International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Patient Identification Using Fingerprint in Global Health

Gaurav Patni *[1], Dr. Shilpa Sharma[2]

*[1]Research Scholar, School of Computer & Systems Sciences, Jaipur National University, Jaipur, Rajasthan, India
[2] Associate Professor, School of Computer & Systems Sciences, Jaipur National University, Jaipur, Rajasthan, India

ABSTRACT

Identifying the right patient with accuracy and matching the patient's personal identify with the correct treatment required for him/her or service that is an important component of patient's safety. The misidentification of in-patients and out-patients can happen all the medical staff members too easily given the fast-paced nature of medical care, and unfortunately, we have had and continue to have our share of these errors. This is why we have made patient identification the first of its Patient Safety Goals using proper Biometric Fingerprint Identification System. If we cannot identify patients properly, how can we expect them to trust us with their health care and treatment ? Therefore we are changing our expectations for how this process should be performed. We are working with the concept of Right Treatment to the Right Patient at the Right Time using the proper identification of the Right Patient using Biometric Fingerprint Identification System.

Keywords: Patient Identification, Biometric Fingerprint, Medical/Health Care, Treatment, and Medical Staff.

I. INTRODUCTION

The Security measure is one of primary concern and in this busy and competitive world, the human is not able to find ways to provide security to his confidential belongings manually.

He keep finding an alternative way which can provide a full fledged security as well as atomized way of identification. In the present scenario of network society, where individuals can easily access their information at anytime and from anywhere, people are also faced with the risk that others can easily access the same information at anytime and from anywhere. Because of this risk, the personal identification technology, which can distinguish between registered legitimate users and imposters, is now generating interest.

Generally for identifying people we are yet using the traditional patterns like passwords, identification cards and PIN verification techniques are being used but with these techniques there are a lot of disadvantages also like that the passwords could be hacked and a card may be stolen by anyone or may be lost.

In the present time the most secured system is fingerprint recognition because a fingerprint of one person never matches the other person. Biometrics studies commonly include fingerprint, face, iris, voice, signature, and hand geometry recognition and verification and a lot of more techniques. Many other modalities are in various stages of development and assessment for future trends of identification.

Among these available biometric traits fingerprint proves to be one of the best traits providing good mismatch ratio, high accuracy in terms of security and also reliable.

BACKGROUND

In this work, by us, a lot of attempts are made for providing security for all domiciles. Up to date, complete security is not discovered with the traditional identification system .

Some ways to secure your Data

We all are very concerned for the issue of data security. A lot of data protection and security model are available in the market which are including multiple perimeter which are helpful into counter applicable threats.

Multiple layers of defense from threats can isolate and protect data should one of the defense perimeters be compromised from internal or external threats. It includes both logical (authorization, authentication, encryption and passwords) and physical (restricted access and locks on server, storage and networking cabinets) security.

Physical security includes maintaining a low profile.
Logical security includes securing your networks with firewalls, running anti spyware and virus-detection programs on servers and network-addressed storage systems.

No storage security strategy would be complete without making sure that applications, databases, file systems and server operating systems are secure to prevent unauthorized or disruptive access to your stored data. Implement storage system based volume or logical unit number mapping and masking as a last line of defense for your stored data.

Some storage and networking tools will encourage you as a user to change management passwords at initial installation. Due diligence is to say the obvious - change default passwords at installation and on an ongoing basis. Likewise, restrict access to management tools to those who need it.

As an admin you must know who has physical access to fixed and removable data-storage media and devices.

Leverage access logs as well as perform background checks of contractor and third-party personnel who will be handling your data and media.

Identify where weak links are in your data-movement processes and correct those deficiencies. Data-discovery tools can be used to identify sensitive data that may not be adequately protected.

If you are currently moving data electronically to avoid losing tapes or are planning to, then make sure data being transmitted over a public or private network is safe and secure. Some techniques to protect data while in-flight include encryption, virtual private networks and the IPSec protocol.

Some important ways to save your work and data are as under -

1. Establish strong passwords
Implementing strong passwords is the easiest thing you can do to strengthen your security. By crafting a hard-to-crack password: use a combination of capital and lower-case letters, numbers and symbols and make it 8 to 12 characters long.

2. Put up a strong firewall
In order to have a properly protected network, "firewalls are a must". A firewall protects your network by controlling internet traffic coming into and flowing out of your business. They're pretty standard across the board.

3. Install antivirus protection
Antivirus and anti-malware software are essentials in your system and must be updated with latest definition for online security weapons, as well.

4. Update your programs regularly
Making sure your computer is "properly patched and updated" is a necessary step towards being fully protected; there's little point in installing all this great software if you're not going to maintain it right.
Frequently updating your programs keeps you up-to-date on any recent issues or holes that programmers have fixed.

5. Secure your LAPTOP’s/TABLET’s/Mobile’s
Because of their portable in nature, these devices are at a higher risk of being lost or stolen than average company desktops. It's important to take some extra steps to make sure that your sensitive data is protected.

6. Secure your mobile phones
Our smartphones hold so much data these days that you should consider them almost as valuable as company computers - and they're much more easily lost or stolen. As such, securing them is another must.

7. Backup regularly
Scheduling regular backups to an external hard drive, or in the cloud, is a painless way to ensure that all your data is stored safely.

The general rule of thumb for backups :-
Servers should have a complete backup weekly, and incremental backups every night; personal computers should also be backed up completely every week.

8. Monitor diligently
The data-leakage prevention software, which is set up at key network touchpoints to look for specific information coming out of your internal network. It can be configured to look for credit card numbers, pieces of code, or any bits of information relevant to your business that would indicate a breach.

9. Be careful with e-mail, IM and surfing the Web
It's not uncommon for a unsuspecting employee to click on a link or download an attachment that they believe is harmless - only to discover they've been infected with a nasty virus, or worse.

Never click on a link that you weren't expecting or you don't know the origination of in an e-mail or IM.

You should take every "warning box" that appears on screen seriously and understand that every new piece of software comes with its own set of security vulnerabilities.

10. Educate your employees
Teaching your employees about safe online habits and proactive defense is crucial.

Prevention is the best approach to handling your data security.

Make sure your employees understand how important your company's data is, and all the measures they can take to protect it.

11. Manage Who Has Access
First, as an organization, take inventory of what data every employee may or may not have access to. Determine which employees still need access and which do not in an effort to limit the amount of data access by employees/admins to a small, manageable number. In addition, have your admins determine which type of access each department/employee needs.
12. Know And Protect Your Most Important Data
As a company, it's important to take the time to identify what you consider the most valuable data and work on protecting that first.

13. Develop A Data Security Plan/Policy
It's important to have a data security plan in place when hacks and breaches occur and a plan that determines which employees need and have access to data, as mentioned above. Thus, these sorts of policies can keep employees in line and organized.

14. Develop Stronger Passwords Throughout Your Organization
Employees need to have stronger and more complicated passwords. Work to help employees develop passwords that are a combination of capital letters, numbers and special characters that will make it much harder for hackers to crack.

A good rule of thumb when creating a new password is to have it be at least 12 characters and to not include a combination of dictionary words, such as "green desk." All and all, passwords should be unique to employees and difficult for computers to guess.

15. Regularly Backup Data
It's important to backup your data on a regular basis. In addition to hacks, loss of data is a serious issue, and organizations need to be prepared for the unexpected. As a business, get in the habit of either automatically or manually backing up data on a weekly or daily basis.

Webs are things that spiders weave with the aim of capturing prey. And if you want a metaphor for thinking about where we are now with networked technology, here's one to think about.

Everything that you do with modern communications equipment leaves a digital trail. And this trail is followed assiduously not just by giant corporations, but also by governments and their security services.

i. Password Authentication:
Next level of Security used password as an authenticating tool. This system stores password of authenticated users for the purpose of validation. System using password authentication provides

considerable security to the users as it acts as a secret of authorized users. This system also have a pitfall that password can be acquired by unauthorized user by continuously trying all the possible combinations. This is also one among the hundreds of attempt made for providing security.

ii. Authentication by RFID card:

Next level of technological development for providing security was authentication by RFID card. This system enriched the level of security. Access is granted only for the user whose RFID code matches with the authorized code. This system also have disadvantage of duplication of RFID card and anyone who possess this card can unlock the door.

II. PROPOSED METHODOLOGY

Our proposed system overcomes all the security problems in existing system and provides high security and efficiency. This is a perfect/optimal solution for saving/protecting one from the hassle of stolen/lost key or an unauthorized entry. Fingerprint is a boon solution for these problems which provides high level of recognition accuracy.

The skin on our finger, palms and soles exhibits a flow like pattern of ridges called friction ridges. The pattern of friction ridges on each finger is unique and immutable. This makes fingerprint a unique identification for everyone. Fingerprint patient identification incorporates the proven technology. Fingerprint scanner scans the fingerprints of users and used for ensuring authentication. Fingerprint scanning is more accurate and cost effective method and duplication is virtually impossible. A Fingerprint recognition system can easily perform verification. In verification, the system compares an input fingerprint to the enrolled fingerprint of a specific user to determine if they are from the same finger. Now the security of our home/office is literally in our hands or rather on our fingertips.

PROPOSED MODEL OF THE SYSTEM RELATED DISCUSSION

When fingerprint module is interfaced to the device, it will be in user mode. In this mode, stored images will be verified with the scanned images. When coming to our application the images of the patient's fingerprint that are registered in the system and their unique ID is already available in the system (they are registered in the module with a unique id). To prove that the persons are our registered patients, they need to scan their fingerprint images. The scanner is interfaced to device, this controller will be controlling the scanning process.
If an unauthorized person tries to scan his fingerprint image then an indication will be given by a buzzer which is interfaced to the controller. The current user instead of him/her can make a new person as the admin by new registration process and the old user's fingerprint image will be deleted from the system to make the new person as admin to control and manage the database.

III. EXPERIMENTAL RESULTS

Step 1: When power is supplied to the device, the initial displays on the LCD shows the instruction for the patients .
Step 2: When the fingerprint is mismatched.
Step 3: When the persons fingerprint matches, display on LCD.
Step 4: After work has been completed, it goes back to step 1.

IV. CONCLUSIONS

The main advantages of using this system are:

- ✓ Easy to use and requires no special training or
- ✓ equipment.
- ✓ Fingerprint is unique for every person it cannot
- ✓ be imitated or fabricated .It is not same in the case
- ✓ of twins also.
- ✓ High accuracy in terms of security.
- ✓ No manual errors.
- ✓ No false intrusions

V. REFERENCES

[1]. Shelly Batra, Sandeep Ahuja, Abhishek Sinha, and Nicholas Gordon, 2012 in Proceedings of M4D 2012 28-29 February 2012 New Delhi, India, "eCompliance : Enhancing Tuberculosis Treatment with Biometric and Mobile Technology", pp 35-40, 2012

[2]. Michael Paik, Navkar Samdaria, Aakar Gupta, Julie Weber, Nupur Bhatnagar, Shelly Batra, Manish Bharadwaj, and William Thies, 2010 , in

Proceeding NSDR'10 Proceedings of the 4th ACM Workshop on Networked Systems for Developing Regions, Article No. 4, "A Biometric Attendance Terminal and its Application to Health Programs in India", pp 1-6, 2010

[3]. Nupur Bhatnagar, Abhishek Sinha, Navkar Samdaria, Aakar Gupta, Shelly Batra, Manish Bhardwaj, and William Thies, 2012 in Springer, "Biometric Monitoring as a Persuasive Technology : Ensuring Patients Visit Health Centers in India's Slums", pp. 169-180, 2012

[4]. Seema Rao, and Prof. K.J.Satoa, 2013, in International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, Issue 4, "An Attendance Monitoring System Using Biometrics Authentication", pp. 379 – 383, April 2013

[5]. O. Shoewu, and O.A.Idowu, 2012, in The Pacific Journal of Science and Technology, Vol 13, No. 1, "Development of Attendance Management System using Biometrics", pp. 300-307, May 2012 (Spring)

[6]. Tiwalade O. Majekodunmi, and Francis E. Idachaba, 2011, in Proceedings of the World Congress of Engineering WCE – 2011, July 6-8, 2011, London, U.K., Vol II, "A Review of the Fingerprint, Speaker Recognition, Face Recognition and Iris Recognition Based Biometric Identification Technologies", 2011

[7]. Michael H. Indico, Luisa M. Lanciso, and Ana L. Vargas, 2014 , in International Journal of Scientific and Research Publications, Vol 4, Issue 1, "Mobile Monitoring and Inquiry System Using Fingerprint Biometrics and SMS Technology", pp. 1-6, January 2014

[8]. Pallavi Verma, and Namit Gupta, 2013, in International Journal of Science and Research (IJSR), Vol 2, Issue 10, "Fingerprint Based Student Attendance System Using GSM", pp. 128 – 131, October 2013

[9]. Hemangi Kulkarni, Aniket Yadav, Darpan Shah, Pratik Bhandari, and Saumya Mahapatra, 2012, in Int. J. Computer Technology & Applications, Vol 3 (2), "Unique ID Management", pp. 520-524, 2012

[10]. K. Jaikumar, M. Santhosh Kumar, S. Rajkumar, and A. Sakthivel, 2015 , in International Journal of Research in Engineering and Technology, Vol 4, Issue 2, "Fingerprint Based Student Attendance System with SMS Alert to Parents", pp. 293-297, Feb 2015

[11]. Smita S. Mudholkar, Pradnya M. Shende, Milind V. Sarode, "Biometrics Authentication Technique for Intrusion Detection Systems Using fingerprint Recognition", in International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol 2, No. 1, pp. 57-65, February 2012

[12]. Gowthami P, and Dr. P. Sathishkumar, 2016 , in International Journal of Innovative Research in Advanced Engineering (IJIRAE), Vol 3, Issue 4, "An Andriod Based Patient Monitoring System", pp. 54-57, April 2016

[13]. Mohd Idzwan, Mohd Salleh, Mohamad Rahimi, Mohamad Rosman, Raja Abdullah, and Raja Yaacob, 2011, in International Conference on Computer Applications and Industrial Electronics (ICCAIE 2011) - IEEE, "Biometric Authentication for Securing Life Cycle Management of Electronic Patient Records", pp. 602-606, 2011

[14]. Abhishek Sinha, Shashank Batra, Dr. Shelly Batra, and Sandeep Ahuja, 2014, in Indian Journal of Medical Informatics – official Organ of Indian Association for Medical Informatics (IAMI), "Using Biometrics to Turn the Tap Off of Multi Drug Resistant TB (MDR TB)", pp.38-41, 2014

[15]. Adebayo Omotosho, Omotanwa Adegbola, Barakat Adelakin, Adeyemi Adelakun, and Justice Emuoyibofarhe, 2014 , in Journal of Biology, Agriculture and Healthcare, Vol 4, No. 18, "Exploiting Multimodal Biometrics in E-Privacy Scheme for Electronic Health Records", pp. 22-33, 2014

[16]. Shirish Joshi, 2016, in International Journal for Scientific Research & Development (IJSRD), Vol 3, Issue 11, "BIOMETRICS : Selecting the Best Solution", pp. 206-208, 2016

[17]. Jayant V. Kulkarni, Bhushan D. Patil, and Raghunath S. Holambe, 2006 , in Pattern Recognition Society : Published by Elsevier Ltd., "Orientation feature for fingerprint matching", pp. 1551-1554, 2006

[18]. Mangesh Raut, Sheetal Kokate, Sandeep Shinde, Sushant Karpe, and Mr. Sachin Barahate, 2015 , in International Journal for Scientific Research & Development (IJSRD), Vol 3, Issue 1, "Virtual

Biometric Fingerprint Attendance System", pp. 511-513, 2015

[19]. Nitin Sambharwal, and Dr. Chander Kant, 2015, in International Journal for Scientific Research & Development (IJSRD), Vol 3, Issue 2, "Biometrics Fingerprint Sensors : An Introduction", pp. 1019-1025, 2015

[20]. Divya K V, Akansha Pandey, Manoj Sharma, Meghashrita Kashyap, and Divya Kumari, 2016, in International Journal for Scientific Research & Development (IJSRD), Vol 3, Issue 12, "A Survey on Biometric Authentication for Accident Victims During Emergencies" pp. 992-994, 2016

[21]. Chirag Singh Sisodia, Aparajiit Shrivastava, 2015, in International Journal for Scientific Research & Development (IJSRD), Vol 3, Issue 9, "A Survey on Network and Security Authentication using Biometrics", pp. 236-241, 2015

[22]. Keerti Arse, 2014, in International Journal for Scientific Research & Development (IJSRD), Vol 2, Issue 9, "A Survey of Automated Biometric Authentication Techniques", pp. 906-908, 2014

[23]. Anjana P, Betty P, 2015, in International Journal for Scientific Research & Development (IJSRD), Vol 2, Issue 12, "An Elaborated View on Biometric Template Protection", pp. 490-495, 2015

[24]. Koichi Ito, Ayumi Morita, Takafumi Aoki, Tatsuo Higuchi, Hiroshi Nakajima, and Koji Kobayashi, 2005, in ICIP – IEEE International Conference, "A Fingerprint Recognition Algorithm Using Phase-Based Image Matching for Low-Quality Fingerprints", pp. II-33 – II-36, 2005

[25]. Rubal Jain, Dr. Chander Kant, 2015, in International Journal for Scientific Research & Development (IJSRD), Vol 3, Issue 2, "Attacks on Biometric Systems : An Overview", pp. 1090-1094, 2015

[26]. Eshraf El-Sisi, 2011, in The International Arab Journal of Information Technology, Vol 8, No. 4, "Design and Implementation Biometric Access Control System Using Fingerprint for Restricted Area Based on Gabor Filter", pp. 355-363, October 2011

[27]. Adewole K.S., Abdulsalam S.O., Babatund e R.S., Shittu T.M., and Oloyede M.O., 2014, in Computer Engineering and Intelligent Systems, Vol 5, No. 2, "Development of Fingerprint Biometric Attendance System for Non-Academic Staff in a Tertiary Institution", pp. 62-70, 2014

[28]. Norshidah Katiran, Helmy Abdul Wahab, Jamal Rasyid, and Abdul Rahman, 2010 , " in Proceedings of EnCon2010 3rd Engineering Conference on Advancement in Mechanical and Manufacturin g for Sustainable Environment April 14-16, 2010, Kuching, Sarawak, Malaysia, "Development of Attendance System using Biometric Fingerprint Identification pp. 1-4, 2010

[29]. Hemlata Patel, and Pallavi Asrodia, 2012, in International Journla of Electrical, Electronics and Computer Engineering, vol1, No. 1, "Employee Attendance Management System Using Fingerprint Recognition", pp. 37-40, 2012

[30]. Oloyede Muhtahir O., Adedoyin Adeyinka O., and Adewole Kayode S., 2013, in International Journal of Applied Information Systems (IJAIS), Vol 5, No. 3, "Fingerprint Biometric Authentication for Enhancing Staff Attendance System", pp. 19-24, February 2013

[31]. Devendra Kumar Yadav, Sumit Singh, Prof. Shashank Pujari, and Pragyan Mishra, 2015, in International Journal of Advanced Research in Electrical , Electronics and Instrumentation Engineering, Vol 4, Issue 6, "Fingerprint Based Attendance System Using Microcontroller and LabView", pp. 5111-5121, June 2015

[32]. Ravi Subban, and Dattatreya P. Mankame, 2013, in Lecture Notes on Software Engineering, Vol 1, No. 2, "A Study of Biometric Approach Using Fingerprint Recognition", pp. 209-213, May 2013