ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

Instrumental Framework for Bank Locker Security Enhancement Using Electric Field Proximity Sensor – An Innovative Approach

Y.V.S. Bharadwaj[1], Venkata Sai Bhageerath Y[2], Prof Prasada Rao YVSSSV[3]

Mobile Banking Security Lab, Institue for Development and Research in Banking Technology, Castle Hills, Road No. Masab Tank, Hyderabad, Telangana, India[1]

National Institute of Technology (NIT), Warangal, Telangana, India[2]

Principal, NRI Institute of Technology, Guntur, Andhra Pradesh, India[3]

ABSTRACT: In this paper a sensor based instrumental framework is presented which helps in enhancing the security aspects of a locker system. In the proposed model an electric field proximity sensor is used. Design of the sensor based instrument embedded in the key slot of the key locker system and number slot of the number locker system along with their working principles is presented. Deployment of the proposed architecture in the lockers enhances the security of the lockers used in financial institutions and eliminates the common internal frauds happening in the existing locker systems.

KEYWORDS: Key based locker, Number based locker, Electric field proximity sensor, lodger, GSM modem, Touch grid cells, and Skinny wires.

I. INTRODUCTION

Security of valuable financial assets is of at most importance to most of the people. Fraudsters find it quite easy to deceive a person, which is hindering the safety of their property. So, they safeguard their assets (which include liquid cash and collaterals) in banks. The cash instruments are secured in banks by maintaining accounts and the collateral assets are safeguarded in locker systems. Lockers are considered as treasure warehouses. Security is the basic essence of locker systems. This is one of the edging factors for customers to tariff cabinets in bank to safeguard their collateral assets. Cosmopolitan culture is a promoting factor for customers to go with lockers for escorting their ornamental assets in financial institutes instead of warding with them. Bank locker systems are broadly classified as:

1. Physical key based locker system
2. Biometric locker system
3. Number based locker system
4. RFID based locker system
5. Pattern based locker system

Characteristics, advantages and disadvantages of the above mentioned locker systems are presented in table-1.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

Table-1: Classification on types of locker systems with their characteristics, advantages and disadvantages

Sl. No	Types of Locker system	Characteristics/ features	Advantages		Disadvantages	
			Technical Factors	Non Technical Factors	Technical Factors	Non Technical Factors
1	Physical key based locker system	• There exist two key slots and a key pair. • One of the key pair is retained by the banker and the other is presented to the customer. • Accessing locker system is possible only when both keys are inserted at the same time.	As it involves physical access, no problem of single point failures	Limits access at customers discretion	Key cloning possible	Key loss
2	Biometric Locker System	• It works based on different sensing scenarios, which include finger print sensing, iris sensing etc. • Biometric scanner scans the biometric details and use them for granting access	• System reorganization efficiency of 96% [2]. • Security Enhancement. • Limits fraud accesses.	• Easy viability • Limited maintenance • More readily available and easy to use.	• Single point failure	Data can be stolen
3	Number based locker system	• Widely used in access control of strong rooms • Specific code or password is used to access the cabinet locker	Centralized data, so easy for maintenance	• Easy use • Eliminates need to carry physical keys • Provides access at customers discretion	• Single point failure	Data can be stolen
4	RFID Based locker system	• It is a wireless non-contact use of radio-frequency electromagnetic fields for transferring data. • It contains electronically stored information for remote access.	Use of micro controller enhances security levels [5]	• Cost efficient • Low power consumption • Compact size • Stand aloneness [3]	• Prone to tag cloning • Limits access, in case of compromised secured element	Limits access, in case of RFID tag damage
5	Pattern based locker system	• It is accessed using a specific number pattern	No problem related to system crashes, since they are to be physically accessed	• Eliminates use of physical key • Limits attempts for accessing locker in case of pattern mismatch	Level of frauds are high	Forgetful

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

In figure 1 a key based locker system (with a 3D illustration of the key slot and its corresponding key pair) and a pattern based locker system are presented.

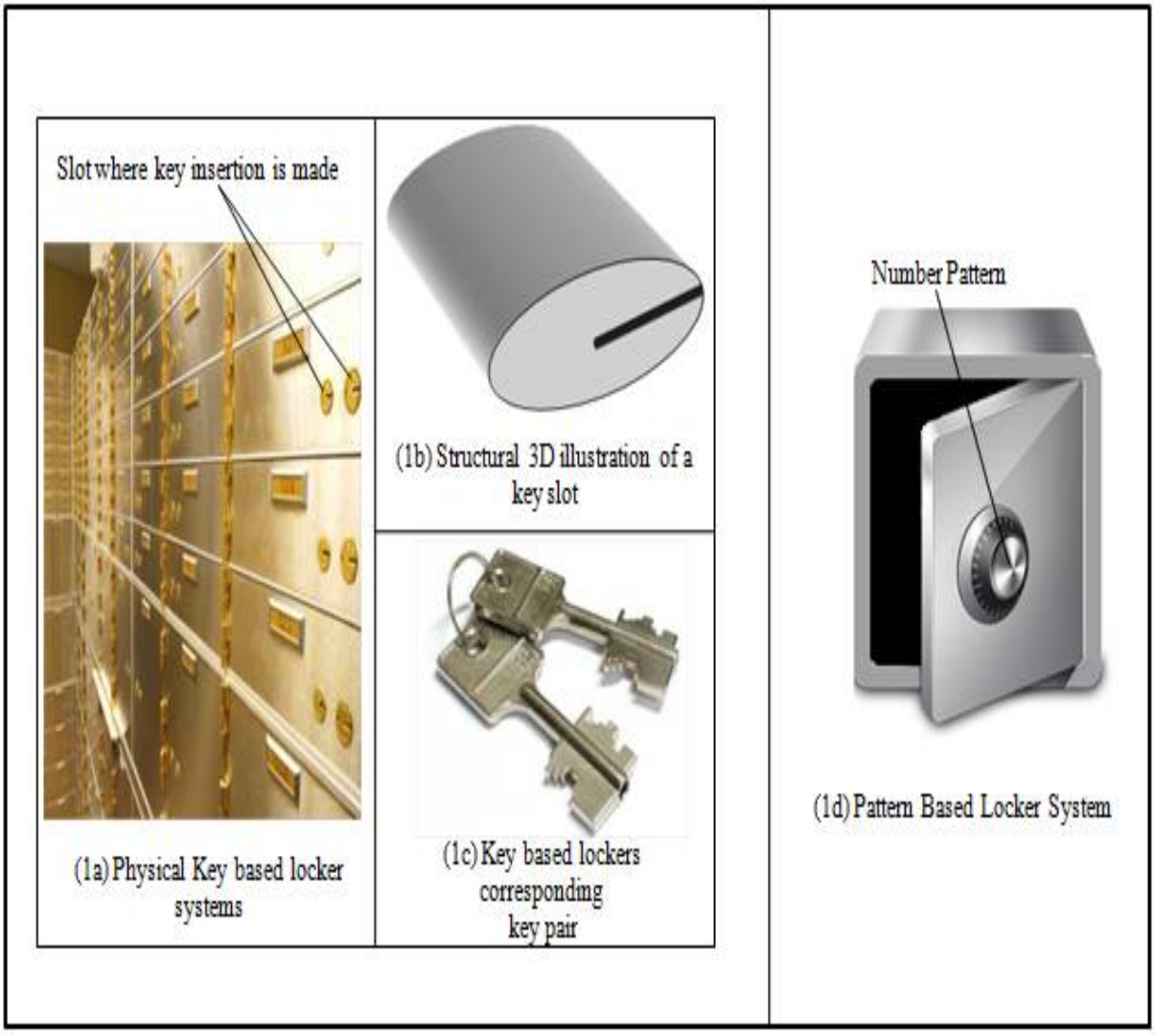


Fig 1: Components of key based locker system and pattern based locker safe

Based on the above mentioned technical and non technical factors which include their utilities, remarks/ observations are made as in table 2.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

Table 2: Remarks/ observations on different types of locker systems

Sl. No	Types of Locker System	Remarks/ Observations
1	Physical key based locker system	Physical key based locker systems are widely used in banks though issues related to key losses, key cloning are present. Reasons for this are the disadvantages associated with other types of locker systems.
2	Biometric locker system	Though the use of biometric locker system is effective in ways like enhancing security, easy viability, limited maintenance etc. As fingerprint reader used in a biometric system limits access to users; it is more reliable than physical key based locker systems. Problems like loss of biometric information stored on a computer discourage the banks in using the biometric locker systems.
3	Number Based Locker System	Issues related to security, power failure and forgetfulness bothers the banks in using number based locker systems, though they eliminate the need to carry physical keys.
4	RFID Based Locker System	Problem of tag cloning and tag damages hinder the use of RFID based locker systems in banks.
5	Pattern Based Locker System	Limited security issues and forgetfulness are the problems related to pattern based locker system. But by taking suitable measures for curbing security issues, it is possible to widen the use of these systems.

The aspects tabulated in table 2 encourage the banks to use the physical key based and pattern based locker systems though few problems related to security fraudulences are involved. These security issues can be overcome by applying sensor technologies.

Though the sensor technology is widely used in various industries, its potential use in financial industry is evolving. Sensor technology serves as a motivating factor for promoting security and surveillance in military, Habitat monitoring, Inventory tracking and in various other sectors for monitoring [1]. The use of sensors in the real world is growing because it is not only affordable, but also very efficient. Sensor technology intern helps in achieving affordable excellence. The major focus of this paper is on how security in physical key based locker system and pattern based locker system could be enhanced using sensor technology.

The safe deposit locker facility norms followed in banks as per their locker policy treat the banker as a custodian and the locker hirer as the lodger [7]. The deposit locker is rented to the lodger after properly been introduced to the financial institution through KYC (Know Your Customer) norms. When a customer lodges a locker, the bank seeks an undertaking from the customer which abstracts that the bank is not responsible for any loss in the collateral property of the customer [6].

II. CHALLENGES IN EXISTING PHYSICAL AND PATTERN BASED LOCKERS

In the current banking system which employs the use of physical or pattern based locker system, there are problems related to security issues. These issues are concerned with internal frauds in locker systems, where the banker himself is involved in such frauds. Many proposals have been made to detect and prevent external frauds that the banks are exposed to, but there are no mechanisms demonstrated to curb the internal fraud incidents. In case of theft, burglary or similar unforeseen events the bank is not held responsible [6]. Even, by chance if the banker is involved in the fraud and demonstrates it as a burglary action to the customer; the lodger cannot blame the banker and held him responsible for the fraud without proper evidence. There were many events where the bank officials were involved in fraudulences

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

[4]. There is a conceptual belief that these internal frauds cannot be curbed and hence the customer stays as a victim, losing his assets.
The proposed system deals with recommendations to control internal frauds in banks using sensors for physical key based or pattern based number lock systems.

III. PROPOSED MODEL TO OVERCOME CHALLENGES IN EXISTING LOCKER SYSTEMS

The internal frauds that occur in the bank locker system could be curbed up to some extent by providing intimation to the lodger i.e., the customer and the bank manager as and when an attempt is made to open the safe lock. This mechanism enables the bank in providing security to its customer assets lodged in lockers at various- branches. The challenging aspect is about security models which involve mechanisms to curb fraudulences that occur in both physical key based and pattern based locker systems. Though the mechanisms involved in both the physical key based and pattern based locker systems are different, the architectural work flow remains the same. The proposed architecture is given in fig 2.

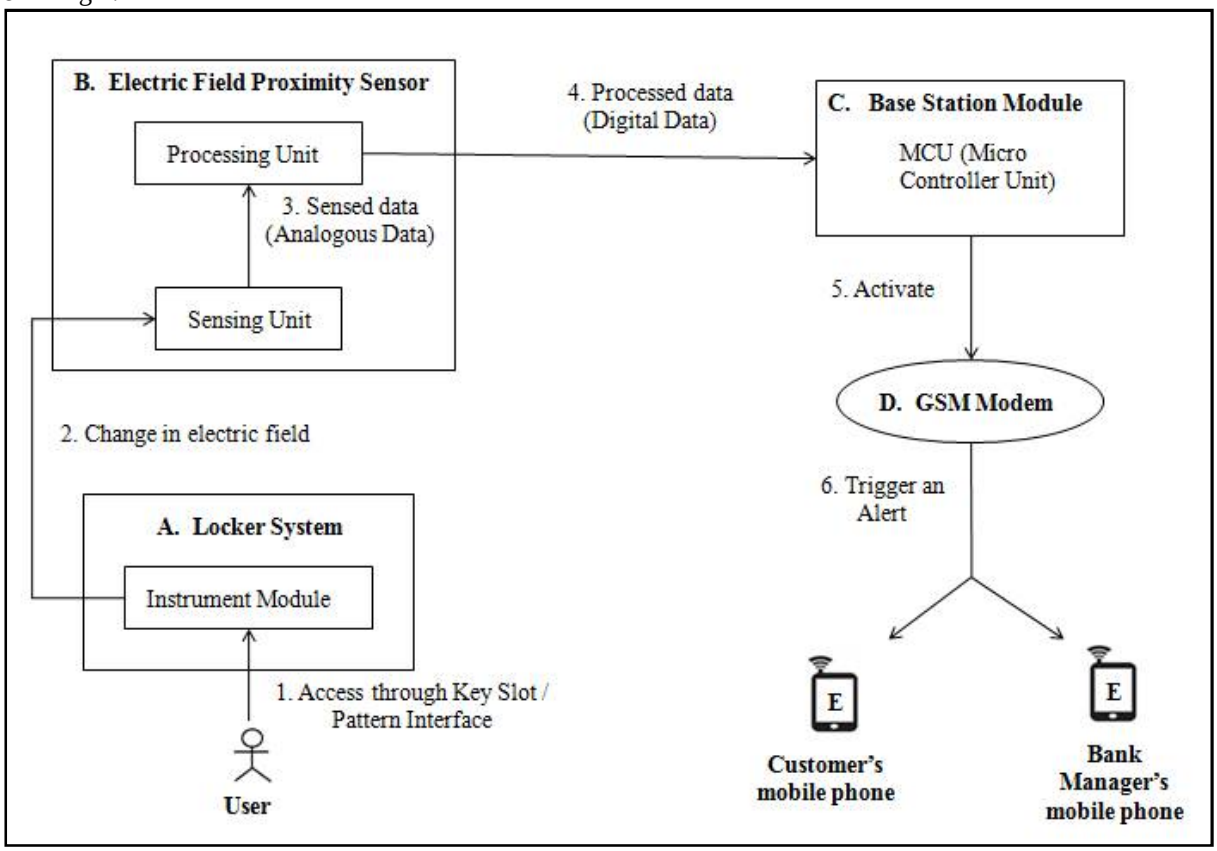


Fig 2: Process flow diagram of the proposed model

The process model involved in all the sections of the architecture model is detailed first and then the work flow process is comprehended. The entities involved in the proposed model are:

A. Locker System
B. Electric field proximity Sensor
C. Base Station Module (MCU- Micro Controlling Unit)
D. GSM Modem
E. Mobile Phone

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

A. Locker System: In the locker system (be it a physical key based locker or pattern based locker), the proposed instrument model is to be placed inside the locker access interface (i.e., in the key slot of the key based locker and in the pattern interface of pattern based locker). The instrument module comprises of an instrument which communicates with the electric field proximity sensor when a change in electric field occurs. Section 3.2.1 details the communication establishment process with the electric field proximity sensor.

B. Electric field proximity Sensor: A proximity sensor is a sensor that is able to detect the presence of nearby objects without any physical contact. The same principle is reflected in an electric field proximity sensor. In this, the change in electric field that occurs in the instrument is detected without any physical contact. And then the sensor communicates with the micro controller. Section 3.3 details the stages and process flow involved in an electric field proximity sensor.

C. Base Station Module (MCU- Micro Controlling Unit): A microcontroller is a small computer on an IC containing a core processor, memory, and programmable input/output peripherals. Here, the micro controller acts as a base station connected to the electric field proximity sensor (input) and GSM modem (output). When a communication from electric field proximity sensor is made, the MCU activates the GSM connected on it.

D. GSM Modem: The responsibility of GSM (Global System for Mobile communication) modem is to trigger an alert message as and when activation by the MCU is made.

E. Mobile Phone: The customer and the bank manager are alerted as and when an access to the locker system is being made. This provides a strong security by limiting the frauds.

3.1 Algorithm citing the complete process of the proposed model

Objective: Alerting both the customer and bank manager about user access on the locker

Notations:

U: User who tries to access the locker system
IL: Locker Interface for user access
Inst: Instrument which is deployed inside the locker interface
A_c: Activation process involved in the process flow
Δ: Change in electric field developed in the instrument
S.U: Sensing Unit present inside the electric field proximity sensor
P.U: Processing Unit which involves in the processing of analogous to digital data
A.D: Analogous Data sensed from change in electric field
D.D: Digital Data produced by the P.U
MCU: Micro controller Unit
GSM: Global System for Mobile communication
M_c: Customer's mobile phone
M_{BM}: Bank Manager's mobile phone

Input: User Access
Output: Alert message

Algorithm:

Step-1: /* When a user accesses the locker system */
U→IL: A_c (inst); /* User access through the locker interface establishes an ambiguous contact with the instrument and activates it */
Step-2: /* this contact causes a change in the electric field in the instrument */

A_c (inst): Δ; /* the process of how change in electric field (Δ) occurs is

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

discussed in 3.2.1 */

Step-3: /* the sensing unit senses the change in electric field and sends the analogous data to the processing unit */

Δ→ S.U: A.D→ P.U;

Step-4: /* the captured analogous data is converted to digital data by the processing unit */

P.U: A.D→ D.D; /* the conversion process of analogous to digital data is discussed in 3.3 */

Step-5: /* Processed digital data is passed to the MCU and this in turn activates the GSM */

D.D→ MCU: A_c (GSM);

Step-6: /* GSM alerts both the customer's and the bank managers mobile phones */

Ac (GSM): A_L → (M_c && M_{BM});

3.2 Design and working of the instrument module present inside the locker interface

The instrument module comprises of an instrument which communicates with the electric field proximity sensor when a change in electric field occurs. This communication establishment process with the electric field proximity sensor is discussed after the main algorithm. The instrument is a collection of skinny wires running on either sides of an insulator as shown in fig 3.

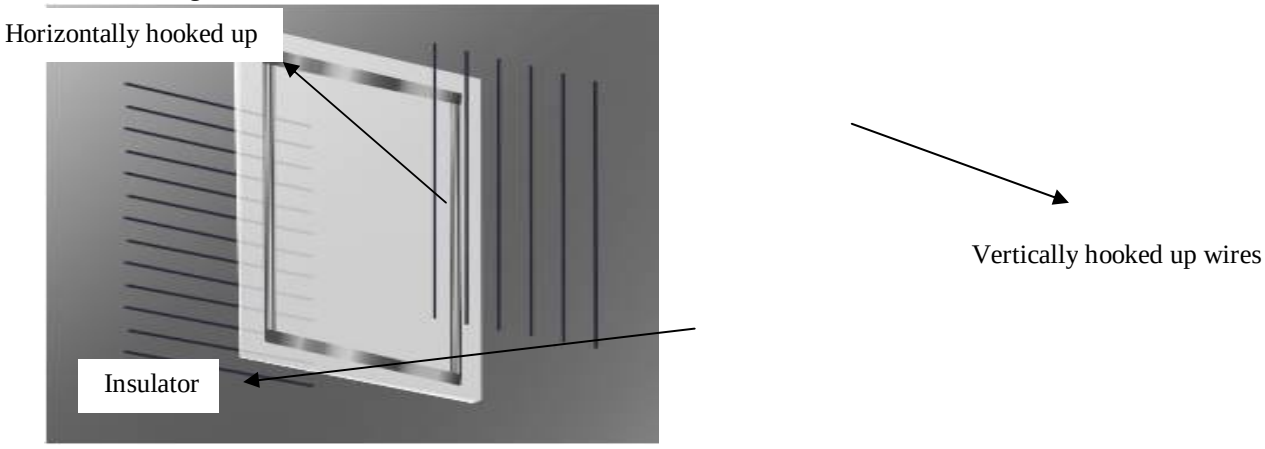


Fig 3: Skinny wires running on either sides of the insulating material

On one side, wires are made to run vertically, and on the other side wires are made to run horizontally [9]. The reason to use an insulator is that, insulators have a property where electrons don't flow and are tightly binded inside an atom. This prevents it to produce electric charge and makes it a bad conductor of electricity. The vertical wires are hooked up to the positive terminal of the battery, and the horizontally placed wires are hooked up to negative terminal of the battery. The positive terminal pulls electrons from the vertical wire and the negative terminal pumps the electrons into the horizontal wires. This establishes an electric charge between the two wires. The front view of the skinny wires running over either sides of the insulator is shown in fig 4. The electric charge is uniform in every cell of the grid pattern.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

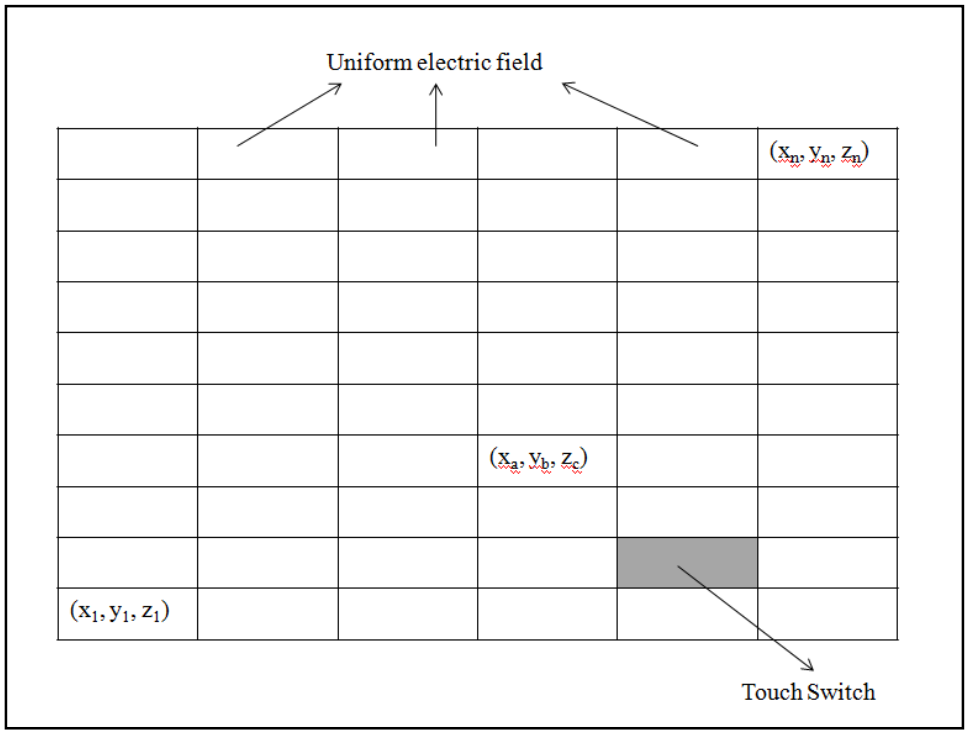


Fig 4: Front view of the Skinny wires running over either sides of the insulator form a grid pattern

This instrument is to be placed within the interface (through which the customer gets an access to the locker) present on the locker (both key based and pattern based locker systems). The complications involved in the placement of the instrument within the interface of the locker are detailed later in section 3.4. When an access to the interface is made, this in turn establishes an indirect contact to the instrument that is placed inside the interface. This ambiguous access will cause the hooked up wires on either sides of the insulator to come closer and hence induces an extra electric filed in few cells of the grid. This extra electric field is detected by an electric field proximity sensor which is fixed on a MCU (Micro Controlled Unit).

3.2.1 Algorithm presenting working of the instrument and the communication establishment process between the instrument and the electric field proximity sensor

Objective: Sensing the change in electric field developed in the instrument

Notations:

1. P= $\{(x_i, y_j, z_k) \mid (i, j, k)=1 \text{ to } n\}$: Set of all cells (Touch switches) in the grid pattern
2. P_p= $\{(x_a, y_b, z_c) \mid (a, ,b ,c)= 1 \text{ to } n \text{ and } (x_a, y_b, z_c) \neq$ distorted electric field touch switches$\}$
3. q: Static charge built in P due to wire hook ups to the battery terminal
4. F: Force of attraction between charged wires on charge point (q) throughout P
5. E: Uniform electric field built in P due to force (F) exerted on charge (q)
6. q': Distorted charge developed at point $(x_i, ,y_j, z_k)$ of the grid due to key insertion in the slot
7. F': Force of attraction developed on charge (q') due to key insertion
8. Δ: Change in electric field
9. E': Distorted electric field at point (x_i, y_j, z_k) due to distorted force (F') on charge (q')

Input: User Access
Output: Electric field change produced in the instrument module

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

Algorithm:

Step-1: /* Electric field (E) built due to force of attraction (F) between charged wires on q */

$E(x_i, y_j, z_k, q) = F(x_i, y_j, z_k)/ q$ /* Electric field developed at a point (x_a, y_b, z_c) */
$E(x_i, y_j, z_k) = E(x_i, y_j, z_k, q)$ /* as electric field is uniform throughout P */

Step-2: /* Consequences of accessing the locker through the interface are sequenced */

While (access through the interface is being made)
Do
$E'(x_i, y_j, z_k) = F'(x_i, y_j, z_k)/ q'$; /* Distorted electric field (E') */

$\Delta = E'(x_i, y_j, z_k) - E(x_a, y_b, z_c)$; /* Change in electric field */

IF ($\Delta \neq 0$) Then /* Check for electric field distortion */
{
Electric field proximity sensor senses the change in electric field
}
END_IF

END while

It is significant to notice that temperature change does not affect the working of the proposed instrumental model because, when temperature changes electric field distortion happens uniformly throughout the grid (i.e., in every cell of the grid) and hence it would not be possible for the electric field proximity sensor to detect the change. This scenario is explained in 3.2.2.

3.2.2 Algorithm showing whether temperature change affects the working of the instrument or not

Objective: Sensing the change in electric field by electric field proximity sensor

Notations:

1. $P = \{(x_i, y_j, z_k) \mid (i, j, k)=1 \text{ to } n\}$: Set of all cells (Touch switches) in the grid pattern
2. q_v: Distorted charge developed in P due to wire hook ups to the battery terminal
3. F_v: Force of attraction between charged wires on charge point (q_v) throughout P
4. E_v: Uniform electric field built in P due to force (F_v) exerted on charge (q_v)

Input: Temperature change (increase || decrease)
Output: Uniform change detection

Algorithm:

Step-1: /* Temperature change causes uniform change in electric field throughout grid */

$E_v(x_i, y_j, z_k) = F_v(x_i, y_j, z_k)/ q_v$

Step-2: While (Temperature changes)

do

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

```
                IF (Ev (xi, yj, zk) - Ev (xp, yq, zr) ≠ 0)    /* (xp, yq, zr) is some point in the grid */

{
                        Electric field proximity sensor senses the change in electric field
                    }

                END_IF
                ELSE uniform change detected
            END while
```

3.3 Working of electric field proximity sensor

A proximity sensor is a sensor that is able to detect the presence of nearby objects without any physical contact. The same principle is reflected in an electric field proximity sensor. In this, the presence of electric field is detected without any physical contact. As discussed early electric field is induced in every touch cell of the grid pattern and as and when a disorder in this electric field happens, the electric field proximity sensor detects the change in the electric field induced in the instrument. This change is sensed/ detected and a communication is made to the micro controlled unit.

Algorithm presenting the work flow process in the Electric field Proximity Sensor module

Objective: Conversion of the sensed data to digital form

Notations:

1. q': Distorted charge developed at point (x_i, ,y_j, z_k) of the grid due to key insertion in the slot
2. F': Force of attraction developed on charge (q') due to key insertion
3. Δ: Change in electric field
4. E: Uniform electric field built in P due to force (F) exerted on charge (q)
5. E': Distorted electric field at point (x_i, y_j, z_k) due to distorted force (F') on charge (q')
6. S.U: Sensing Unit present in the Electric field Proximity Sensor
7. P.U: Processing Unit in an Electric field Proximity Sensor
8. A.D: Analog data sensed from change in electric field
9. $(A.D)_q$: Quantized analog data
10. D.D: Digital Data produced by the P.U
11. COM: Comparator for converting analog data to digital data

Input: Change in electric field (Δ)
Output: Digital Data

Algorithm:

Step-1: /* Change in electric field is sensed by the S.U of Electric field Proximity Sensor */

```
E' (xi, yj, zk) = F' (xi, yj, zk)/ q';
Δ = E' (xi, yj, zk) - E (xi, yj, zk);        /* Change in electric field (Δ)*/
S.U←Δ;                                       /* Sensing unit senses the change in electric field (Δ)*/
```

Step-2: /* Nature of sensed data */

```
A.D ← Sensed Data                            /* The data sensed by the S.U is analogous */
P.U← A.D;
```

Step-3: /* When A.D is passed as an input to the processing Unit, it converts it into D.D */

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

While (True)
Do

Quantize A.D;
IF (Quantization completed) THEN Break;
ELSE CONTINUE;

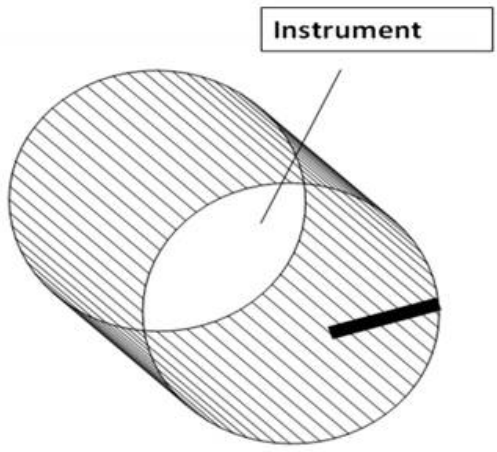
END while
$(A.D)_q$→COM: D.D;

3.4 Instrument set up in the locker interface of both key based lockers and number based lockers

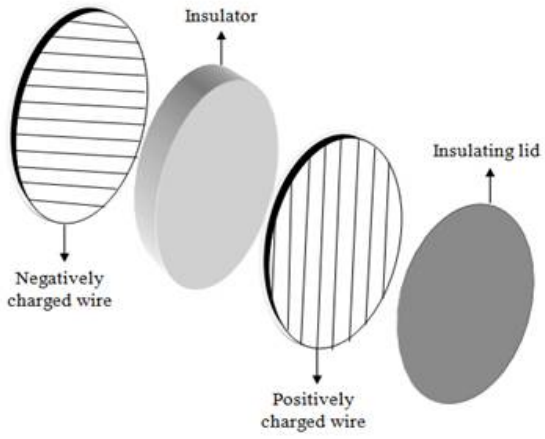
The complication involved in the proposed model is the placement of instrument inside the locker interface. This process of instrument deployment in the interface differs in both the key based locker systems and the pattern based locker systems which are discussed below:

a) Instrument set up in key based locker systems
b) Instrument set up in pattern based locker systems

a) Instrument set up in key based locker systems: (To check an attempt made by unauthorized user to access a physical key locker through cloned keys): The instrument setup is to be deployed underneath the key slot of the locker as shown in figure 5.1, so that whenever an unauthorized access is made using the cloned key through the key slot, it gets in contact with the instrument which in turn builds an electric field charge in the touch grid of the instrument and the proximity sensor triggers a message to the customer and the bank manager through the GSM modem setup by sensing the change in the electric field sensitivity. However, there is a challenge in this model i.e., when the key is inserted in the key slot it gets in direct contact with the charged up instrument and hence generates shock. To avoid this, the instrument is kept away from direct contact of key using an insulating lid interface, so that irrespective of the type of material the key is made off (i.e., either a conductor or an insulator) it does not generate shock. The internal structure of the instrument model deployed inside the key slot of the key based locker system is shown in figure 5.2.



(5.1): Instrument deployment in the key slot of the key based locker



(5.2): Internal structure of instrument in a key based locker system

Fig 5: Instrument deployment in a key based locker and its internal structure

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

b) Instrument set up in pattern based locker systems: (To check an attempt made by unauthorized user to access a pattern based locker system): The above discussed instrument design model works fine in a key based locker system. But, the scenario involved in a pattern based locker system is different. There are two different cases involved in this model, which are:

- When interface of the pattern based locker is made of a conductive material
- When interface of the pattern based locker is made of a non- conductive material

In the first case, the instrument model proposed for the key based locker system in figure 5.2 works fine. But, in the second case as the interface of the pattern based locker system is made of a non- conductive material, the insulating cover lid will be an overhead in the instrument design. Therefore the deflated instrument design model in the second case of the pattern based locker system need not have the insulating lid.

A comparison between the existing and the proposed system is tabulated in table 3.

Table 3: Comparison between existing and the proposed system

S. No	Existing System	Proposed System
1	Passive System	Active System
2	Vulnerable to Attacks	No Vulnerability
3	Security Issues	Highly secured
4	Access cannot be sensed	Sensitive to access
5	Intimation to customer about his/her locker access is not made	Customer is alarmed during his/her locker access

IV. CONCLUSION

In this paper a sensor based instrumental framework is presented which helps in enhancing the security aspects of a locker system. An electric field proximity sensor is used to support the working of the instrument model. The main objective is to curb the internal frauds (which involves the banker) occurring in bank locker systems. Past works (Raghu Ram.Gangi, et al. [3]) on security enhancement in bank lockers involved complex methodologies and were more of digital interface [8]. They are not only costly but also are prone to many security issues (especially internal fraud issues) as in Ramani R., et al. [5]. But, the proposed model not only reduces cost but also curbs internal frauds occurring in banks.

REFERENCES

[1] Arampatzis, Th; Lygeros, J.; Manesis, S., "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks," Intelligent Control, 2005. Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation , vol., no., pp.719,724, 27-29 June 2005.
[2] Y. L. Lay, et al. “Biometric Locker System”. Proceedings of the World Congress on Engineering and Computer Science 2011, pp 366-369.
[3] Raghu Ram.Gangi, et al. “Locker opening and closing system using RFID, fingerprint, password and GSM”. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 2, March – April 2013, pp 142- 145.
[4] The Indian Express Archive- http://www.indianexpress.com/news/rs-28crore-fraud-cbi-raids-houses-of-bank-officials-construction-firm-owner/1117451/
[5] Ramani R., et al. “Bank Locker Security System based on RFID and GSM Technology”. International Journal of Computer Applications 57(18):15-20, November 2012. Published by Foundation of Computer Science, New York, USA.
[6] Bank Locker policy- http://www.lvbank.com/userfiles/file/lockerpolicy.pdf
[7] About Bank Locker security issues- http://wqaindia.hubpages.com/hub/How-Secured-are-Bank-Lockers
[8] Digitalized security system- http://www.dcmsme.gov.in/reports/electronic/Digitalsafelocker.pdf
[9] IPhone Working- http://electronics.howstuffworks.com/iphone2.htm