Table of Contents

Abstract

RFID works on the principle of Radio Frequency but when it comes to location tracking there are huge chances of disbanding the system or the reader via harming activities like kill tag, operating high frequency kit that may disrupt the operation of RFID. There are many algorithms in the market that handle the threat but still there are some loopholes that have led to them being debunked. We use SHA-3 to handle security issues of RFID as we are deploying it in a centralized system with a network of multiple other distributed RFID readers. The basic working of RFID readers will be discussed for tracking the students inside the school. The working SHA-3 algorithm and its advantages over the other algorithms from its league will be explored.

KEYWORDS: RFID Tracking, security algorithms, SHA-3 algorithm.

1. Introduction

Nowadays, parents are worried about their children because of the high rate of kidnapping. Moreover, parents are having long working hours, so they simply do not have as much time to spend for their children Moreover, they will be persuaded by kidnapper before they enter the school. So, it is the responsibility for the school to take care of their students and they also know in-time and able to send an alert message to their parents if the students are not at the school at school start time. This System ensures safety of the students by making their parents aware about the various important status about their students like in-time, out-time, everything about their arrival. By using RFID technology, it is easy track the student thus enhances the security and safety in selected zone. The information about student such as in time and out time from school will be recorded to web based system and SMS will be automatically sent to their parents that the student arrived to school safely. SMS will be sent to parents whose children are absent without taking leave. The parents can log into system website and monitor the details of their children. The implementation of School Security System(SSS) via RFID to avoid crime, illegal activates by students and reduce worries among parents.

The whole communication under the server which will be handled the administrator of the school/college. The system is implemented comprising of network which raises the chances of breach of confidentiality for which latest security algorithm called SHA-3 is implemented. It belongs to Keccak Sponge family and differs from its predecessors in terms of construction but is high in processing speed and security. RFID is a fast growing technology that has been introduced by Mario Cardullo, it is the first true ancestor of modern RFID patented on January 23, 1973 as it was a passive radio transponder with memory. The RFID data that is used to index the student record in database is made secure by turning RFID data into hash value using SHA-3 algorithm that ensures data integrity as the RFID data stored in database becomes impossible to decipher thus the record of student cannot be accessed.

2. Project Objectives

School Security System (SSS) using Radio Frequency Identification (RFID) project consists of the following major objectives:

- Information flow between parents and school which helps to track their respective wards
- Enhances security to the school children
- It informs in-time, out-time of students to its respective parents

3. Research Background

3.1 Problem statement

Maintaining Security is the most common burning issues nowadays. Every parents wants their children to be safe in any place they go. There is high rate of kidnapping of school children, so the parents are worried. Moreover, parents stays busy all the time at their daily schedules. They don't have much time to talk and spend some more time with their children's, which are creating generation gap between the children and parents. Children's are not getting proper attention and care. However, many children are in contact with the strangers. School is the another home of children. There is no any system that notify the students' parents, whether their children reached into the school safely or not.

3.2 Scope

The worse nightmare a parent can have is losing their child. However, a little care can make a lot of difference. RFID tags are already attached to a lot of products we buy. Using it with the id card of your child can fetch a lot of benefits. RFID can be equipped for the simple reason that it lets the parents have peace of mind. The proposed system will be very useful to maintain children's security. With the successful installation and use of this system in school, parents and school staffs can get proper timing and location of children/students.

- Can be widely used in school, colleges and offices
- In product supply chain
- In tracking visitors
- In employee tracking
- In prisons
- Can be used in library and canteen

3.3 Project Goals

The main goal of this project is to provide security to the school students and let their parents know about the in and out time of their children in school. It removes the gap between parents and children. This system ensures security of the school students. It reduces crime and illegal activities inside school boundary. Reduce worries among parents towards their children. The system ensures that students from the time they enter the school gates, until the time they have safely left the premises with their guardians.

3.4 Deliverables

- Project plan
- RFID devices
- Requirement Definition
- System Design
- Software Development
- Release
- Final Report

3.5 Constraints

Constraints of this project are as follows: -

- To develop an web based system
- The language is displayed in English
- I3 processor based computer
- Minimum RAM of 1GB

3.6 Assumptions

Assumptions of this project are as follows: -

- It is assumed that the project will be finished on given time.
- It is assumed that users will have mobile phones.
- It is assumed that the users will be familiar with the Internet.
- It is assumed that the users will be familiar with the SMS service

4. Literature Review

An immense amount work has been done in fields like patient monitoring system, student attendance tracking system and monitoring of supply chain management system using RFID.

4.1 RFID based Cloud Supply Chain Management

This paper describes briefly the underlying principle of RFID, introduction about supply chain management process and the proposed solution RFID based cloud based SCM services like storing the product data, tracking the product across the supply chain, inventory control, warehouse managements, retail store management, delivery and billing in Point of sale terminal using EPC (Electronic Product Code).

It is a cloud based system so the users are in the threat of the loss of the data if there is not a strong database. The tracking system is also online so that there can be a chance of robbery and the stole of goods.

4.2 RFID in cloud environment for Attendance monitoring system

This paper presents the overview of interfacing RFID with cloud computing for updating students' attendance and updating it into the parents' corner and faculty mails. This is likely to realize in exam halls or classrooms where the RFID card readers are stationed at the entrance to mark the student's entry and buzzer is also provided to alarm on the entry of an unintended person.

There is a great chance of the failure while using online system because there is always a chance that the servers being down and if the servers are down there will be no chance of no attendance in the particular days if the servers are down. This poses as a challenge while using this system.

4.3 RFID Technology for IoT-Based Personal Healthcare in Smart Spaces

It presents a survey on the state-of-the-art of RFID for application to body centric systems and for gathering information (temperature, humidity, and other gases) about the user's living environment. The various types of RFID tags like the wearable and implanted ones to track human motions, gestures and overnight living environment are discussed.

But when there is a vast network comprising of communicating nodes then there are chances of breach of data and compromise in its integrity. The most concerned issues are the tracking and the location privacy.

So secure algorithm needs to be adapted like MD5, SHA-1, SHA-2, and SHA-3. The efficiency of these algorithms is discussed below to choose the best amongst them.

Name of the Algorithm	Size of output	Rounds	Collision status
MD5	128	60	YES
SHA	160	80	YES
SHA-1	160	80	YES
SHA-2	256/512	60/80	THEORITICAL
SHA-192	192	80	NO
SHA-192	192	64	NO
SHA-3	256/512	24	NO

Fig: Comparison between MD5 and SHA hash algorithms on general properties basis

In October 2012, the National Institute of Standards and Technology (NIST) chose the Keccak algorithm as the new SHA-3 standard. The problem with SHA-1 and SHA-2 is that they both use the same engine, called Merkle-Damgard, to process message text which means that a successful attack on SHA-1 becomes a potential threat on SHA-2.

The Init() function prepares the internal state (S) for the given hash size. The Update() function starts the compression or absorb phase. This is where the message text is combined with the internal state, then permutated. The Final() function starts the extraction or squeeze phase. This is where bits from the internal state are extracted and assembled to form the hash value.
The key properties of a secure cryptographic hash function are:

- Output length is smaller compared to input and input cannot be determined from output
- Computation is fast and efficient for any sized input
- Any change to input affects the output bits
- Strong collision resistance.

While using my system there is a zero chance of failing because we use the best system and always have a backup system running and there is a huge amount of chance that our system can function up to 90 percent. There is a chance that we use SCM services like storing the product data, tracking the product across the supply chain, inventory control, warehouse managements, retail store management, delivery and billing in Point of sale terminal using EPC (Electronic Product Code). This system can be the same for some part and we must update on some of the parts so the system can be fully prepared.

4.4 Advantages of using SHA-3 algorithm over other previous algorithms

Keccak has been officially chosen to be the SHA-3 algorithm. Because it is based on a sponge function instead of Merkle–Damgård, it should not be vulnerable to the same kinds of attacks that earlier SHA algorithms might be. Specifically, it is not vulnerable to length extension attacks, which affect all M-D hashes like MD5, SHA-1, SHA-2.

SHA-3 has not been finalized; candidate algorithms are still being reviewed by NIST, and the finalist is expected to be announced in 2012. That said, there are a few reasons one would choose to support SHA-3 or even SHA-2 over SHA-1.

First, there are theoretical attacks against SHA-1 that reduce the difficulty of finding collisions. These attacks are still impractical, and SHA-1 can be relied on for strong security for hashes and signatures that expire in a few years' time. SHA-2 is similar to SHA-1, but has not been shown to be susceptible to the same attacks.

Second, NIST has recommended that the United States Federal Government stop using SHA-1. Practically, this means that if you ever want your code or project to be used by the Federal Government, you should not use SHA-1

The previous algorithms did not provide the appropriate security to the system that are stored on the centralized system. The centralized system is installed on computer where admin can add and remove the details of the students and updates into the local database. The main purpose of designing the new school security system with SHA-3 algorithm is to provide maximum security of the school students which will be better in any previous algorithms (SHA-1 and SHA-2).

5. Research Methodology

5.1 Algorithm (flowchart)

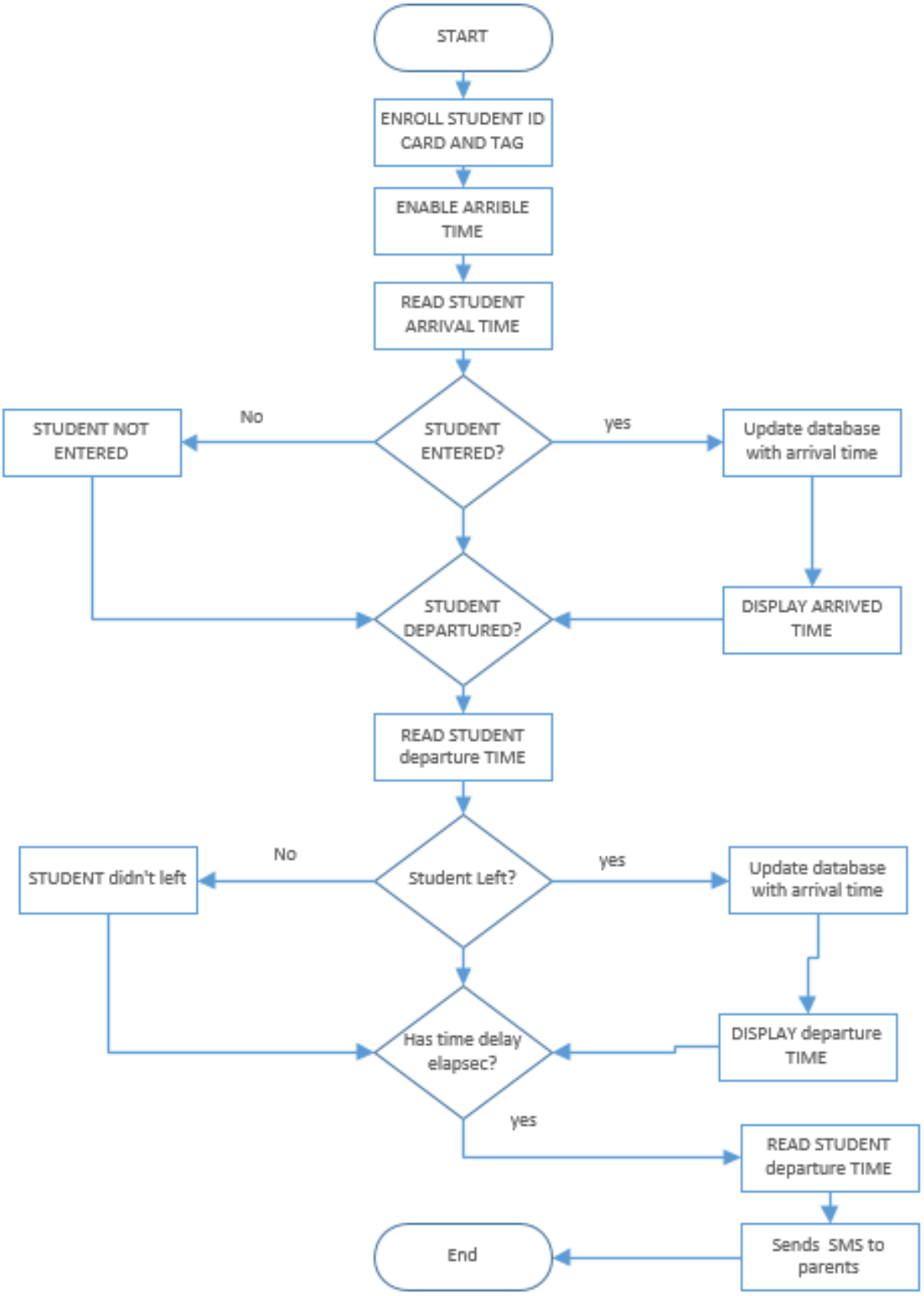


Figure 1:Flowchart

5.2 Block Diagram

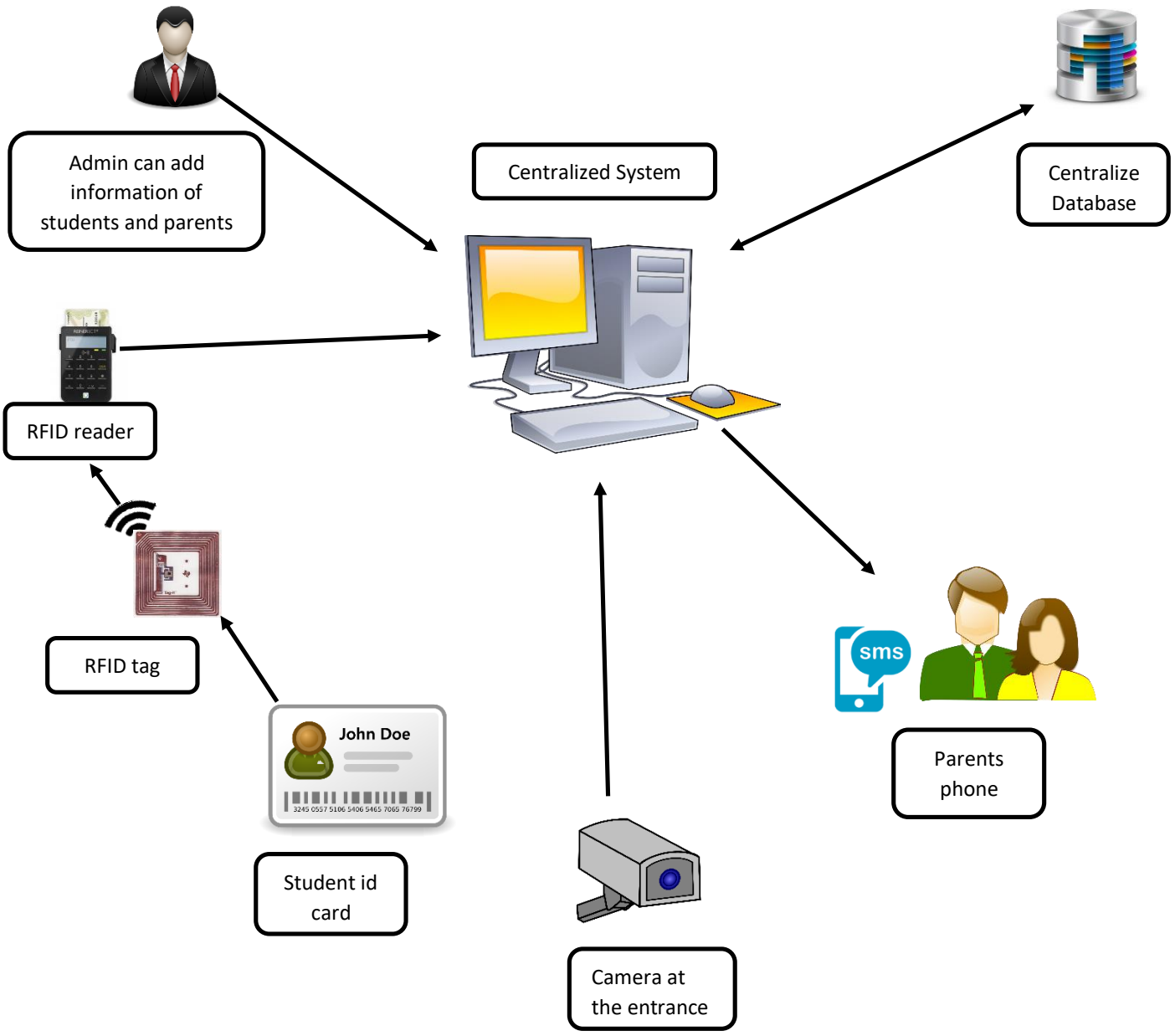


Fig2. Block diagram of Student Tracking System

5.3 Working process of Student Tracking System

- The student swipes his RFID card at the entrance where the RFID reader is installed and it sends a notification/SMS to his parent that he/she has reached the school.
- The server is the centralized medium that makes it possible and it is handled by the admin.
- The admin gets a desktop interface wherein he can add, update or delete records of students and parents.
- The server uses web services like SOAP so that it can easily be deployed on cloud and uses RxTx library in order to support serial communication with RFID reader and RS232 and also uses JMYRON library to support camera.
- The server sends the SMS template to the respective parent given that the RFID number on student's ID matches with the number present in the database, RFID number acts as the primary key. But since there are chances of loss of integrity of data, the transmission is made secure by converting 12 digits of RFID to hash value that cannot be deciphered and then stored in the database. So while matching, the hash values are compared. So the server uses SHA-3 algorithm to secure the data.

5.4 Gantt chart

ID	Task Name	Start	Finish	Duration
1	Research	1/1/2019	1/23/2019	20d
2	Requirement gathering	1/24/2019	1/29/2019	5d
3	System analysis	1/29/2019	2/8/2019	10d
4	System design	2/10/2019	2/22/2019	12d
5	Development and coding	2/25/2019	3/31/2019	30d
6	Testing	4/1/2019	4/7/2019	6d
7	Implementation	4/8/2019	4/15/2019	7d
8	Documentation	1/1/2019	4/15/2019	90d

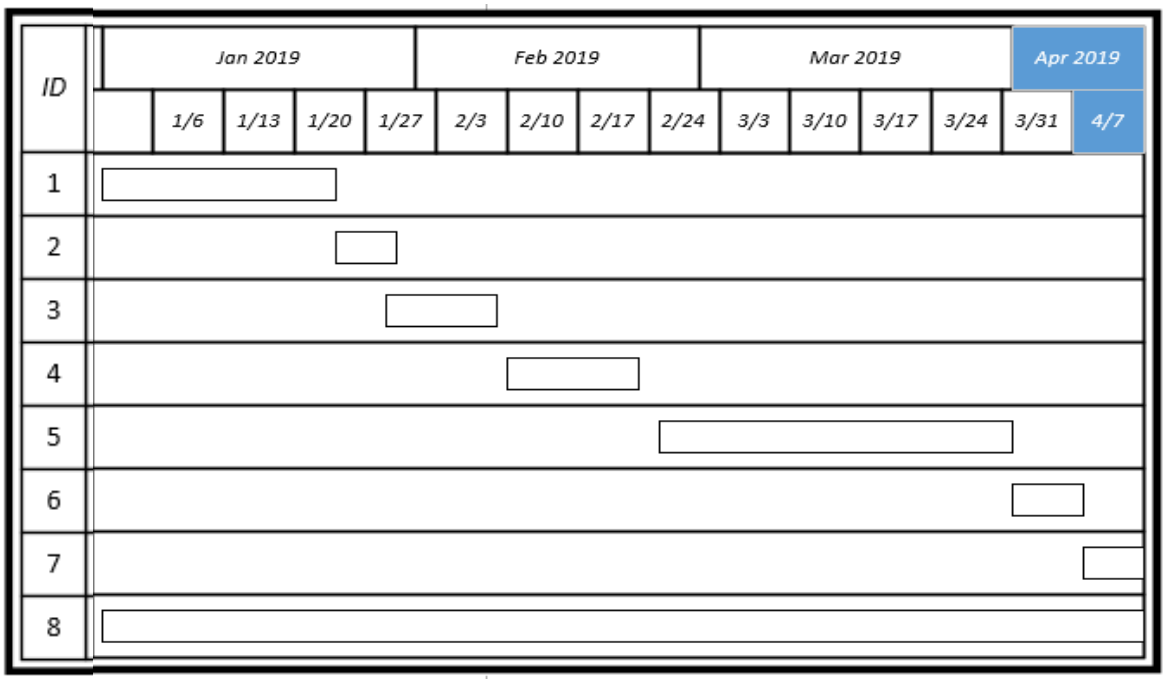


Figure1: Gantt chart table

5.5 Milestones

Milestone	Estimated completion (days) From 09/03/2018 to 12/10/2018
Research	20
Requirement Gathering	5
System analysis	10
System design	12
Development and coding	30
Testing	6
Implementation	7
Final documentation	90

Conclusion

In this way, we have discussed the idea about the student tracker system inside school premises using RFID and SHA-3 algorithm used to has the data sent over the network. The SHA-3 algorithm proves to be the right choice for data security and there is proper transmission of data. The parents thus, are able to keep a track of children via SMS and RFID tracker. Thus automation of this tracking service is a boon to both the parents and teachers as it brings transparency in their communication.

Appendix A:

Padmashree International College

School Security System using RFID technology under SHA-3 Algorithm
Suman Dangol
Id: 00015898

Nilai University

Abstract

RFID works on the principle of Radio Frequency but when it comes to location tracking there are huge chances of disbanding the system. We use SHA-3 to handle security issues of RFID as we are deploying it in a centralized system with a network of multiple other distributed RFID readers. The basic working of RFID readers will be discussed for tracking the students inside the school.

Problem statement

Maintaining Security is the most common burning issues nowadays. There is high rate of kidnapping of school children, so the parents are worried. There is no any system that notify the students' parents, whether their children reached into the school safely or not.

Objectives

- Information flow between parents and school which helps to track their respective wards
- Enhances security to the school children
- It informs in-time, out-time of students to its respective parents

Scope

- Can be widely used in school, colleges and offices
- In tracking visitors, employee
- In employee tracking

Literature Review

RFID based Cloud Supply Chain Management

This paper describes briefly the underlying principle of RFID, introduction about supply chain management process and the proposed solution RFID based cloud based SCM services.

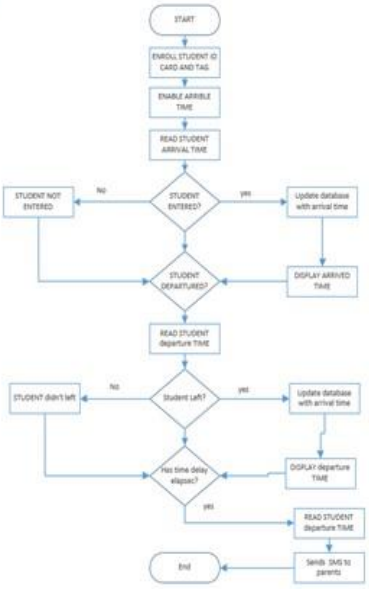
RFID in cloud environment for Attendance monitoring system

This paper presents the overview of interfacing RFID with cloud computing for updating students' attendance and updating it into the parents' corner and faculty mails.

Major Drawbacks

- The problem with SHA-1 and SHA-2 is that they both use the same engine which lacks proper data security
- Output length is smaller compared to input and input cannot be determined from output
- Problem with the storage and database

Research Methodology



Conclusion

The SHA-3 algorithm proves to be the right choice for data security and there is proper transmission of data. The parents thus, are able to keep a track of children via SMS and RFID tracker.

Supervisor: Mr Prawesh Dhungana

Figure3: Poster

References

- (PDF) Students attendance management system using RFID and GSM module. Available from: https://www.researchgate.net/publication/318940720_Students_attendance_management_system_using_RFID_and_GSM_module [accessed Sep 08 2018].

- Impinj.com. (2018). Different Types of RFID Systems | Impinj. [online] Available at: http://www.impinj.com/resources/about-rfid/the-different-types-of-rfid-systems/ [Accessed 9 Sep. 2018].

- Arxiv.org. (2018). [online] Available at: https://arxiv.org/ftp/arxiv/papers/1105/1105.3790.pdf [Accessed 9 Sep. 2018].

- Dr. Dobb's. (2018). Keccak: The New SHA-3 Encryption Standard. [online] Available at: http://www.drdobbs.com/security/keccak-the-new-sha-3-encryption-standard/240154037 [Accessed 9 nov. 2018].

- Search Security. (2018). Secure Hash Algorithm-3: How SHA-3 is a next-gen security tool. [online] Available at: http://searchsecurity.techtarget.com/tip/Secure-Hash-Algorithm-3-How-SHA-3-is-a-next-gen-security-tool [Accessed 9 Dec. 2018].

- Asecuritysite.com. (2018). SHA-3/Keccak. [online] Available at: https://asecuritysite.com/encryption/sha3 [Accessed 9 Sep. 2018].

- Infosec.gov.hk. (2018). [online] Available at: http://www.infosec.gov.hk/english/technical/files/rfid.pdf [Accessed 10 Dec. 2018].