.

- Users:

Citizens/Consumers:
Citizens are the end-consumers. They receive their goods and services from their local Supplier (SP) i.e., fair price shops.
Supplier / Shopkeeper (SP):
SPs are at the end of the Distribution Chain. They are responsible for providing services to the end-user i.e., Citizens.
Distribution Authority (DA):
DAs are responsible for distributing goods to local shops. They take orders from shops for commodities and deliver them.

- Servers:

Trusted Third Party [TTP]:
As the name suggests the server belongs to a trusted non-governmental organization. The role of this organization is to keep a watch on the distribution process.
The TTP is responsible for managing the keys of the users involved. These keys are used for digitally signing transactions and thus giving legitimacy to the transactions. The TTP is also responsible for generating such keys for every user during their registration. The algorithm used, as mentioned earlier, is ECDSA. This server generates a pair of Public and Private keys for each user. The server is responsible for securely storing these keys in its database (Symmetric key cryptography can be used to encrypt the database). The server provides endpoints for users to sign their transactions before submitting them to the primary accounting (Relay) server. The server can also provide APIs to later verify these signatures and make the primary server accountable. This server can also act as a trusted payment gateway for the user's transactions. The concept of TTP was inspired by[1].

Relay Server [RS]:
This server is responsible for providing a channel of communication (relaying messages) between the several users (citizens and intermediaries) involved in the process. This essentially means providing a way to communicate the requirements of goods to the provider. This server keeps these requests (transactions) in its database for accounting purposes. The transactions are also authenticated by digital signatures from the users which are provided by the TTP. In this way, the server’s activities are accounted for by the third party mentioned above.

B. The Proposed Functioning of the System

In order to implement such a system, we need a secure app installed on the customer's and intermediary's machines. This app could be a website or a mobile/Desktop application. This app will communicate with the aforementioned servers and carry on the following process.

The terms requester and provider used in this section refer to the user requesting items and the user responsible for delivering those items respectively. In the case of citizens ordering items from shopkeepers (Supplier), the citizen is the requester and the supplier is the provider. The same goes for supplier and distributor. Supplier is the requester when it orders items from its local distributor, the provider.

The following steps will be followed by the requester and provider:

- The requester initiates a request for certain commodities with the provider.
- Then it digitally signs the request through the TTP. The request along with its signature is then sent to the Relay Server.
- The relay server processes the request and finds out if the request is valid. The request is valid if the items ordered are within the customer's quota limits and the provider has the stock of the items ordered. If the request is valid, the order is placed and the quota and stock information are updated accordingly. As the order is placed, the provider is made aware of this new order.
- The next step is the payment of the items ordered. This is done by the requester through the TPP's payment gateway. The payment token is then digitally signed as before and stored on the Relay Server. The provider is again made aware of the payment success.
- The last step in the process is the actual delivery of the goods. When the commodities are delivered to the requester the provider verifies the requester with a QR code.
- This verification of the requester is the verification of actual contact between the provider and requester. The QR code will contain the requester's confirmation token signed with its private key. The provider submitting this token to the Relay server will mark the end of the transaction. This means that the requested goods have been successfully delivered to the intended requester.
- Every time any user (provider as well as requester) is submitting something to the Relay server, it is providing its digital signature. This digital signature could be later verified to check the authenticity of the Relay Server. Through this mechanism, the TTP keeps a watch on the Relay server.

VI. RESULTS

- The Digital nature of the proposed system mitigates the drawbacks of the current system.
- It guarantees accounting of each transaction in the system in a centralized fashion, which solves the issue of leakages. While at the same time the model is centralized, it envisions a trusted third party to monitor the process.

VII. CONCLUSION AND FUTURE WORK

This commodity distribution system can help in minimizing the malpractices that happen in traditional systems. This model is not only a centralized digital alternative to replace the old process. It also envisions a trusted third party to keep an eye on the whole process and thus improves the overall security of the process.

Some screenshots of the app UI

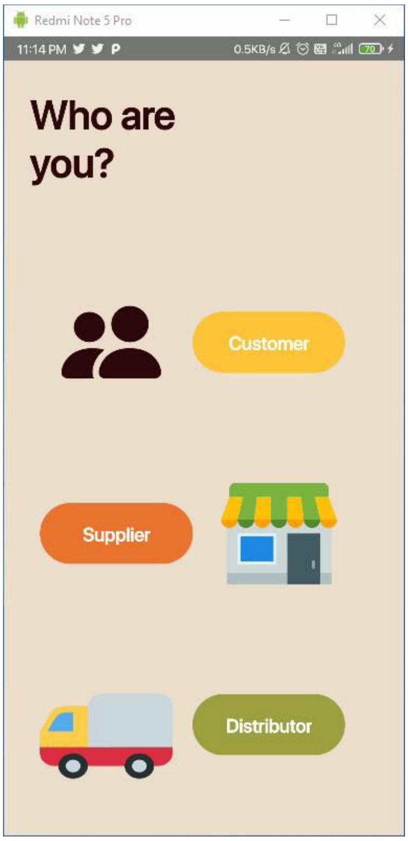
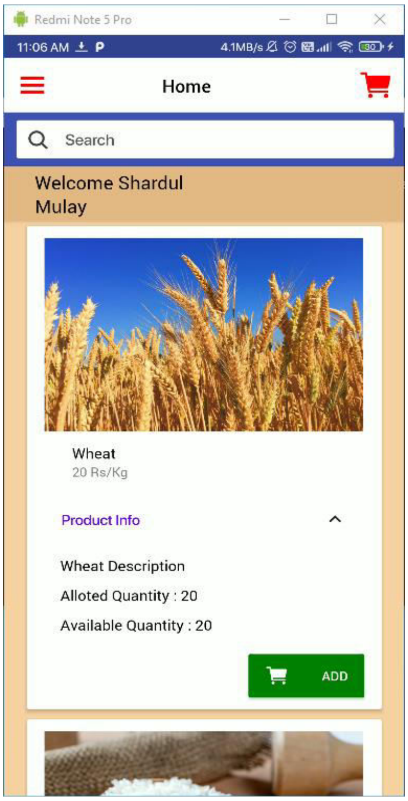


Fig. 1: Choose the type of user



Welcome Shardul Mulay

Wheat
20 Rs/Kg

Wheat Description
Alloted Quantity : 20
Available Quantity : 20

Fig. 2: Home screen for customer

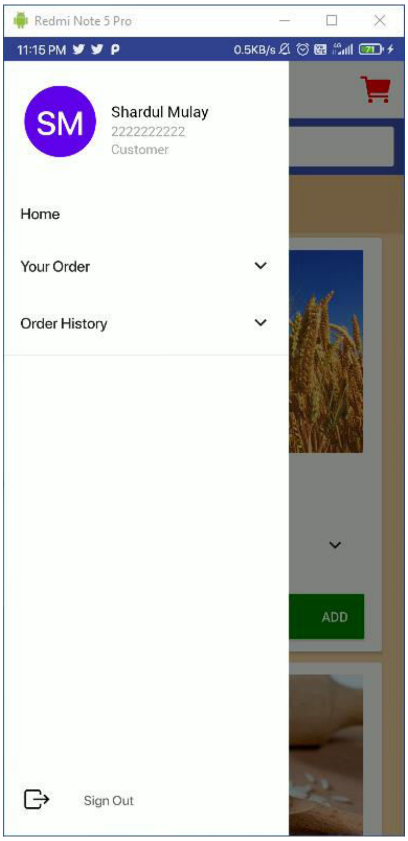
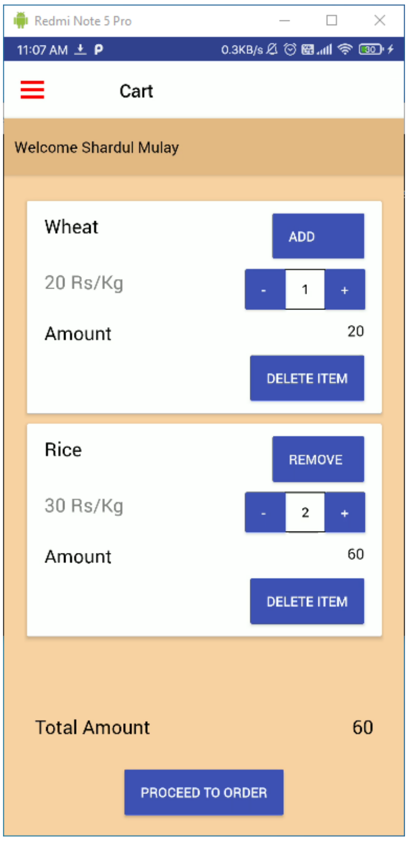


Fig.3: Drawer menu with options related to the user type



Welcome Shardul Mulay

Wheat

20 Rs/Kg 1

Amount 20

Rice

30 Rs/Kg 2

Amount 60

Total Amount 60

Fig. 4: Customer's cart

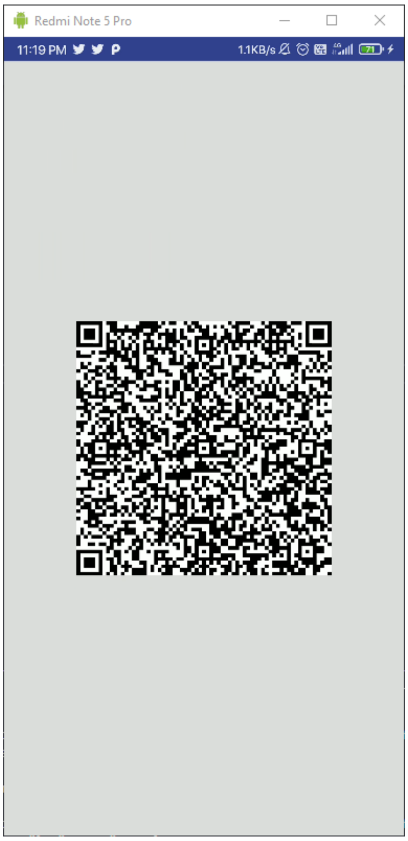


Fig.5: QR-code screen for confirmation of delivery

We can add more cryptographic mechanisms to the process to make the Relay Server more accountable and improve the authenticity of data.If better variations of the cryptographic techniques used are available in the future, they can be added to improve the overall security of the project. Additional security could be provided with Biometric authentication.

REFERENCES

[1] Mohammed A. Hassouna “A Secure Governmental Supported Service Distribution Model Using Identity-based Cryptography”, International Journal of Computer Science and Information Security (IJCSIS), Vol. 18, No. 5, May 2020.

[2] “Public Distribution System in India". Indian Institute of Management Ahmedabad. Retrieved 5 October 2011.

[3] D. Lavanya Kumari, Prof. K. Santha Kumari “Public Distribution System in India: An Overview”, Indian journal of applied research, May 2015

[4] NealKoblitz “Elliptic Curve Cryptosystems”, Mathematics of Computation, January 1987.

[5] AbdessalemAbidi, BelgacemBouallegue, Fatma Kahri. “Implementation of Elliptic Curve Digital Signature Algorithm”, Global Summit on Computer & Information Technology, June 2014.

[6] Joan Daemen, Vincent Rijmen “AES Proposal: Rijndael”, International Carnahan Conference on Security Technology, September 1999

[7] “Public Distribution System". Ministry of Consumer Affairs, Food and Public Distribution (India). December 2010.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details