ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Student Tracker Using RFID and Live Feeds

Akarsha Sudheer [1], Amar Bade [2], Vishal Dhar [3], Nilesh Raghuwanshi [4], A.Y.Syed [5]

U.G. Student, Department of Computer Engineering, JSPMs JSCOE, Pune, Maharashtra, India[1,2,3,4]

Assistant Professor, Department of Computer Engineering, JSPMs JSCOE, Pune, Maharashtra, India[5]

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 centralised system with a network of multiple other distributed RFID readers. The basic working of RFID readers and live cameras will be discussed for tracking the students. The working SHA-3 algorithm and its adavntages over the other algorithms from its league will be explored.

KEYWORDS: RFID Tracking, security algorithms, SHA-3, live cameras.

I. INTRODUCTION

Technology is influencing almost every aspect of this world. All the primitive methods are being superseded by the automated systems. The educational system around the globe is also under the influence of the automation and technology. Although there are less percentile of the schools and colleges which are using the automated methods for teaching and communication with the students and their parents, the numbers is increasing every year showing the positive approach of the people towards the change.The main objective is that the parent should be able to monitor the attendance and assignments of their ward on daily basis without actually visiting the school/college. Besides this, direct live feed from the school can also be provided by which parent can ensure and track the location of their ward within the school without using any of the GPS services. The system is designed using Android and Java along with the SOAP web service technology. The parents will be able to login to the application using the user id and password provided at the time of admission. After login the services provided can be used by them. The staff can also send assignments over this system which will reduce their efforts and time. 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 [1]. There are basically three types of RFID viz. 1) Passive: They send a radio signal to the tag that then uses the transmitted signal to power on, and reflect energy back to the reader. They do not require a power source or transmitter, they are cheaper, smaller, and their ranges are limited to less than 10m. 2) Active: In active, tags have their own transmitter and power source that broadcast their own signal to transmit the information stored on their microchips and their range is upto 100m. There are two main types of active tags: transponders (do not actively radiate radio waves until they receive a reader signal, they conserve battery life) and beacons (used in most real-time locating systems (RTLS), in order to track the precise location of an asset continuously, they emit signals at pre-set intervals) and 3) Battery-Assisted Passive(BAP) [2].

The work in this paper is divided in two stages 1) Student tracking 2) RFID data hashing. The student activity is tracked and monitored via the RFID readers that sense the RFID tag containing the number unique to each student. Thereafter,the distance travelled is mapped onto the admin's system and he is able to view the places traversed by the students during school hours in the campus premises. Alongwith that the image of the student is captured as he/she passes the place where the reader is fixed thus the it can be verified whether the card holder is the original owner or not.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

During student activity tracking, 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.
Paper is organized as follows. Section II describes papers and resources related to the domain, and explores the extensive study done to implement the system. The flow diagram represents the step of the algorithm. Section III covers the working of the Student tracker system and the SHA-3 algorithm that is used. Section IV presents experimental results showing results of RFID tracked data. Section V covers the merits and demerits on using RFID and SHA-3. Section VI explains the different fields where such system can be deployed. Finally, Section VII presents conclusion.

II. RELATED WORK

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.

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(Electromic Product Code) [3].

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 [4].

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 bodycentric 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 [5].

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 [6].
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 [7].

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

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. In Keccak, the Hash() serves as the entry function that takes four arguments: the hash size (n) in bits, the message text (M) and its size (N) in bits, and a hash variable (H).
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 [8].

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 [9].

SHA-3 is a family of sponge functions consisting of two parameters, the bitrate r and capacity c. The sum, r + c determine the width of the SHA-3 function permutation used in the sponge construction and is restricted to a maximum value of 1600. Selection of r and c depends on the desired hash output value. For a 256-bit hash output r = 1088 and c = 512 and for 512-bit hash output r = 576 and c = 1024 is selected. There are 24 rounds in the compression function (Core) of SHA-3 and each round consists of 5 steps, *Theta* (θ), *Rho*(ρ), *Pi*(π), *Chi* (χ) and *Iota* (i).

The SHA-3 hash function operation consists of three phases: 1.Initialization is simply the initialization of state matrix (A) with all zeros. 2.In the absorbing phase each r-bit wide block of the message is XORed with the current matrix state and 24 rounds of the compression functions are performed. 3.In the squeezing phase the state matrix is simply truncated to the desired length of hash output [10]. The following piece of code shows implementation for 256 bits hash [11]:
public void checkSHA3(string message)

```
{
        if(message == null)
                return;

        byte[] bytes = null;
        byte[] r = null;
        SHA3.SHA3Unmanaged hash = null;
        System.Text.ASCIIEncoding encoding = new System.Text.ASCIIEncoding();

        hash =new SHA3Unmanaged(256);
        bytes = encoding.GetBytes(message);
        r = hash.ComputeHash(bytes);
        hash1 = Global.ByteToString(r);
}
```

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

III. WORKING OF THE TRACKER

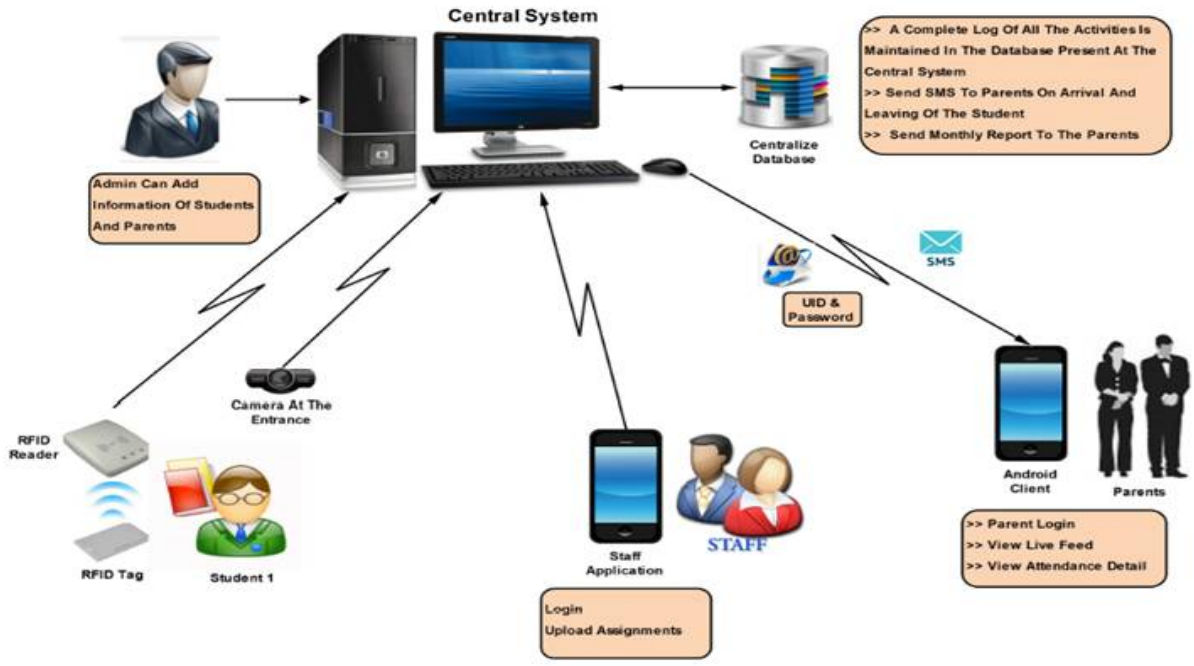

Fig. Block diagram of Student tracking System

Explanation:

- 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 has reached the campus. The server is the centralised 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 ae 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.
- The overall movement of student is tracked. Every corner of the campus is fixed with RFID reader and the cameras. The RFID readers are connected with cameras so that live image of student can be captured the moment he passes the room and the the complete movement can be viewed on a map by the admin.
- The parents on the other hand get the attendance and live feed of the selective rooms on their android app, thus this helps them to track their ward. They also get to view the assignments uploaded by the teachers.
- The teachers also have access to this app but with their own set of credentials that they can use to log in and upload assignments and view defaulter's list.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

IV. EXPERIMENTAL RESULTS

Figures show the results of using RFID to track the movement of students in the campus premises that can be tracked by the admin and the parents along with their attendance. Figs. 1 (a), 1(b), 1(c),1(d) represent the functions at the admin side. The admin logs in first using his credentials and then gets a homepage on his desktop.

1. Fig 1(a) is login page on admin side where the COM port (RFID reader connection) and password are entered.

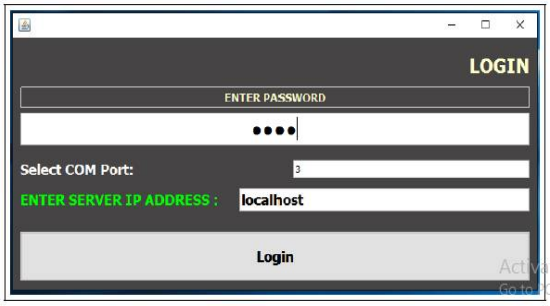

Fig.1(a) Admin login page

2. Fig 1(b) is the admin homepage showing options to add and track students.

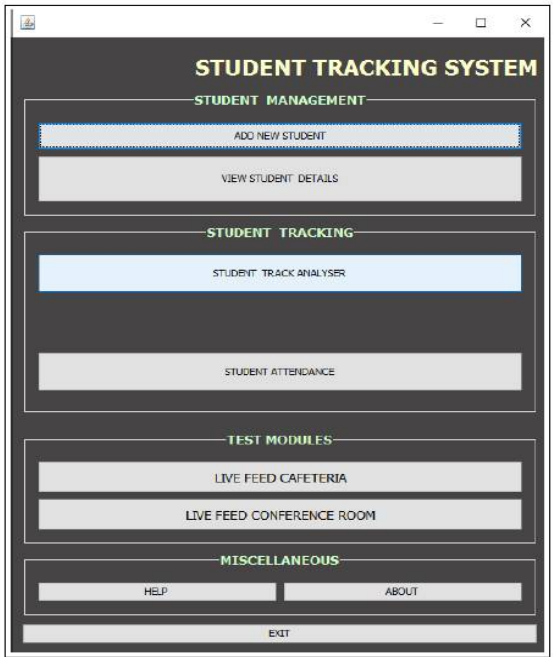

Fig.1(b) Admin home page

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

3. Fig 1(c) shows the student RFID card being read by the passive reader.

Fig.1(c) Student swipes his card for registration

4. The student is tracked and his movements are shown on map alongwith the images on admin side.

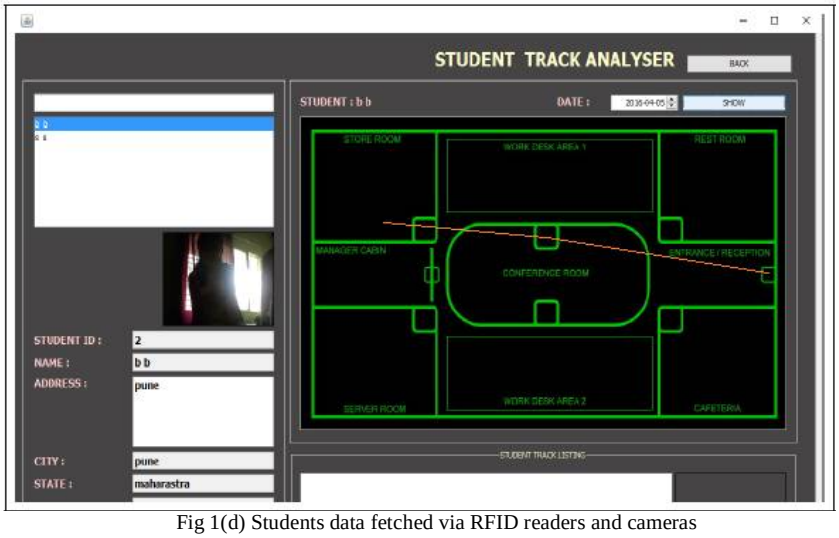

Fig 1(d) Students data fetched via RFID readers and cameras

The figs. 2(a), 2(b), 2(c), 2(d), 2(e) represent parent side functionality to view student's progress and track his/her activities. The parent logs in using the credential allotted during admission and gets a homepage.

1. The app asks the user to enter the IP of the LAN etwork they want to connect to where the server is present.

Fig 2(a) Parent app connecting to LAN network

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

2. The parent is supposed to enter the unique credentials allotted during admission.

Fig. 2(b) Parent login page

3. After entering credentials, user is directed to homepage where he gets the option to view attendance or live feed.

Fig.2(c) Parent home page

4. The live feed option shows the realtime video of the selected room to the parents.

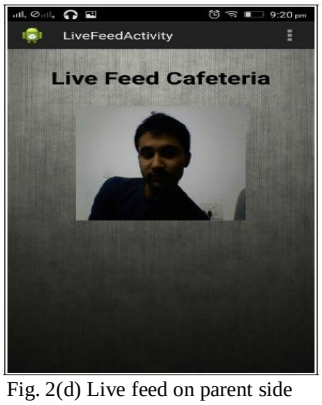

Fig. 2(d) Live feed on parent side

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

5. The attendance on a monthly basis can be viewed.

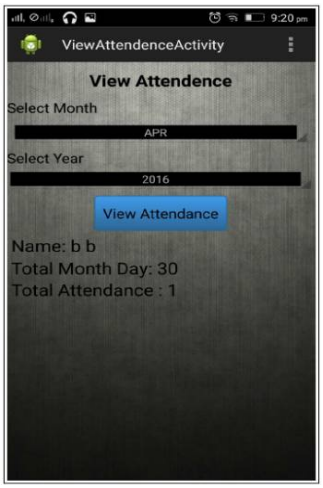

Fig. 2(e) Monthly attendance

V. ADVANTAGES AND DISADVANTAGES

Advantages:

- RFID identifies and accounts for items quickly, easily, accurately and cost-effectively.
- SHA-3 has many benefits such as performance and good resistance traits.
- The tag can stand a harsh environment and multiple tags can be read/written at the same time.
- No line of sight requirement and long read range in case of active RFID tags.

Disadvantages:

- Cost increases as the number of readers increases therefore is not preferable for large geogrphical area.
- Use an illegal high power radio frequency (RF) transmitter in an attempt to jam frequencies [12].

VI. APPLICATIONS

- **In product supply chain**
  The complete process can be tracked right from manufacturing to the deployment at client side so that no error gets introduced.

- **In tracking visitors**
  At some exquisite exhibit wherein high profile visitors frequent, their movements can be tracked in order to secure the premise given that they should possess a RFID card.

- **In employee tracking**
  It can be deployed in companies to keep a tab on the employees and see whether they sincerely do their job during working hours and accordingly pay them.

- **In prison**
  The prisoners with implanted RFID chip can be tracked within the premise so that there are less chances of jailbreak.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

- **In mental asylums**
  In hospitals where the mentally ill people are treated always face a problem when some of their patients who may even be violent go missing so it can be reduced once the patients are implanted with RFID tracking chips.

VII. CONCLUSION

In this way, we have discussed the idea about the student tracker system 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 their ward via SMS, live feed and RFID tracker and similarly teachers too get a prompt defaulter's list without having to manually compute. Thus automation of this tracking service is a boon to both the parents and teachers as it brings transparency in their communication.

REFERENCES

[1] https://en.wikipedia.org/wiki/Radio-frequency_identification
[2] http://www.impinj.com/resources/about-rfid/the-different-types-of-rfid-systems/
[3] B.Andal Supriya, Ilango Djearamane,"RFID based Cloud Supply Chain Management", International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013.
[4] A.Parvathy, B. Rajasekhar, C.Nithya, K.Thenmozhi, J.B.B. Rayappan, Pethuru Raj, and Rengarajan Amirtharajan,"RFID in cloud environment for Attendance monitoring system", International Journal of Engineering and Technology (IJET), Vol. 5, No. 3, Jun-Jul 2013.
[5] Sara Amendola, Rossella Lodato, Sabina Manzari, Cecilia Occhiuzzi, and Gaetano Marrocco, "RFID Technology for IoT-Based Personal Healthcare in Smart Spaces", IEEE Internet of Things Journal, Vol. 1, No. 2, April 2014.
[6] https://arxiv.org/ftp/arxiv/papers/1105/1105.3790.pdf
[7] C.G Thomas, Robin Thomas Jose,"A Comparative Study on Different Hashing Algorithms",International Journal of Innovative Research in Computer and Communication Engineering ,Vol. 3, Special Issue 7, October 2015.
[8] http://www.drdobbs.com/security/keccak-the-new-sha-3-encryption-standard/240154037
[9] http://searchsecurity.techtarget.com/tip/Secure-Hash-Algorithm-3-How-SHA-3-is-a-next-gen-security-tool
[10] Muzaffar Rao, Thomas Newe and Ian Grout, "Secure Hash Algorithm-3(SHA-3) implementation on Xilinx FPGAs, Suitable for IoT Applications",Proceedings of the 8th International Conference on Sensing Technology, Sept 2-4,2014.
[11] https://asecuritysite.com/encryption/sha3
[12] www.infosec.gov.hk/english/technical/files/rfid.pdf