SBFR: SHA Based Fingerprint Recognition for Secured Smart Ration Management System

V. Kovendan[1], B. Ramyabharathi[2], G. Haritha[3]

[1]*Assistant Professor, Department of CSE, Arasu Engineering College, Kumbakonam, Tamil Nadu, India*
[2, 3]*M.E Student, Department of CSE, Arasu Engineering College, Kumbakonam, Tamil Nadu, India*

Abstract: **- Finger print recognition is an efficient method of identifying an individual. Fingerprint is one of the most well-known biometrics solutions for verification on electronic systems. Finger print security applications arefrequently upgraded on infrared cameras and video cameras for providing security system such as logins and transaction authentications. Hence this technology is implemented in the newly designed smart rationing system. The present system in the ration shops is like the shopkeeper sees the ration book of the user and gives the quantity of grocery the user asks for. Nevertheless there will not be proper constancy in supplying the grocery things to the customer. Every now and then even there may be coincidental that different customerstaking the grocery on same ration cards and also used by unauthorized persons. To avoid all these issues, we have proposed secure finger print recognition for card less and automatic smart ration management system with high security.**

Keywords: **ATMEGA- Microcontroller,Finger print, Google Cloud Msg, SHA, Smart PDS.**

I. INTRODUCTION

Public distribution system is amajor commodities distributed embraceprimary food grains, such as wheat, rice, sugar, and kerosene, over and done with a system of fair price plantsto established in quite a lot of states across the country. Food Organization of India, aadministration entity, accomplishes the public distribution system. The scheme is frequently blamed for its inefficiency and rural-urban bias. It has not been able to fulfill the objective for which it was formed card .Government of India provides various facilities for ration distribution towards poor and needy people. In months, if not buy the materials at the end of the month, they will sale to others without any intimation to the government and customers, so the shopkeepers are misusing of these materials by selling in the market and doing corruption. Public Distribution System is one of the widely contentiousproblems that implicatemisuse. The proposed system aids to control the corruption which is taking place in ration shop by replacing manual work with automatic system based on ATMEGA microcontroller [3]. We can also add, update and delete the details of the family member's information easily. Once consumer is validated by Finger print template [2], the system asks the consumer to select appropriate material and quantity of material through keypad and consumer willget material.GCM interfaced with microcontroller sends information in the form of SMS to related people. The proposed automatic finger print ration shop system would bring transparency in public distribution system and become helpful to prevent malpractices.

1.1 Existing Work

In the previous PDS public distribution system (fig.1) shopkeeper checks the ration card of the consumer and then provides the grocery items as the user asks for. User information is maintained by them which is not secured and there will not be proper regularity in providing the grocery items, and customers information and grocery item can able to access by third party so it leads to theft of customers information.

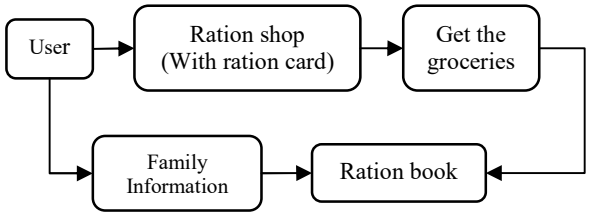

Fig.1 PDS Ration System

1.2. Related Work:

GCM (fig.2) uses XMPP protocol for message generation purpose. Where the XMPP and HTTP protocol are interconnected with the Google cloud messaging server with the help of these two protocol GCM server will send an SMS to the consumer's mobile phone.

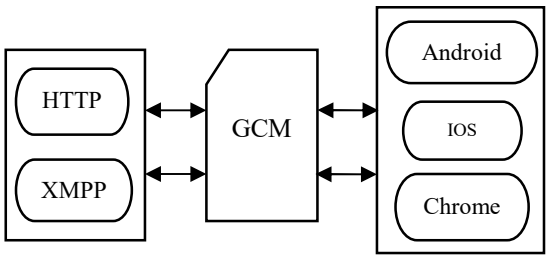

Fig.2 Google Cloud Messaging

II. PROPOSED CONTRIBUTION

Proposed system aids to control the corruption and provides the commodities to the needy and poor people

regularly. In this system we develop a web application for maintaining the ration networks data stored in the data base and it stores the member's information with finger print recognition based authentication. SHA-256 algorithm provides high security compared to other algorithm to the user's data. Only with the help of user's finger printdata, their information can be stored and retrieved.

Every consumer has a unique own finger print id which is registered by the Government authority. From this system we can avoid the misuse of our card by others and this system is highly secure with this system we can add, update, and delete the family members in to the ration network instantly. It is an automated process, manual intervention is less and there is no need of keeping an account of all purchased details in the notebook. All the details are stored in the database and the purchased details are notified to the consumers by sending an SMS to the family members registered number. The purchased overall groceries are updated in the government database, so that this process will avoid corruption.

III. IMPLEMENTATION

From the above review study we are going to implement finger print recognition based ration management system (fig.3), finger print recognition refers to the automatic method of identifying or confirming the identity of an individual based on the comparison of two finger print templates [8]. Finger printrecognition is one of the most well-known biometrics and it is by far the most used biometric solution for authentication on computerized systems.

The ration system is only based on the finger printauthentication. Each user must be authenticated with finger printstored template, if the stored data is matches with users scanned finger printdata, then the user will get access to use their ration card information, not only the user,our system includes the shopkeeper to use his unique finger printto open the system. First we store all family members' information with finger print template in the database for authentication, so using this system one of the family members can buy grocery items of over smart ration card. The system must include the display which must show the following information's

User 1

Card no.:8975538244

Balance material: rice-20kg, oil-5 liter

Delivered material:12.35pm,06/2/2017

Available material in ration shop:

Rice-100kg, oil-50litre, wheat-200kg

User 2

Invalid id

Fig.3 Automatic rationing system

IV. METHODS AND ALGORITHMS

The existing conventional ration distribution system has two basic issues one is renewing the ration card every year and corruption done by the employees by selling the grocery items in market with less price this can be overcome by using finger printsystemand Google cloud messaging (GCM) [6] is a globally accepted standard for digital cellular communication. This system can be implemented with help of ATMEGA microcontroller [3].

A. SHA Algorithm:

Hash functions transform arbitrary large bit strings called *messages*, into small, fixed-length bit strings called *message digests*, such that digests identify the messages that produced them with a very high probability. Digests are in that sense finger print: a function of the message, simple, yet complex enough that they allow identification of their message, with a very low probability that different messages will share the same digests [7]. In SHA-256, messages up to 2^{64} bit (2.3 hexabytes, or 2.3 billion gigabytes) are transformed into digests of size 256 bits (32 bytes). For perspective, this means that an object 7 times the size of Facebook's data warehouse in 2014passed to SHA-256 would produce a chunk of data the size of a 32-letter string of ASCII characters, and that string would the object's very special finger print.

$$\text{SHA} - 256: \quad B^1 U \dots U B^{64} \rightarrow B^{256}$$

$$\text{M} \rightarrow \quad H$$

A prominent use case of hashing is *data integrity verification* of large files, which relies on the comparison of actual and expected message digests, or*checksums*. Another is hashing as part of the encryption/decryption journey. Before a *message* can be encrypted with an algorithm like RSA, it needs to be hashed. In the rest of this article, we explore what hashing does to a message; with a view to later develop a better understanding of RSA.

Pre-processing: Hashing with SHA-256

Padding If we note M the message to be hashed, and l its length in bits where $l < 2^{64}$, then as a first step we create the padded message M', which is message M plus a right padding, such that M' is of length l', a multiple of 512. Specifically, we use padding P such that M' is:

Blocks M' is parsed into N blocks of size 512 bits, M^1 to M^N, and each block is expressed as 16 input blocks of size 32 bits, M_0 to M_{15}.

Hash initialization. The initial hash value H^0 of length 256 bits (8 input blocks of 32 bits) is set by taking the first 32 bits of the fractional parts of the square roots of the first eight prime numbers:

Algorithm:

The hash is produced by processing each message block M^i of M' in order. For each of message block M^i:

1. Message schedule- We create a message schedule W^i, consisting of four 512-bit message blocks (each made of 16 input blocks). The first block of W^i is message block M^i, and the next three blocks are variations of M^i, obtained through the formulas in the illustration below:

A detail: note that if we align all message schedules W^i vertically, the first column reads from top to bottom as the complete message $M' = M^1 \| .. \| M^N$.

2. The big shuffle. The input blocks of message schedule W are fed, one after the other, to a function represented below as a graph. The graph takes as inputs a hash $\omega^i(t)$ and a message schedule input block $W^i(t)$, and outputs a hash $\omega^i(t+1)$. The initial hash $\omega^i(0)$ fed to the graph is the intermediate hash H^{i-1}: in the case of W^1, it's H^0 defined in the pre-processing step.

$\omega^i(0)$ and $W^i(0)$ produce $\omega^i(1)$;

in turn $\omega^i(1)$ and $W^i(1)$ produce $\omega^i(2)$, etc., until $\omega^i(63)$ is produced.

3. New hash. After all input blocks from W^i have been used and we $\omega(63)$ has been created, we can create the new hash H^i such that each input block of H^i is the sum of the corresponding input block of H^{i-1} plus the corresponding input block of $\omega^i(63)$:

$H^i(j) = H^{i-1}(j) + \omega^i(63)(j)$ where + is the addition modulo 2^n

If other message blocks M^i remain, repeat the process (message schedule, big shuffle, creation of the new hash H^i)

If W^i was the last message schedule, then $H^i = H$ is message M's final hash or digest—its so very special in finger print.

This concludes the overview of SHA-256 as described in FIPS 180–4. A few closing thoughts:

SHA-256 projects into B^{256}, a space of ~1e77 possible values, which is lots of potential digests: a good thing that provides the intuition that collisions are unlikely that said, we do not prove here that collisions are unlikely, we even know they exist given the subjective nature of the hashing function. We know however that (i) given a limited amount of things to hash, we're unlikely to find collisions (ii) no collisions have been found to date for SHA-256.

B. Automatic ration syste using ADMEGA microcontroller:

It has 8-16 Kb (fig.5) of Flash program memory 1Kbyte Internal SRAM I/O Ports: 23 I/ line can be obtained from three ports; namely Port B, Port C and Port D. T External Interrupt source, located at port D.

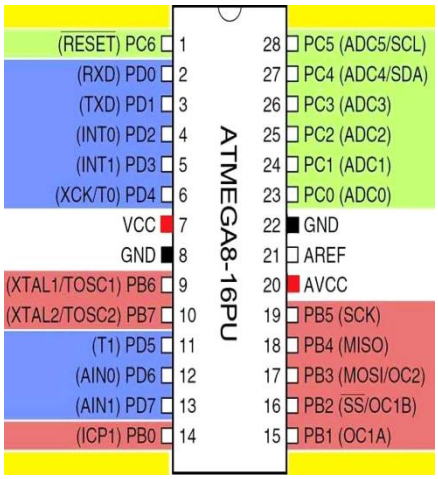

Fig. 4 AGMEGA pin configuration

C. Finger Print Verification System

This Algorithm is used for the verification purpose. It analyses (fig.5) the acquired finger printimagewith the stored finger print image which a user already stored in the database and checks whether the finger print image matches or not. If the template matches then the access is granted or else access will be denied, by using this finger print matching system we can provide the security from unauthorized persons accessing the customers information.

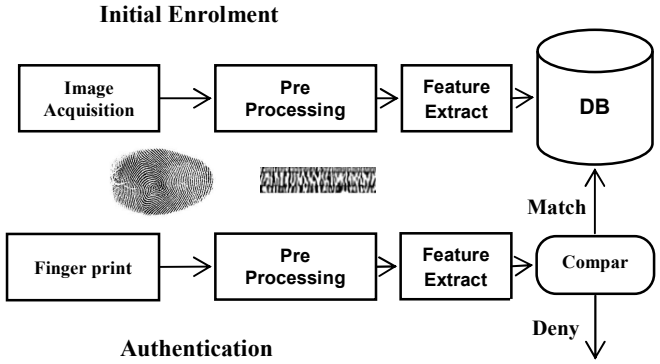

Fig.5Finger Print Matching System

This finger print algorithm runs in following steps, at the initial enrollment phase first the finger print image was acquired by using the device and the image was processed by segmentation, normalization, and binarization and thinning. Then the feature was extracted from the preprocessed information and stored in database. At the authentication phase fingerprint was processed and compare with data base that needs to match with previously stored finger print to get access.

V. MESSAGE GENERATION SYSTEM

In this module we generate SMS to family header phone, Fig.6 shows as when the grocery items is purchased from the ration shop the purchased information are stored in

database for future verification and also send as an SMS to all the members of the family. When ration staff update product Quantity in the website that information also send as an SMS to all the family in that region. Google Cloud Message[5] uses XMPP protocol for message generation purpose. Where the XMPP and HTTP are interconnected with the Google cloud messaging server with the help of these two protocol GCM server will send an SMS to the consumer's mobile.

Fig.6 Message Generation from PDS

VI. CONCLUSION

The proposed finger printauthentication is thestandard method and unique among all the other individual biometrics methods for identification/verification of an individual.By using the extraction algorithm and SHA verification algorithm captured finger printimage is scanned and verified then the image undergoes several process like segmentation, orientation, butrification and thinning hence by doing all these process the finger print character of one person cannot be hacked by others and this process is more secure than the previous works. Hence we implemented this technology in this system whichportrays the Automation of the Public Distribution System (PDS) and its recompense over the present fair price shops. The automatic PDS is easy to implement and requires much less hard work when compared to the other system using of this system we can avoid the malfunctions because there is no manual operations.Now in a new system all information is stored in database, so implementing this will be really helpful to the people below poverty line. In future this system can be implemented to the Indian rationing system to lead our country in an uncorrupted way. We can control the corruption taking place in the PDS as this system is fully based on finger print biometric authentication technology it is not as easier to view and hack the details of other users and it is highly secured.

REFERENCES

[1]. Parvathy A, VenkataRohit Raj, Venumadhav, Manikanta, "RFID Based Exam Hall Maintenance /System", IJCA Special Issue on "Artificial Intelligence Techniques - Novel Approaches & Practical Applications" AIT, 2011

[2]. Security Authentication Scheme Based on Certificateless Signature and Fingerprint RecognitionZhu Yanqiong ; XuHui ; Gao Zhan2011 Seventh International Conference on Computational Intelligence and Security, 2011

[3]. Design and implementation control of interfering mobile device with stepper motor and microcontroller ATmega 16Dong QuangHuy ; Jan Leuchter ; Jiri Buzek ; VitezslavStekly ; Le Thanh Bang 2017 International Conference on Military Technologies (ICMT)Year: 2017.

[4]. R.Ramani ,S. Selvaraju, S.Valarmathy, P.Niranjan, "Bank Locker security System Based on RFID and GSM Technology", International Journal of Computer Applications (IJCA) (0975 – 8887) Volume 57– No.18, November 2012

[5]. E-Health Services for Elderly Care Based on Google Cloud Messaging Ching-Nung Yang ; Fu-Heng Wu ; Sin-Yen Tsai ; Wen-Chun Kuo 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)Year: 2015Volume 1, Issue 3, June 2012 www.ijcsn.org ISSN 2277-5420

[6]. Cloud computing platform for applications in social-commercial area George Suciu ; Cristina Butca ; NarcisaMocanu ; Stefan CiprianArseni 2015 Conference Grid, Cloud & High Performance Computing in Science (ROLCG) Year: 2015

[7]. Fingerprint Matching on Smart Card: A ReviewKedimotseBaruni ; Albert Helberg ; Kishor Nair2016 International Conference on Computational Science and Computational Intelligence (CSCI)

[8]. Fast camera fingerprint matching in very large databasesSametTaspinar ;Husrev T. Sencar ; SevincBayram ; NasirMemon2017 IEEE International Conference on Image Processing (ICIP)Year: 2017

[9]. ingerprint Identification System Based On Neural Network Mr. Lokhande S.K., Prof. Mrs. Dhongde V.S. ME (VLSI & Embedded Systems), Vishwabharati Academy's College of Engineering, Ahmednagar (MS), India.

[10]. A Security-Enhanced Alignment-Free Fuzzy Vault-Based Fingerprint Cryptosystem Using Pair-Polar Minutiae StructuresCaiLi ;Jiankun HuIEEE Transactions on Information Forensics and SecurityYear: 2016