International Journal of Advance Research in Science and Engineering
Vol. No.6, Special Issue (01), September 2017, BVCNSCS 2017
www.ijarse.com
IJARSE
ISSN 2319 - 8354

SENSOR-ENABLED DEVICES, APPLICATIONS AND SECURITY ISSUES

P. S. K. Kalyan
M.COM
Bhavan's Vivekananda College
Sainikpuri, Secunderabad, Telangana (India)

ABSTRACT: *The globe is now stepping into an advanced virtual or digital age with various advancements in technology both physical and virtual. In recent years, the technology has become more user friendly with the development of micro and nano devices. The network or the inter-connection between these things is known as "Internet of Things" (IoT). With the inclusion of advanced wireless sensor technologies, the human life has become easier with more accurate and secured outputs. The introduction of various sensors has paved a way for the birth of smart cities, smart vehicles, smart phones and other sensor enabled devices.*

Keywords: Digital age, technology, network, IoT, wireless sensors, secured outputs, sensor enabled devices.

I. INTRODUCTION

In the present smart world, almost every person has a one or the other smart device, it may be a smart phone, smart cards, various types of scanners or any other smart device containing hi-tech sensors which are used for various accessibility and security purposes.

According to the International Data Corporation (IDC), a total of 344.3 million smart phones shipped worldwide in the first quarter of 2017 (1Q17). Worldwide smart phone shipments grew 3.4% in 1Q17 year over year. With this we can say that the usage of smart phones is increasing seamlessly day by day.

II. METHODOLOGY

The information is gathered from various secondary sources such as internet, various published articles, survey reports and from other literary works.

III. OBJECTIVES

A. To study the applications of various sensors

The main objective of this article is to study the main applications of various sensors used in various devices.

B. To discuss various security issues

The other main objective of this article is to discuss various security risks and issues in using various sensor-enabled devices and to suggest various measures to overcome the same.

IV. APPLICATIONS OF SENSORS

This section will discuss various major sensors today used and various applications of these sensors.

Though there are many sensor enabled devices are available in the market, the study mainly focuses on smart phones because, latest smart phones comes with various advanced sensor technologies out of the box and majority of the people uses smart phones.

Sensor wise elaboration is given below.

A. Fingerprint Scanners

Most of the today's smart phones come with fingerprint scanner support. Fingerprint scanners are the small sensors that accept and identify the fingerprints of a person. These scanners are mainly used for biometric identification and data authentication purposes. If these sensors detect an invalid identification, access for which it is protecting will be denied with an alert message. It stores the fingerprints of the owner at the time of calibration and compares it every time when someone tries to access the data.

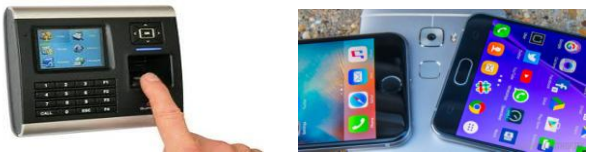

Figure 1: Fingerprint Scanners

B. Iris scanners

These are the scanners that scan the human irises around the pupil of the eye. Every individual iris has a unique pattern and these scanners recognize these patterns using mathematical and statistical pattern-recognition methods for automated biometric identification purposes. Iris recognition is different from retinal recognition. Iris scanners use video images for pattern recognition and retinal scanners are based on ocular biometric technology which recognizes unique patterns on person's retinal blood vessels and often mistook with iris scanners.

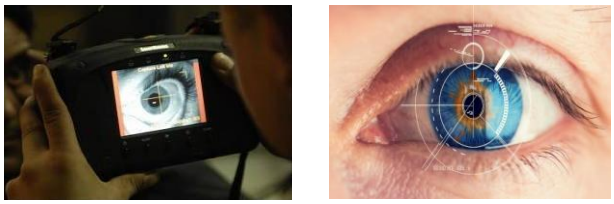

Figure 2: Iris scanner and Iris pattern recognition.

C. Electronic Data Capture (EDC)

The Electronic Data Capture devices or commonly known as Card-Swipe machines use infrared rays to read the information stored in the magnetic strip/chip on the debit and credit cards. The information is sent to the acquirer company

and then to the issuing bank for authorization. Issuing Bank can accept or reject the authorization request. Once the request is accepted, the transaction will take place and the machine prints the slip with transaction details for the purpose of merchant's records.

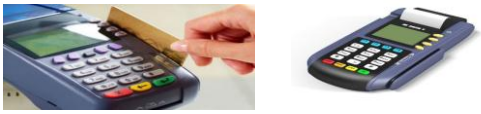

Figure 3: Electronic Data Capture (EDC) Machines.

D. Barcode and QR code readers

These readers scan and read the printed barcodes and out puts the content to a computer. These scanners use light sensor to capture and read the barcode content and a decoder circuitry to convert optical impulses to electrical ones to transfer to a computer. There are various types of barcode readers, some of them are listed below.

- Pen-type scanners
- Laser scanners
- CCD readers (LED scanners)
- Cameras-based scanners
- Omni directional scanners

Apart from above all types, barcodes can also be scanned using smart phone cameras.

Figure 4: Barcode scanners.

V. SECURITY ISSUES

Though there are various technological advancements in the run of improving security aspects, the security of the content still remains doubtful because of the advanced techniques used by the hackers. Solarin is the most secured and non hackable phone in the world made by Sirin labs providing extreme level encryption for calls and messages though a bit expensive ($ 14000). Following are various security issues in using sensor enabled devices.

A. Fingerprint scanners

Almost all smart phones in the present market have fingerprint scanners for user authorization and accessibility for the content in the device. Various security risks in using fingerprint authorization are as follows.

- Most of the android devices are easily hacked and the data stored in them are easily stolen by the hackers .
- Fingerprint scanners store the user data at the time of calibration and hackers can easily access the stored data and use it for other illegal activities.
- When using fingerprints in biometric identification purposes, entire fingerprints structure is stored in the third party devices which will lead to security risks.

B. Iris scanners

The latest innovation in the biometric identification technology is the introduction of "Iris scanners". These share the same security risks as with the fingerprint scanners. The patterns of human iris are stored in the device and the alternative pass code also cached in the device which can be easily accessed when hacked. Comparatively, iris scanners are more secure than fingerprint scanners because fingerprint impressions of an individual can easily be copied but iris of an individual cannot be copied. Only way to crack the iris scanner is by hacking the device.

C. Electronic Data Capture (EDC machines).

EDC machines or card-swipe machines are one of the most hsck prone devices in the market. Users are afraid of giving their card details due to very high security risks in using card-swipe machines. Various reasons for users being afraid of using card-swipe nachines are listetd below.

- All the card details are scanned by the swipe machines.
- User need to enter his security code in trust of a third party device.
- Scanner stores all the card and user bank account details which are very confidential.
- User/customer doesn't know whether the account details are cleared from the device after the completion of the transaction.
- Customers feel insecure to give their security pin to a stranger or to his device.

D. Barcode and QR code scanners

These type of scanners are generally used in shopping malls to scan barcodes or QR codes labeled on the products. There are very less security risk using these scanners because no personal information is stored in the device. The major noticeable risk with these scanners is wrong prices if the scanner fails to scan/decode the barcode information correctly. Customer need to check the MRP of the product physically in case of device failure which is not done in real cases, customers simply pays the money and after regrets for the mistake done.

VI. SUGGESTIONS

In light of above all security risks, various suggestions have been drawn which are as under:

- Users of fingerprint enabled smart phone devices need to frequently clear their device's cache memory to ensure that the data stored in that memory is being erased.
- While using Iris scanners, users need to do the same as in the case of fingerprint scanners.
- Customers need to ensure that the fingerprint scanner bed is cleaned to ensure that no fingerprint impressions left on the scanner bed.
- While using card swipe machines and ATMs, customers need to be very careful and check

whether the merchant is using the authorized machines and everything is cleared after the completion of the payment process.

- When giving card details in the ATM machine, card holder have to check the number pad on the machine because various chips are incorporated under the ATM machine number pad to record the key strokes and hack the card holder's accounts for personal and illegal use.
- After the money has been drawn from the machine, user need to wait for a moment to check whether the screen is returned to Bank's home page or still on a transaction page.
- Customer need to cross check the bill printed by the barcode scanner with the MRP on the product physically.

Though these are all known facts, customers ignore these small things and keep their data in the hands of hackers unknowingly.

VII. CONCLUSION

Though the increased usage of advanced technologies points the development in the latest technologies, there are also increasing security risks alongside.

People using latest technologies must be aware of the security risk of their data and must know that the sensors in the devices they use have an access to their personal information and must take safety measures and live happily without any personal data risks.

VIII. ACKNOWLEDGMENT

I would like to thank Prof. Y. Ashok, Principal, Bhavan's Vivekananda Degree College. I thank all the lecturers of Computer Science Department, Bhavan's Vivekananda Degree College who helped in gathering the information regarding the article. A special thanks to Ms. S. Jayalaxmi, Ms. M.Amitha and Mr. N. Bhaskar, lecturers in Computer Science Department, Bhavan's Vivekananda Degree College.

IX. REFERENCES

[1]. https://www.digicert.com/blog/biometric-authentication-methods/

[2]. http://www.vocativ.com/407315/iris-scanners-smartphone-security/

[3].https://developer.android.com/guide/topics/sensors/sensors_overview.html

[4]. http://www.idc.com/promo/smartphone-market-share/vendor

[5]. https://en.wikipedia.org/wiki/Iris_recognition

[6]. https://www.quora.com/What-is-the-back-end-process-of-a-transaction-done-from-a-card-swiping-terminal-using-a-debit-credit-card

[7]. https://en.wikipedia.org/wiki/Electronic_data_capture

[8]. https://en.wikipedia.org/wiki/Barcode_reader

[9]. https://www.theverge.com/2016/5/2/11540962/iphone-samsung-fingerprint-duplicate-hack-security

[10]. Juan Chen , Zhengkui Lin, Ying Hu 1 and Bailing Wang, "Hiding the Source Based on Limited Flooding for Sensor Networks". ISSN 1424-8220, doi:10.3390/s151129129.

[11]. Naser Alajmi and Khaled Elleithy, "Multi-Layer Approach for the Detection of Selective Forwarding Attacks Naser Alajmi * and Khaled Elleithy". ISSN 1424-8220, doi:10.3390/s151129332