ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 4, March 2016*

National Conference on Signal Processing, Instrumentation and Communication Engineering (SPICE' 16)

Organized by

Dept. of ECE, Mar Baselios Institute of Technology & Science (MBITS), Kothamangalam, Kerala-686693, India

An Effective Biometric Security System Enabled Through Wireless Link

Sherin Thomas[1], Eldhose P Sim[2]

Assistant Professor, Dept. of ECE, Mar Baselios Institute of Technology and Science, Nellimattom, Kothamangalam, Kerala, India

Assistant Professor, Dept. of ECE, Cochin Institute of Science and Technology, Nellimattom, Kothamangalam, Kerala, India

ABSTRACT: We know that most of the electronic gadgets which is in need of security are being secured with certain confidential passwords, PINs or visual patterns during the past years, but, which in turn became vulnerable to intrusion and theft. Thus a better alternative, the biometric authentication was introduced. Biometric security systems have been researched for many years. The fingerprint biometric security thus seemed to be a bit more secure because a fingerprint is extremely unique and difficult to mimic. But then too if a cell phone is only protected by biometrics, it can still be resold and used once it is wiped clean (flashing). Additionally, a fingerprint verification system in the mobile phone combined with a fingerprint biometric feature enabled mobile charger that acts as a dongle with a solid state relay, will be a viable solution to theft. But this put forward the difficulty that if the cell phone is ever to be separated from its synced charger indefinitely, the cell phone would be rendered useless. For that this paper suggests a new methodology for authentication with an additional feature which keeps the cell phone alive in the absence of charger. To meet this demand we have also provide a novel approach known as radio frequency energy harvesting by using rectenna. Rectenna is a rectifying antenna which converts the electromagnetic waves to electrical DC signal. Whenever the user wants to log in to the mobile without the help of the charger, the mobile device and charger is configured through a remote VPN network; and thus the biometric security is enabled via this wireless link. We can apply this security feature to any electronic gadgets, which thus provides a biometric mobile gadget with high level security wireless charging.

KEYWORDS: Rectenna, Biometrics, Radio frequency energy harvesting, VPN network.

I.INTRODUCTION

In the present world every customers are using the smart phones, the customer requirements are also increasing day by day. The main issues we are facing while using a smart phone is charging problem and secondary issue is that the security concern in terms of confidential data may be carry by the device. For stratifying the secondary issue there are lot of ways are available, now a day's all smart phones are protected by either passwords or PIN or visual patterns. All the exiting methods for protecting the mobile are not highly secure; there may be a chance of instruction. The proposed works are aiming to solve the both issues that are discussed early. The security features are enabled by using biometric feature and the charging issues are overcome by designing a new device called rectenna.

II.RELATED WORK

As the existing system, a cell phone and a cell phone charger would utilize a capacitive fingerprint reader which enables functionality. For example, when a cell phone is purchased, the cell phone would be programmed with the user's fingerprint. At that point in time, the cell phone charger would also be programmed with the user's fingerprint and can only be re-programmed by the manufacturer. The fingerprints then become an encrypted key which allows the two devices to be synced. This could also apply to a car charger, house charger, and USB cord. With the USB cord that connects to a PC, the phone's biometric reader could act as the authorization point. Once the cell phone and charger contain the encrypted fingerprint key, the charger acts as a device dongle embedded with a solid state relay (on/off) that has to plug into the phone and be authorized to activate the charge. Additionally, the cell phone should be manufactured with a built-in lithium battery that cannot be removed. If the cell phone is ever to be separated from its synced charger

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 4, March 2016*

National Conference on Signal Processing, Instrumentation and Communication Engineering (SPICE' 16)

Organized by

Dept. of ECE, Mar Baselios Institute of Technology & Science (MBITS), Kothamangalam, Kerala-686693, India

indefinitely, the cell phone would be rendered useless. Another security feature that would be added is programming the power button to only lock and unlock the phone. This way if a cell phone were to be stolen, there would be no way to shutdown the phone without proper authorization.

The user could then use a program such as Lookout (Android OS) to remotely destroy the data in a theft situation without having to worry about their phone being turned off. Ultimately, by the time someone steals a cell phone and attempts to hack the phone using artificial fingerprints, there should be enough time for the owner to remove their profile which is backed up onto a remote server. As we shall see later through the experimental methods in this research, biometric systems alone are too vulnerable and this proposed theory will be tested. Currently, the RF energy harvesting has attracted much attention to supply power for some small devices such as wearable and battery-free sensors [2]. The core device of such a wireless energy harvesting system is the rectifying antenna which is also called as the rectenna.

III.PROBLEM DEFINITION

As considering the existing system found that the cell phone became useless without the charger. If the mobile user forgot to take the charger (Treat it as a device) while the user is out of station there is no other way to log on to the mobile and to enable charging. So we can convey that the biometric features that are included in the mobile device do not satisfy all the requirements of the user. Even though the mobile phone is not compactable with other mobile chargers, and whenever the charge becomes low, there is a method to charge the mobile with the authentication of the same biometric features. For that this paper suggest a new methodology for authentication with the same biometric feature and enables charging without the help of biometric charger i.e. by using rectenna which converts the electromagnetic waves to electrical DC signal. In the last few years, excluding high power applications, wireless power transfer has been often used in microwave radiation with relatively low power densities [2].

IV. PROPOSED SYSTEM AND ARCHITECTURE

The proposed system deals with the compatibility of the mobile device with the same biometric features without carrying charger and enables charging when the battery becomes low through an external device (Not a portable charger). For that if the user is out of station and enables the user to log in to the system. The pre programming with the biometric data is done in the mobile device as well as in the charger. Whenever the user wants to log in to the mobile without the help of the charger, the mobile device and charger is configured through a remote VPN network .When ever user try to give the biometric features input to the mobile device, it is verified with the template stored in the mobile device which is compared and a copy of this received input transferred to destination as an image and is compared with the template stored in the biometric charger. If a match is found, then it allows logging in to the system.

A drawback that can arise in the proposed system is the continuous connectivity of the mobile with internet and thus the battery life. In the present scenario we know that the battery life of a smart phone is very less. In order to resolve this issue and enables charging through the same authentication with an external device known as rectenna (rectifying antenna), a device used in wireless power transmission. A rectenna is a specialized radio antenna which is used to convert radio waves into direct current electricity. It consists of a dipole antenna with an RF diode connected across the dipole elements. The diode rectifies the AC current induced in the antenna by the microwaves, to produce DC power, which powers a load connected across the diode. Schottky diodes are usually used because they have the lowest voltage drop and highest speed and therefore have the lowest power losses due to conduction and switching. Large rectennas consist of an array of many such dipole elements

Fig.1 shows a block diagram of a basic energy harvesting system, where a transducer typically an antenna or antenna array harvests ambient electromagnetic energy. This harvested energy is rectified and filtered. The recovered DC then, either powers a low powered device directly, or stored in a super capacitor for higher power low duty-cycle operation.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 4, March 2016*

National Conference on Signal Processing, Instrumentation and Communication Engineering (SPICE' 16)

Organized by

Dept. of ECE, Mar Baselios Institute of Technology & Science (MBITS), Kothamangalam, Kerala-686693, India

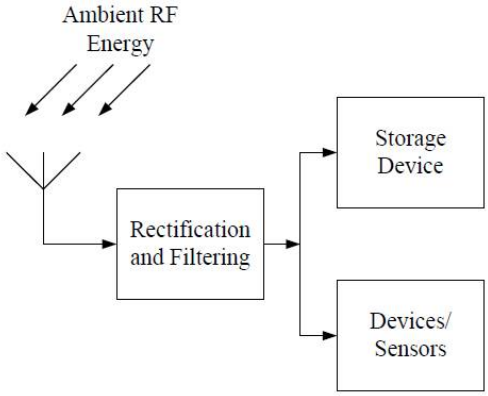

Fig.1: Basic energy harvesting block diagram

The safety regulation can be verified by the specific absorption rate (SAR) distribution in tissues surrounding the head-mountable passive DBS. Radio frequency electrical current in rectenna will induce electric field in surrounding tissues. Moreover, a part of the radiated EM wave from the far filed transmitter will be directly absorbed into tissues and may increase the tissue temperature. The absorption is due to the power loss with dielectric polarization. The SAR is a measure of the amount of the electromagnetic energy absorbed by biological tissue. The SAR is calculated by measuring the electric field in the stimulated tissue around the device. The formula used for SAR calculation is [1]:

$$SAR = (\sigma/\rho)\,|E|^2 = J^2/\rho\sigma \ [W/kg] \quad (1)$$

Where, E is the rms value of the electric field strength in the tissue [V/m], J is the current density [A/m], σ is the conductivity of body tissue [S/m], and ρ is the density of body tissues [kg/m3]. The value of SAR depends on the operating frequency, the antenna type and the distance between the antenna and the body tissue.

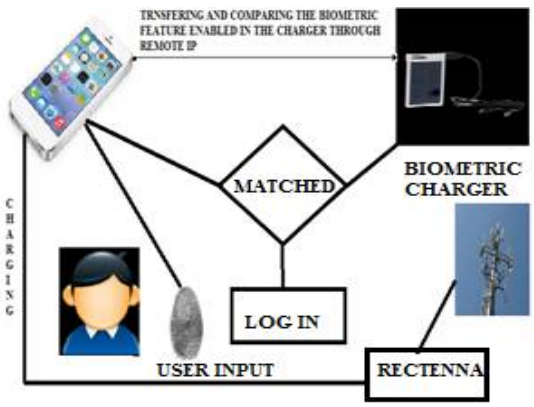

Fig. 2: Proposed architecture

V. PROPOSED ALGORITHM

Input: User finger print
Output: Hashed Template

1) Receive the user input from the user
2) Process the input
3) Extract the features from the input
4) Create a template
5) Hash the template using any security algorithm
6) Store the template in both devices for each time when user input comes
7) Check with stored template and verify.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 4, March 2016*

National Conference on Signal Processing, Instrumentation and Communication Engineering (SPICE' 16)

Organized by

Dept. of ECE, Mar Baselios Institute of Technology & Science (MBITS), Kothamangalam, Kerala-686693, India

If (match)
Log on to the mobile
Else
Mobile accessing is blocked
End

VI.CONCLUSION AND FUTURE WORK

The knowledge-based or password-based (PIN) authentication methods have been proven to be weak solutions as the probability of tracking these passwords is high. [4] Biometric authentication is a better alternative solution against intrusions and theft of mobile cellular devices and must be combined with other technology to create better security. Overall, the majority of faces, voices, and fingerprints are not duplicated unless replicated .Looking all the aspects of biometric system we see that it offers very high accuracy, and requires only small storage space, thus reducing the size of the database memory required.
By taking stock of the biometric fingerprint feature, we see that it can make mistakes with the dryness or dirty of the finger's skin, as well as with the age. Another problem that we must consider replications of faces, voices, and fingerprints can be used to obtain authorization illegally [3].

To establish a fail-safe, there must be a system that combines biometrics with other hardware such as rectenna (figure 1), a device that handles wireless charging. Rectenna combined with VPN and biometric provides a much better security against theft and intrusion. In other words, if a cell phone is only protected by biometrics, it can still be resold and used once it is wiped clean. Some independent business owners even like to take cell phones and flash them under another provider to access a market that is not typically available. By incorporating biometrics into a device while establishing a key/lock system (cell phone and charger), theft and intrusion of cell phones would be discouraged. Furthermore, it is important to note that this application can be utilized for any device that requires power.

Even though the proposed system faces lot of difficulties in the sense of DDOS attacks and IP spoofing an additional feature is to be used in the smart phones so as to make the system to be more secure.
In future the system can be developed focusing on the following facts:

- Implementation of the system at lower cost is difficult
- To allow the user to make changes in the biometric feature in charger when in need.
- Once the charger get damaged the system will became inactive
- Changes in the biometric characters of human being make the system useless.
- Increasing rectenna performance at lower power level.
- Making rectenna structure even more compact.
- Heating up of battery due to continuous charging while using rectenna.

REFERENCES

[1] N. A. Saidatul, A. A. H. Azremi, R. B. Ahmad, P. J. Soh, and F. Malek, ''Multiband fractal planar inverted F antenna (F-PIFA) for mobile phone application,'' PIER B, vol. 14, no. 1, pp. 127–148, 2009.
[2] Monti, G., Corchia, L. and Tarricone, L. (2013) UHF Wearable Rectenna *on Textile Materials. IEEE Transactions on Antennas and Propagation*, 61, 3869-3873.
[3] H. Manabe, R. Sasaki, Y. Yamakawa, and T. Sasamoto, "Security Evaluation of Biometrics Authentication,"Electronics & Communication Engineering Journal, pp. 34-39, Sep. 2009.
[4] E. Syta, S. Kurkovsky, and B. Casano, "RFID-based Authentication Middleware for Mobile Devices," Electronics & Communication Engineering Journal, pp. 1-10, Jan. 2010.
[5] N. Goldsman, N. Dhar, F.Yesilkoy, A. Akturk, S. Potbhare, M. Peckerar "Simulation Study of rectifying antenna structure for Infrared wave energy harvesting applications" SISPAD 2012, September 5-7, 2012, Denver, CO, USA.
[6] M. S. Sodha and A. Dixit, A critical look at electric field emission of electrons from metallic surfaces, J. Appl. Phys. **104**, 064909, 2008.
[7] A.P.Sample,D.A.Meyer and L.R.Smith "Analysis experimental results and range adaption of magnetically coupled reasonators for wireless power transfer,"IEEE Trans.ind.electron.,vol.58,no.2,pp.544-554 feb 2011.
[8] I. Garnica, I. Casunova and I. Lin "high off mid range wireless power system in 2011 IEEE MTT-S-information microwave workshop series on innovative wireless power transmission technologies system and applications. (IMWS), Kyoto, may 2011 pp.73-76.