March 2023

Biometric System and Applications

Edited By | Dr. Sandhya Dass

CIIR RESEARCH PUBLICATIONS

Contents

Preface

A biometric device serves as an authentication and security identification tool. These gadgets rely on automated techniques to confirm or identify a real person's identification based on a physical or behavioural trait. These traits include voice recognition, iris, face, and fingerprint recognition. Voting's main purpose is to provide citizens the chance to exercise their right to freely express their opinions on certain matters, laws, citizen initiatives, constitutional changes, recalls, and/or candidates for office. Technology is increasingly being utilised to help voters cast their ballots. Nearly all voting systems worldwide have the following procedures to enable the use of this right: identification and verification of voters, voting and keeping track of voted ballots, vote tallying, election results publication.

Voter identification is needed twice throughout the election process: first, at voter registration to secure the right to vote; and second, when voting to enable a citizen to exercise that right by ensuring that the individual meets all conditions to vote. (authentication). Historical objects and ancient archaeological artefacts have been found to still contain a lot of fingerprints on them. Significant advancements in fingerprinting and identification have been achieved since this was found. A thorough description of the anatomical structures of fingerprints was written in 1788. Afterward, in 1823, fingerprints started to be categorised into nine groups (Handbook), and by the 19th century, Sir Francis Galton had developed analytical techniques for matching fingerprints. With the advancement of the criminal justice system, a need for some visually distinguishable characteristic to be used to uniquely identify offenders. In 1901, Richard Edward Henry of Scotland Yard first used fingerprinting, and because to its effectiveness, its application in the area of law enforcement has since risen.

Since its inception, the discipline of biometrics has grown to include several physical identifying methods. Even Nevertheless, law enforcement continues to favour the human fingerprint as a biometric identification tool. These ideas about human identity have sparked the creation of fingerprint scanners, which allow for the fast identification of people and the granting of access rights. These gadgets' primary function is to go at a person's fingerprint information and compare it to a database of other fingerprints. Almost everyone in the world is born with a fingerprint, which is distinctive and completely identifies us from the other 6.5 billion individuals that live on our planet. The fingerprint has proved to be a very valuable component of biometric security as a result of this. This fact also explains why fingerprint scanners are beneficial in the first place. But this is by no means the sole purpose for them.

The fact that fingerprint scanners provide a rapid, simple, effective, and secure method of authentication for someone with the right access credentials is another significant factor in their utilization. Today, identification may be completed quickly and quite accurately. The usage of automated fingerprint identification systems (AFIS) that record, store, search, match, and identify fingerprints is growing quickly as a consequence. A microcontroller, various peripherals, and AFIS may be used to create an embedded system that is a complete electronic voting machine with a fingerprint print identification system.

Dr. Sandhya Dass
Editor

CHAPTER 1

INTRODUCTION TO SECURE EVM

Mr. Vijaya Krishna
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- vijayakrishna@presidencyuniversity.in

Each citizen has the right to vote and choose their representative. India is a democratic country, and each individual has the freedom to express their opinions through voting. By supporting a candidate in the future election, citizens will also have the opportunity to alter the ruling party. Voting is not only done to choose the government's representatives; it is also done to choose the heads of institutions like banks, colleges, and societies. Using biometrics, it is possible to identify someone based on their physical characteristics. The most common biometrics used to identify a person include their fingerprint, iris, face, voice, etc. The first of biometrics' two main uses is one-to-one matching, while the second is one-too-many matchings. The biometric sample is compared to the previously stored samples in one-to-many matching. It compares with the previously saved sample in one-to-one matching. Faster security and more practical user verification are the outcomes of the biometric technique. Password security is inferior to biometric security. Because each person's fingerprint is distinct, they can be used as a mark of signature, verification, and authenticity [1].

The biometric that is utilised in this research is the fingerprint. Every person's fingerprint will be unique. In this project, the user's fingerprint is utilised to authenticate him or her and to enable voting based on the image of his or her fingerprint. Three categories of fingerprint matching exist: correlation-based matching, detail-based matching, and pattern-based (or image-based) matching. When two fingerprint pictures are overlapped during correlation-based matching. Consequently, for varied alignments, the correlation between corresponding pixels is determined. The minutiae from the two fingerprints are collected and stored as a set in a two-dimensional plane during minutiae-based matching [2]. Finding the alignment between the template and the input minutiae sets that yields the greatest number of minutiae pairings is the matching approach. The pattern-based (or image-based) matching method compares the candidate's fingerprint to a template that has been stored. The photos must be aligned in the same orientation for this to work. In order to accomplish this, the algorithm locates and centres on a central spot inside the fingerprint image. The sort, size, and orientation of the patterns within the aligned fingerprint image are contained in the template in a pattern-based algorithm. Digital data storage is used almost universally. Most chores are completed online as part of the creation of a digital India. Online voting enables voters to cast their ballots from anywhere in the world. One method for facilitating online voting is thing talk. Finding results online speeds up the process [3].

Since everything was done manually, it will take longer to announce the winner. In order to avoid repeat voting, each voter will be marked with ink on their finger after casting their ballot. Until the development of electronic voting machines, this method was used. All people of a nation like India have the right to vote. In India, the people have the right to choose who will serve as their leader

ISBN 978-81-962236-1-8 March 2023

for the foreseeable future. If the populace is dissatisfied with that leader, they will have the opportunity to elect a new one in the subsequent election. But numerous errors are being made, which have no bearing on the right outcome. It takes more time and is less secure with the current system. The voter must cast their ballot at the appropriate centre. Additionally, postal voting is not very secure. In this study, the right strategies are used to achieve the research's ultimate goal, which is to create a system that stops electoral malpractices from happening. Each candidate who is qualified to vote has their fingerprint entered and saved in the system. The biometric identification system that is used is fingerprint [4]. The stored database is matched with the stored fingerprint and the stored Aadhar number. It offers voter identification proof. Additionally, it looks to see if a voter has cast several ballots in a single election. The outcome will likewise be kept in the cloud. Voting can be done online from anywhere in the globe because it uses the cloud. A warning will be generated if the confirmed voter attempts to vote more than once. Here, a buzzer sound is being used to signal that an error has occurred [5].

Elections have a significant role in the administration of India. It is a process for choosing a candidate to lead the government. This study provides information on secure voting procedures and the biometric election process. People had faith in the electronic voting system since it produces accurate results because choosing a candidate for the government was crucial. Therefore, the EVM needs to be built to be extremely safe and secure. Voting machines, ballots, punch cards, e-voting, block chains, microcontrollers, network security, i-voting, online voting, and GSM modules are just a few of the technologies used in elections today. However, there are still a lot of difficulties with EVM today. As a result, this research describes a suggested technique for a protected EVM that uses facial recognition biometrics and an IOT-enabled ID card. Voters are unable to repeat their votes thanks to biometric facial recognition technology. Everyone had an own ID number called an Aadhar. For transmitting findings promptly, IOT is helpful.

According to data from Science Direct, the use of EVM technology in the scientific community has increased over the past 20 years. Democracy was founded on elections, which are characterised by a set of regulations that must be adhered to both while voting and after results are announced. There were several voting methods, including paper ballots, punch cards, and optical mark sense ballots, that may select a single winner, such as the prime minister, or a number of victors, such as members of the parliament or boards of directors. An electronic voting mechanism that uses human biometrics is the fingerprint voting system. Voters in India selected their own future, therefore we introduced a new voting system to raise the country's living standards. Currently, India's voting system counts votes manually or via electronic voting machines (EVMs), which may lead to discrepancies or double counting [6]

The likelihood of duplication will be reduced as a result of EVM. Sometimes voters are coerced and encouraged to support certain political parties, which results in erroneous voting and skews the outcome of the election. Utilizing this approach will provide for control, authenticity, and precision. One important step in the election process is the counting of the votes. Vote theft must not occur, and the election process must be trustworthy and transparent in order for voters to have confidence in it. Only those who pre-registered will be mentioned and given the opportunity to vote. To store the votes, electronic voting machines are utilized. There were two different ways to

cast a vote: absentee voting and presence voting. Today, data is retrieved, saved, and processed as digital information. At the moment of voting, a voter's fingerprint is scanned using a fingerprint sensor used in this process. Additionally, we use a national identity card number that is specific to each individual, preventing any vote fraud. The user will be given a specific spot to enter his or her name, Aadhar card number, and finger impression; the aforementioned information will be sorted based on a district-specific government database. Our system has several levels of authenticity. For example, a voter will be recognized using all of their identity-related information, including their name, gender, nationality, fingerprints, and Aadhar numbers, before being allowed to cast their ballot [7].

Bibliography:

[1] S. Srinivas, B. Ashwin Kumar, and R. Srishylam, "Blockchain-based E-Voting System using Proof of Voting (PoV) Consensus Algorithm," *CVR J. Sci. Technol.*, 2020, doi: 10.32377/cvrjst1819.

[2] S. Mariappan, J. Rajendran, H. Ramiah, P. I. Mak, J. Yin, and R. P. Martins, "An 800 MHz-to-3.3 GHz 20-MHz Channel Bandwidth WPD CMOS Power Amplifier for Multiband Uplink Radio Transceivers," *IEEE Trans. Circuits Syst. II Express Briefs*, 2021, doi: 10.1109/TCSII.2020.3035758.

[3] K. Srikrishnaswetha, S. Kumar, and D. Ghai, "Secured Electronic Voting Machine Using Biometric Technique with Unique Identity Number and IOT," in *Lecture Notes in Networks and Systems*, 2020. doi: 10.1007/978-981-15-3172-9_31.

[4] D. D. Gaikwad, A. N. Hambir, hantanu S. Chavan, G. K. Khedkar, and D. S. V. Athawale, "Real Estate Land Transaction System Using Blockchain," *Int. J. Res. Appl. Sci. Eng. Technol.*, 2022, doi: 10.22214/ijraset.2022.40633.

[5] T. Shanthi, R. Saranya, S. Selvasridevi, K. Srinandini, and S. Sripriya, "Voting system based on finger print and face recognition," *Int. J. Pharm. Res.*, 2020, doi: 10.31838/ijpr/2020.12.01.233.

[6] A. Sreeram, L. Kiran Kumar, J. Natarajan, and C. Ashwini, "The New Age of Democracy—Voting System," *J. Comput. Theor. Nanosci.*, 2020, doi: 10.1166/jctn.2020.8422.

[7] B. Madhuri, M. G. Adarsha, K. R. Pradhyumna, and B. M. Prajwal, "Secured Smart Voting System using Aadhar," 2018. doi: 10.1109/ICECIT.2017.8453308.

CHAPTER 2

WORKING PRINCIPLE OF ELECTRONIC VOTING MACHINES

Mr. Vijaya Krishna
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- vijayakrishna@presidencyuniversity.in

The improvement of the security of electronic voting machines is the central goal that unites all the publications under consideration. In all the cases given here, biometrics, in particular fingerprint sensing, has been employed as the authenticating feature. The fundamental block diagram is displayed in accordance with the examined publications. Above was shown the generalized block diagram [1]. A number of changes have been made to this, such as connecting the various blocks or adding extra equipment, to improve security and simplify the voting procedure for the voters. The following are the primary voting phases on which the various reviewed journals have concentrated:

Registration: Prior to any polling, registration is the first step. Since there are voting systems everywhere, this section addresses the registering of the biometric authentication characteristics, assuming that national citizen registration has previously been completed. Before the first elections, when voters had to identify or enroll their fingerprints, a database for recording fingerprint patterns had been constructed. A few additional cases have included the use of a government database, specifically the Aadhar card database. A few publications have also used additional biometrics, such as speech recognition, iris scanning, and finger vein authentication, for security purposes. Voters must be registered in practically every country in order to be allowed to cast a ballot [2]. Voter registration is to guarantee that everyone who is eligible to vote may do so, to stop ineligible people from casting ballots, and to prevent the same person from casting repeated ballots. Making sure that all eligible voters may exercise their right to vote depends in large part on the accuracy of the voter registration list. As may easily occur in post-conflict nations and elsewhere if processes are not carefully developed and implemented, registration methods should be created to guarantee that women are not inadvertently disadvantaged or disenfranchised. All individuals who have achieved the requisite age have the right to vote therefore that is the foundation upon which voter registration should be based. According to United Nations guidelines, no one should be prohibited from registering to vote because of their race, sex, language, or religion. It is generally agreed upon that voting should not be subject to poll taxes or criteria regarding literacy, income, or education. But there are reasonable grounds for restricting voting based on citizenship, mental competence, or a criminal history. The compiled, certified listings of everyone eligible to vote are known as voter registrations. Contrarily, the phrase "voter list" is sometimes used to refer to a list of people who have registered to vote in a certain constituency for a specific election [3].

Identification: Choosing a legitimate identity is the next important election-related step. A few of the older journals have created their models based on the national identity documents that are

ISBN 978-81-962236-1-8 March 2023

currently in use. Indian periodicals have suggested adopting the Aadhar number as a legitimate form of identification for voters. RFID prototypes haven't been used much to replace this. The use of QR code scanning has also been documented. Voter identification is necessary at two stages of the electoral process: first, during registration to establish the right to vote; and second, when voting to enable a citizen to exercise their right to vote by confirming that the individual fulfils all conditions. The majority of nations conduct voter identification and identity verification manually, however some have adopted and other nations are experimenting with a computerized or at least semi-automatic technique to confirm voters' identities and their eligibility to vote. This suggests that there is a voter database kept electronically. Actually, the technologies utilized to create the voter register have an impact on the technology used for voter identification at election time [4].

Processor: A variety of processors have been utilized to make the systems more technologically advanced and to broaden the possibilities for future upgrades. Using Arduino, implementations have been made. ARM processors in a variety of variants and other microcontrollers have also been utilized extensively. The Android platform has also seen attempts at exploitation.

Voting process: The actual Election Day, when the proposed ideas are put to the test, serves as the primary and decisive voting phase. According to the established procedure, voters must be present in the voting booth for their identities to be verified before casting their ballots. In a democracy, the process of voting is vital. It is an opportunity for a nation's residents to have a voice in the individuals who represent them or a matter that affects them. One of the duties of American citizens is to vote and participate in elections in an informed manner. The voting procedure is pretty simple in the United States. An eligible voter first registers, researches the contenders and issues, locates their polling place, and then casts their vote on Election Day [5].

This technique extends the current methodology with more security by using fingerprint authentication and programming many modes. Although the majority of journals still allow in-person voting, just a small number have suggested an online voting option, meaning that physical presence at a polling place is not required. In a few publications, the idea of casting an online ballot while in the voting booth has also been discussed. Additionally, the Raspberry Pi-based distributed server approach has been used. The major goal of online voting is to provide a safe and trustworthy online voting application while also taking into account the new generation of people who are above 18 years old. All of the citizens' information will be kept in a single, centralized database. Details about the individual utilizing our system will be checked against database data and validated. Voters won't be permitted to cast ballots if the database's data and their personal information don't match. The system will check for double voting if the details match. No more votes may be cast by a voter who has already cast one ballot [6].

Bibliography:

[1] S. Chauhan, M. Jaiswal, and A. K. Kar, “The acceptance of electronic voting machines in India: A UTAUT approach,” *Electron. Gov.*, 2018, doi: 10.1504/EG.2018.093427.

[2] K. Gurucharan, B. Kiranmai, S. S. Kiran, and M. R. Kumar, “Xilinx based electronic voting machine,” *Int. J. Eng. Adv. Technol.*, 2019, doi: 10.35940/ijeat.A1484.109119.

[3] M. M. Sarker, M. A. I. Shah, T. M. N. U. Akhund, and M. S. Uddin, “An Approach of

Automated Electronic Voting Management System for Bangladesh Using Biometric Fingerprint," *Int. J. Adv. Eng. Res. Sci.*, 2016, doi: 10.22161/ijaers/3.11.11.

[4] S. Agarwal, A. Haider, A. Jamwal, P. Dev, and R. Chandel, "Biometric Based Secured Remote Electronic Voting System," in *2020 7th International Conference on Smart Structures and Systems (ICSSS)*, Jul. 2020, pp. 1–5. doi: 10.1109/ICSSS49621.2020.9202212.

[5] T. Shanthi, R. Saranya, S. Selvasridevi, K. Srinandini, and S. Sripriya, "Voting system based on finger print and face recognition," *Int. J. Pharm. Res.*, 2020, doi: 10.31838/ijpr/2020.12.01.233.

[6] B. Madhuri, M. G. Adarsha, K. R. Pradhyumna, and B. M. Prajwal, "Secured Smart Voting System using Aadhar," 2018. doi: 10.1109/ICECIT.2017.8453308.

CHAPTER 3

FINGERPRINT SENSOR

Mr. Vijaya Krishna
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- vijayakrishna@presidencyuniversity.in

The optical fingerprint sensor, high-speed DSP processor, high-performance fingerprint synchronization algorithm, high-capacity FLASH chips, and other hardware and software components make up the fingerprint module. It has a simple structure, stable performance, and features functions for fingerprint entry, image processing, fingerprint matching, searching, and template storage. The fingerprint module has two interfaces: TTL UART and USB 2.0. USB 2.0 interfaces are frequently connected to computers; the RS232 interface may be a TTL level; the default baud rate is 57600. This rate can be changed; ask a communication protocol. Microcontrollers, such as ARM, DSP, and other serial devices with a correlation are frequently connected directly [1].

Fingerprint Voting System: The Fingerprint Based Voting is a program that recognizes users based on the patterns on their fingers. Each person has a unique finger pattern, making it simple to identify a voter. The voting process uses the voter's fingerprint. The user is uniquely identified by their fingerprint. Every human being has a unique set of minute traits on their finger prints. Voters' fingerprints are used as identification. A voter may only cast one ballot for a candidate; the system forbids casting further ballots. The system will let the administrator upload each candidate's name and picture who has been put forward for the election. Only candidates who have been nominated may have their names and photos added by the admin. Admin will check the voter before registering the voter's name. Admin will register the voter after authenticating the user by checking the user's identification documentation. After the election is over, the admin will immediately remove the amount of candidates they added to the system. The election's finish date must be added by the administrator. The user may log in and cast their vote for the candidates who have been nominated once they have received their user ID and password from the administrator. The technology will let the user select just one candidate to vote for. The technology will let the user cast one vote in a certain election. Whenever the new election is declared, the admin has the option to add as many candidates as desired. Using the election id, the administrator may examine the election results. Users may watch the election results as well [2].

The biometric that is utilized in this research is the fingerprint. Every person's fingerprint will be unique. In this project, the user's fingerprint is utilised to authenticate him or her and to enable voting based on the picture of his or her fingerprint. Three categories of fingerprint matching exist: pattern-based (or image-based), minutiae-based, and correlation-based matching. In correlation-based matching, two fingerprint pictures are overlaid, and various alignments are performed to determine the correlation between corresponding pixels. The minutiae from the two fingerprints are collected and stored as a set in a two-dimensional plane during minutiae-based matching. Determining the alignment between both the template and the input minutiae sets that yields the greatest number of minutiae pairings is the matching approach. The pattern-based (or image-based)

ISBN 978-81-962236-1-8 March 2023

matching approach compares the candidate's fingerprint to a template that has been saved. The photos must be aligned in the same orientation for this to work. In order to do this, the algorithm locates and concentrates on a central spot inside the fingerprint picture. The kind, size, and orientation of the patterns inside the aligned fingerprint picture are contained in the template in a pattern-based method. Digital data storage is used almost everywhere. Most chores are completed online as part of the creation of a digital India. Online voting enables voters to cast their ballots from anywhere in the globe. One method for facilitating online voting is Thing speak. Finding results online speeds up the process [3].

Voting used to include stamping a piece of paper with a vote stamp for the appropriate candidate, then putting it into a ballot box. The candidate who received the most votes will be declared the victor after counting each vote in each ballot box and adding up all the votes cast for each contender. Since everything was done manually, it will take longer to announce the winner. In order to avoid repeat voting, each voter will be marked with ink on their finger after casting their ballot. Until the development of electronic voting machines, this approach was used. Every citizen of a nation like India has the right to vote. In India, the people have the right to choose who will serve as their leader for the foreseeable future [4]. If the populace is dissatisfied with that leader, they will have the opportunity to elect a new one in the subsequent election. But numerous errors are being made, which have no bearing on the right outcome. It takes more time and is less secure with the current system. The voter must cast their ballot at the appropriate centre. Additionally, postal voting is not very secure. In this study, the right strategies are used to achieve the research's ultimate goal, which is to create a system that stops electoral malpractices from happening [5].

Each candidate who is qualified to vote has their fingerprint entered and kept in the system. The biometric identification system that is employed is fingerprint. The saved database is matched with the stored fingerprint and the stored Aadhar number. It offers voter identification proof. Additionally, it looks to see if a voter has cast several ballots in a single election. The outcome will likewise be kept in the cloud. Voting can be done online from anywhere in the globe since it uses the cloud. A warning will be generated if the confirmed voter attempts to vote more than once. In this case, a buzzer sound is being used to signal a misconduct [6].

Advantages

- The voting process will not let a voter select more than two candidates.
- The technology will let a person cast a single ballot for a certain election.
- The user will be uniquely identifiable by the system when it authenticates him using his fingerprint.

Disadvantages

- The voter may not be recognized by the system if their finger pattern has been destroyed or has been severed in any way.

Bibliography:

[1] X. Jiang *et al.*, “Monolithic ultrasound fingerprint sensor,” *Microsystems Nanoeng.*, 2017, doi: 10.1038/micronano.2017.59.

[2] X. Jiang *et al.*, “Monolithic ultrasound fingerprint sensor,” *Microsystems Nanoeng.*, vol. 3,

no. 1, p. 17059, Nov. 2017, doi: 10.1038/micronano.2017.59.

[3] A. Sen, M. Sen, and A. Ambekar, "Improved Electronic Voting Machine with Real Time Data Analysis," *Commun. Appl. Electron.*, 2016, doi: 10.5120/cae2016652420.

[4] M. M. Hoquec, "A Simplified Electronic Voting Machine System," *Int. J. Adv. Sci. Technol.*, 2014, doi: 10.14257/ijast.2014.62.07.

[5] K. Annapurna, V. Chandrani, P. Mounika, and P. T. Sree, "Design of Authenticated Radio Frequency Identification based Electronic Voting Machine," 2021. doi: 10.1109/ICICT50816.2021.9358668.

[6] A. C. S. Sheela and G. F. Ramya, "E-voting system using homomorphic encryption technique," 2021. doi: 10.1088/1742-6596/1770/1/012011.

CHAPTER 4

LIQUID CRYSTAL DISPLAY

Dr. A. Maheswari Senthil Kumar
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- a.maheswari@presidencyuniversity.in

Liquid Crystal Display (LCD) screens are electrical display modules that have a variety of uses. A 16x2 LCD display is a very fundamental module that is frequently included into many different devices and circuits. These modules are preferable over multi-segment LEDs with seven segments and additional segments. The explanations are that LCDs are inexpensive, easily programmable, and have no restrictions on showing unusual and even customized characters, animations, and other content. With a 16x2 LCD, there are 2 lines that can each display 16 characters. Each character on this LCD is presented using a 5x7 pixel matrix. The Command and Data registers on this LCD are its two registers. The command instructions sent to the LCD are stored in the command register. A command is a directive issued to an LCD device to carry out a certain operation, such as initializing it, clearing its screen, adjusting the cursor, managing the display, etc. The data that will be shown on the LCD is kept in the data register. The character's ASCII value, which will be shown on the LCD, is the data. Click to find out more about an LCD's internal construction (Figure 1) [1].

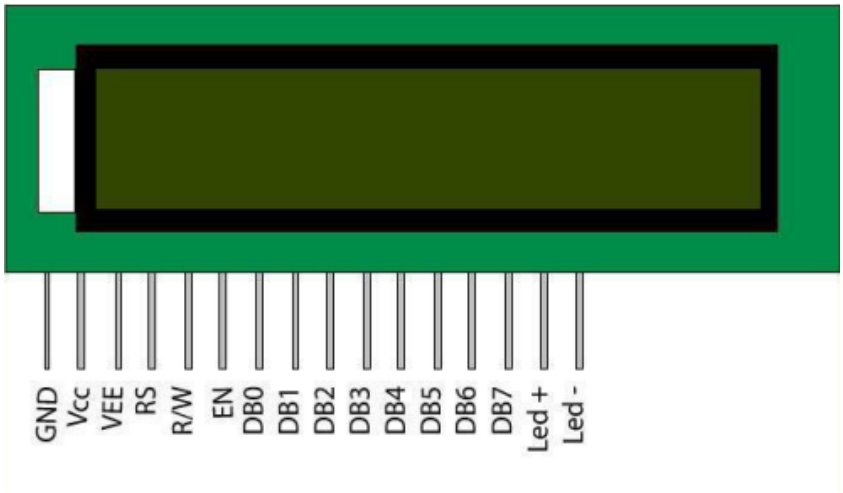

Figure 1: Represented LCD Modules.the

Any number of colour or monochrome pixels can be found inside an LCD, which is a small, flat display device that is arranged in front of a source of light or reflector. A column of liquid crystal molecules suspended between two transparent electrodes, two polarising filters with perpendicular polarity axes, and a column of liquid crystal molecules make up each pixel. Light flowing through one would be obstructed by the other without the liquid crystals separating them. To allow light to flow through the other filter, the liquid crystal twists the polarisation of the light entering the first one. Utilizing input and output methods that can speak with people directly, a software must

ISBN 978-81-962236-1-8 March 2023

engage with the outside world. An LCD is one of the most often used accessories for controllers [2].

A flat display screen known as a liquid crystal display (LCD) is used in digital equipment such laptops, computers, TVs, smartphones, and portable video games. As implied by the name, liquid crystal is a substance that flows like a liquid and has certain solid qualities. These LCD screens are very tiny and use less electricity than LEDs. Liquid crystals have a molecular structure that is halfway between solid crystal and liquid isotropic. Nematic liquid crystal molecular arrangement, in which molecules are somewhat aligned, is utilized in liquid crystal displays (LCDs). For instance, when the temperature rises, ice cubes melt and liquid crystals appear to be in a condition halfway between them and water. Two polarized glass components make up the LCD's construction. One positive electrode and one negative electrode are employed. These electrodes, which are constructed of indium-tin-oxide, are used to apply external voltage to LCDs. Between two sheets of glass is a liquid crystal layer that is between 10 and 20 microns thick. By altering the polarization, light is either passed through or prevented [3].

Liquid crystal display operation:

The core tenet of LCD operation is light blocking. Light is not generated by it on its own. The usage of an external light source. When external light travels from one polarizer to the next, the liquid crystal receives an external supply, and the polarized light aligns itself to generate an image. The sealed thick layer of liquid crystal has a transparent layer on both sides that serves as the indium oxide conducting surface. The molecular configuration is not altered when no external bias is applied. The molecular arrangement is altered when the external bias is applied, making that part seem dark and the other area appear clear [4].

Advantages:

- It is slim and little.
- Little power usage
- Less heat is produced when operating
- Less heat is produced when operating

Disadvantages:

- Low operation speed
- Shorter lifespan
- Limited viewing angles [5]

Bibliography:

[1] V. Malathy, N. Shilpa, M. Anand, and R. Elavarasi, “Radio frequency identification based electronic voting machine using fingerprint module,” 2020. doi: 10.1088/1757-899X/981/3/032018.

[2] Z. He, C. Zhang, Y. Dong, and S. T. Wu, “Emerging perovskite nanocrystals-enhanced solid-state lighting and liquid-crystal displays,” *Crystals*. 2019. doi: 10.3390/cryst9020059.

[3] L. Rocchetti, A. Amato, and F. Beolchini, "Recovery of indium from liquid crystal displays," *J. Clean. Prod.*, 2016, doi: 10.1016/j.jclepro.2015.12.080.

[4] M. Mele and G. Campana, "Advancing towards sustainability in liquid crystal display 3D printing via adaptive slicing," *Sustain. Prod. Consum.*, 2022, doi: 10.1016/j.spc.2021.12.024.

[5] learnelectronicswithme, "Liquid Crystal Display(LCD), Construction, Working, Advantages, Disadvantages and Applications," 2022.

ISBN 978-81-962236-1-8 March 2023

CHAPTER 5

RASPBERRY PI 3B+

Dr. A. Maheswari Senthil Kumar
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- a.maheswari@presidencyuniversity.in

The Raspberry Pi is a tiny computer the size of a credit card that runs Linux on an ARM processor. The Raspberry Pi 3 Model B+ is the product in question. It contains four USB ports, an Ethernet port, HDMI output, audio output, Bluetooth 4.2, Bluetooth Low Energy (BLE), dual-band WiFi, and 0.1″-spaced pins that allow access to general-purpose inputs and outputs (GPIO). An operating system-containing microSD card is necessary for the Raspberry Pi (not included). The Raspberry Pi is incredibly well-liked, and there are a tonne of example projects and online resources for it (Figure 1) [1].

Figure 1: Represented the RASPBERRY PI 3B+.

- **Benefits of choosing the Raspberry Pi 3 B+ Android.**

The Raspberry Pi 3 B+ is a fantastic choice for Android installation for a number of reasons. These consist of:

Excellent support for touch screens: Android on the Raspberry Pi 3 B+ supports touch screens natively. Because the touch-screen code is not optimized at the OS level, Linux distributions rely on software that runs on top of the main OS, such as Kodi, to support touch screens. People engaging with Android on the Raspberry Pi 3 B+ will have a comfortable user experience because the touch-screen functionality of Android is consistent with other Android devices [2].

Wide app ecosystem: On the Raspberry Pi 3 B+, there is a significant range of Android applications. This means that adding pre-existing apps might significantly improve the user experience as opposed to your firm having to spend money on further development. Due to

ISBN 978-81-962236-1-8

Android's popularity, these apps are often updated and improved, ensuring that Android on Raspberry Pi 3 B+ devices maintains parity with more widely used devices. The Google Play Store depends on GMS (Google Mobile Services), a collection of apps and APIs. GSM is not supported by Android on the Raspberry Pi 3 B+, although users may download a wide variety of apps from the open-source software store F-Droid [3].

Outstanding developer support: The Android developer community as a whole is quite supportive of Android on Raspberry Pi 3 B+. Although there aren't as many OS-level developers, their number is increasing because to the need for Android on Raspberry Pi 3 B+ solutions.

There are reportedly 5.9 million Android developers worldwide, compared to fewer than half that number for iOS, according to market research company Evans Data.

Android was created for portable devices: Small-powered devices were considered when developing the Android OS. Although a customized version of Android that has been converted to function especially on the Raspberry Pi 3 B+ is required to install Android on that device, the Android OS was designed from the beginning with this degree of operability in mind.

Android is cost-free: Android on the Raspberry Pi 3 B+ is open-source, meaning it may be customized and altered to suit the needs of any application. Unlike proprietary options, embedded Android promotes innovation and helps to create a market that is free from barriers to entry.

Device management and remote updates: Android on the Raspberry Pi 3 B+ makes fleet management of Raspberry Pi devices simpler due to its possible support for remote device management. Stock It is up to developers to expressly integrate these features into any version of Android for Raspberry Pi 3 B+ and to offer a user interface to control those devices, as was done with the emteria. Android provides the APIs required to allow Mobile Device Management (MDM) capability. Android OS version running on a Raspberry Pi 3 B+ [3]. The Raspberry Pi 3 B+ needs the following to enable Android's remote device management features:

A Raspberry Pi 3 B+ version of Android that has been specially modified to include MDM capabilities (such as emteria.OS)

A strong backend infrastructure that creates updates, distributes them to devices, and manages security.

Well-known user interface: The UI of Android on the Raspberry Pi 3 B+ is recognisable. Because consumers may use the gadget right away without having to search for menus and functionalities, the user experience is improved [4].

Excellent programming tool support: Many different development environments offer top-notch assistance for Android programming. Several of these tools are free and open-source [5].

Bibliography:

[1] M. Kamalakannan and K. Devadharshini, “Controlling the Speed of Conveyor Belt using Python – Raspberry Pi 3B+,” *Orient. J. Comput. Sci. Technol.*, 2019, doi: 10.13005/ojcst12.02.05.

[2] F. Budiman, M. Rivai, and M. A. Nugroho, "Monitoring and Control System for Ammonia and pH Levels for Fish Cultivation Implemented on Raspberry Pi 3B," 2019. doi: 10.1109/ISITIA.2019.8937217.

[3] R. Pandey, V. Jyothindar, and U. K. Chopra, "Vulnerability Assessment and Penetration Testing: A portable solution Implementation," 2020. doi: 10.1109/CICN49253.2020.9242640.

[4] M. Irfan, "CNN Image classifier on Raspberry pi 3B using pre trained data," *Mukt Shabd J.*, 2019.

[5] Emteria, "How to install Android on Raspberry Pi 3 B+," 2022.

ISBN 978-81-962236-1-8 March 2023

CHAPTER 6

ARDUINO NANO AND PI CAMERA

Dr. A Maheswari Senthil Kumar
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- a.maheswari@presidencyuniversity.in

Arduino Nano:

Robotics, automation, embedded systems, Internet of Things (IoT), and electronics applications frequently employ Arduino boards. Originally intended for non-technical consumers and students, these boards are now often employed in industrial applications [1].

Similar features of the Arduino Nano are also included in the Arduino Duemilanove, albeit in a different packaging. The ATmega328P microprocessor, which also powers the Arduino UNO, is incorporated inside the Nano [2]. The UNO board is offered in PDIP (Plastic Dual-In-line Package) form with 30 pins, whereas Nano is offered in TQFP (Plastic Quad Flat Pack) form with 32 pins. This is the primary distinction between both. While the Arduino UNO has 6 ADC ports, the Arduino Nano has 8 ADC ports, which are made possible by the additional 2 pins. The Nano board includes a mini-USB port rather than a DC power connection like previous Arduino boards. Both coding and serial monitoring are done using this port. The intriguing aspect of Nano is that the power source selection jumper is ineffective, and it will choose the source with the highest potential (Figure 1).

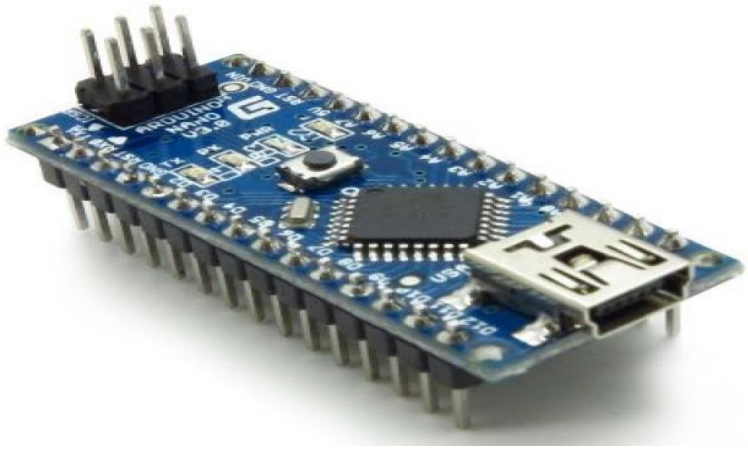

Figure 1: Representation of Arduino Nano.

- **Technical Requirements:**

The Arduino Nano board's technical specs are as follows:

- The Nano board's operational voltage ranges from 5V to 12V.

ISBN 978-81-962236-1-8 March 2023

- Nano has a total of 22 input/output pins.
- There are 8 analogue pins and 14 digital pins.
- The 14 digital pins include 6 PWM (Pulse Width Modulation) pins. The Arduino Nano's 6 PWM pins are used to translate digital signals into analogue impulses. The conversion is accomplished by changing the pulse's width.
- The Arduino Nano's crystal oscillator operates at a 16MHz frequency.
- Numerous applications, including robotics, control systems, measurement, automated, and embedded systems, employ the Arduino Nano.
- QR Code Scanner, DIY Arduino Pedometer, and more projects were developed using Arduino Nano.
- Additionally, Arduino Nano may be WiFi connected.
- Nano's features are comparable to those of the Arduino UNO.
- Nano is a special option for making electronic projects and devices with a small footprint because to its adaptability and eco-friendliness [3].

➢ **Pi Camera:**

A lightweight, portable camera that enables Raspberry Pi is called the Pi camera module. It uses the MIPI camera serial interface standard to talk to the Raspberry Pi. It is typically employed in projects involving image processing, machine learning, or surveillance. Since the payload of the camera is so small, it is frequently employed in surveillance drones. In addition to these modules, Pi may make use of regular USB cameras that are connected to computers [4].

Figure 1: Represented the Pi Camera.

High resolution video and images may be captured using the Pi Camera module. The Raspberry Pi Board contains a CSI (Camera Serial Port) interface, which allows for direct attachment of the PiCamera module. Using a 15-pin ribbon cable, this Pi Camera module may be connected to the CSI port of the Raspberry Pi.

➢ **Benefits of the Pi Camera:**

The Pi camera version 1.3 here. The features of it are as follows:

- 5 MP resolution
- HD video recording is available in several frame rates, such as 1080p @ 30 frames per second, 720p @ 60 frames per second, and 960p @ 45 frames per second.
- Wide, still (motionless) pictures with a resolution of 2592x1944 pixels are also possible.
- Enable CSI Interface [5].

Bibliography:

[1] Arduino, "Arduino Nano - Arduino Official Store," *Store.Arduino.Cc/Usa/*. 2017.

[2] A. Sultana, S. Fatima, H. Mubeen, R. Begum, K. Sohelrana, and A. Jameel, "A Review on Smart IoT based Gesture Controlled Grass Cutting Vehicle," 2020. doi: 10.1109/ICOEI48184.2020.9142981.

[3] Javatpoint, "Arduino Nano," 2022.

[4] V. Romashchenko, M. Brutscheck, and I. Chmielewski, "Organisation and Implementation of ResNet Face Recognition Architectures in the Environment of Zigbee-based Data Transmission Protocol," 2020. doi: 10.1109/MCNA50957.2020.9264283.

[5] Electronicwings, "Pi Camera Module Interface with Raspberry Pi using Python."

CHAPTER 7

INTRODUCTION TO BIOMETRIC SYSTEM

Mrs. Annapurna H. S.
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- annapurna.hs@presidencyuniversity.in

In recent years most of the emerging technologies are improved to preserve the patient details in an emergency case. Our project aims to provide the secured identification of the patient medical report in an emergency case using fingerprint based biometric system. Biometrics is physical and behavioral characteristics, which can be analyzed to identify a person digitally and grant access to data or systems. The future pretends a new era of biometrics. Advances in technology will make them more attractive in healthcare organizations. Decreasing in coast will make biometric a more palatable move. The biometric security systems act as a catch-and-release method to control access to certain data [1] .

An individual must submit their distinctive behavioral feature, which will be compared to a database in the structure, in order to be admitted to the biometric security structure. By doing this, we may obtain accurate patient medical history and data on their prior medical history. This fingerprint-based biometric technology is useful for the medical staff to continue treating the patient in case of emergency, particularly when the victim is unable to furnish their medical reports.

Electronic health records are now more often used in global healthcare than paper-based medical records (EHR). The following are some advantages of using EHRs to easily get patient data: Information that is current and accurate at the point of sale [2].

- incredibly well-coordinated and effective care
- safe exchange of patient data between doctors
- less medical mistakes
- safer prescription techniques

However, for these advantages to materialize, hospitals, doctors, and other healthcare organizations must consistently and precisely confirm the identities of all patients. Some medical facilities have responded to this fact by switching from biographic forms of identification, such as names, dates of birth, and Social Security numbers, to biometric ones, which are more reliable. In order to guarantee that the appropriate individuals receive care, patients must be identified using biologically distinctive characteristics (such as their face, fingerprint, iris, or voice). This creates a safer and more efficient environment for global healthcare. The distinct, quantifiable traits that are used to identify and categories people are called biometric identifiers. Physiological traits connected to a person's physical attributes, such as body form, are frequently characterized as biometric identifiers. Examples include fingerprint, palm vein, face identification, DNA, biometric traits, iris recognition, retina, aroma, voice, ear shape, and stride, among others. A person's behavior pattern is influenced by their behavioral traits, which can include but are not limited to their typing speed, locomotion, signature, behavioral profile, and credentials [3]. The latter category of biometrics has been dubbed "behaviometrics" by some researchers. Knowledge-based

ISBN 978-81-962236-1-8 March 2023

identifying systems and token-based identity systems, like a passport or driver's license, are more conventional methods of access control.

The identification of patients and staff may be made more secure with the use of biometrics technology like fingerprint scanners, finger vein readers, face recognition software, iris scanners, and others. This would assure that careers are dealing with the correct demographic and medical information, and that only the right personnel have access to the relevant information. It would also aid dependably verify whether patients are who they claim they are. However, the healthcare industry has been sluggish to adopt biometric technology. Although many clinics and hospitals have adopted some basic technology, biometrics is still not widely used in healthcare procedures. To get the technology accepted by the general public, hospital CISOs and biometrics technology suppliers will still need to put in some time and effort. In order to allow access to systems, devices, or data, a person might be digitally identified by their physical or behavioural features. These biometric identifiers include things like fingerprints, face patterns, speech patterns, and typing cadences. Each of these markers is thought to be particular to the person, and they can be combined to increase identification precision [4].

There will be a new biometric age in the future. The technologies will become more appealing to healthcare companies as they advance. Biometrics will become more acceptable as costs decline. In turn, other technologies such as artificial intelligence will help biometrics grow. The mainstreaming of biometrics, however, confronts several difficulties. These include interoperability, cost, personnel, and privacy. There is much territory to cover, therefore experts from biometrics technology companies, consulting businesses, and healthcare provider associations gave their perspectives on the way forward.

A biometric system compares biometric traits like a person's face, iris, fingerprints, etc. to successfully authenticate or identify them. Biometric technologies are being incorporated into the most ordinary aspects of daily life as interest in biometrics grows. Automated Biometric Identification System, or ABIS, is the most effective. Using fingerprints as identification is one popular biometrics application. Although it may be applied in more elevated or high-security circumstances, this system has only lately been customized for specific consumers. For instance, starting with the iPhone 5s, Apple was the first biggest smartphone maker to integrate a fingerprint login system. Other manufacturers quickly followed. Voice recognition software and iris or retina scans are examples of further biometric technologies [5].

Data breaches are becoming more frequent as society begins to depend more largely on technology and electronic information exchange. Target and Home Depot are two well-known instances of companies that have recently been the target of hackers. One technique for preventing these intrusions is biometrics. Since so many people use credit cards, internet banking, and smartphones to transfer money, it's crucial to adopt security measures like biometrics to thwart fraud, hackers, and breaches. Many banks and financial institutions exploit the technology built into newer phones by developing applications that need fingerprint authentication to access data, and as mobile technology advances, so do their particular biometrics systems. Customers may quickly and easily access protected financial information [6].

For the mass market, businesses have started to invest in more diversified biometric technologies. Zoloz is currently working on technologies that will enable participating businesses to safeguard customer account information using face recognition technology. Another business, Nymi, created ECG-reading wristbands that can scan a person's heartbeat and utilise that information to connect

ISBN 978-81-962236-1-8 March 2023

through Bluetooth to a secure network. MasterCard and Relay Investments are two businesses that are supporting this growth. Financial investors are drawn to the concept of employing data that is specific to each individual to safeguard information since biometrics are associated with higher levels of security. Technology that is still in development, biometrics has promise for the future. But be careful to examine the precise technology being used if you're thinking about investing in a business that uses biometrics, certain biometric technologies are more private than others, and some businesses have more sophisticated systems than others.

Bibliography

[1] J. Effah and E. Owusu-Oware, "From national to sector level biometric systems: the case of Ghana," *Inf. Technol. Dev.*, 2021, doi: 10.1080/02681102.2020.1818543.

[2] M. Joshi, B. Mazumdar, and S. Dey, "A comprehensive security analysis of match-in-database fingerprint biometric system," *Pattern Recognit. Lett.*, 2020, doi: 10.1016/j.patrec.2020.07.024.

[3] S. A. Raurale, J. McAllister, and J. M. Del Rincon, "EMG Biometric Systems Based on Different Wrist-Hand Movements," *IEEE Access*, 2021, doi: 10.1109/ACCESS.2021.3050704.

[4] F. Ennaama, K. Benhida, and A. Boulahoual, "Comparative and analysis study of biometric systems," *J. Theor. Appl. Inf. Technol.*, 2019.

[5] R. Páez, M. Pérez, G. Ramírez, J. Montes, and L. Bouvarel, "An architecture for biometric electronic identification document system based on blockchain," *Futur. Internet*, 2020, doi: 10.3390/fi12010010.

[6] M. Adámek, M. Matýsek, and P. Neumann, "Security of biometric systems," 2015. doi: 10.1016/j.proeng.2015.01.355.

ISBN 978-81-962236-1-8

CHAPTER 8

TYPES OF BIOMETRIC SYSTEM

Dr. Mohammed Aarif K. O.
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- mohammed.aarif@presidencyuniversity.in

Physical biometrics and behavioral biometrics are the two different categories of biometric systems. Take a look at how they vary from one another.

Physical Biometrics

The biometric information of a person is saved in a database with the use of specialised equipment (scanners, sensors, and other readers). This data, like a fingerprint, is saved by the system and transformed into digital data. The system then matches the fresh data with what is already in its database when the finger is reapplied to the scanner. Finally, if there is a match, the system will either verify the user's identity and provide them access or deny the request if there is not. Face recognition is a simple process for modern smartphone video cameras and recorders thanks to built-in sensors driven by neural networks. In this way, an individual is identified by their photograph [1].

Behavioral Biometrics

A recognition method called behavioural biometrics uses a person's dynamic or behavioural traits to identify them. These traits may include the dynamics of a person's handwriting and signature, voice and speech rhythms, gesture detection, typing speed, the way a person uses a tablet or smartphone and even their gait. As it doesn't require a user's active engagement to move on with the authentication procedure, this kind is also called passive biometrics. These dynamic authentication techniques are predicated on a person's behavioural traits. As they replicate any activity, they consider each person's distinctive behaviour and id motions. Voice recognition is a system that simultaneously analyses the dynamic and static aspects of human voice, combining physical and behavioural biometrics [2].

Fingerprint Scanning

Physical biometrics includes the identification of fingerprints. A fingerprint scanner is used to validate data for this authentication technique. Even with the variety of biometric systems, we can easily categorise them into three types that operate in three distinct ways: using an optical sensor to turn a fingerprint into a digital code, saving conversion that used a linear thermal sensor, and turning a fingerprint using a capacitive authentication sensor. Despite this diversity, the sole distinction for the end-user is which manipulations—applying their finger (optical and capacitance) or directing it via a sensor—are to be made with the scanner (thermal) [3].

Advantages of Fingerprint Scanning

- Unique identifiers that are distinct to the individual are fingerprints.
- This type of authentication is widely known.
- No need to keep track of difficult passwords.
- There are also fingerprint scanners for sale on Amazon, and they are reasonably priced.

ISBN 978-81-962236-1-8 March 2023

Disadvantages of Fingerprint Scanning

- Permanent or transient injuries might cause scans to malfunction.
- With techniques that duplicate and recreate fingerprints, it is a technique that can be gotten around. Even while copying a fingerprint is challenging, it is not impossible.
- It can be gotten around by using someone else's finger when they're unconscious or asleep [4].

Voice Recognition

Each person has a unique voice that is just as unique as their face or fingerprints. The widespread usage of phones in business communications presents a great potential for the application of this biometric authentication technique. Additionally, speech recognition is incredibly user-friendly and involves little effort on the part of the user. The processing of user speech is a direct application of voice biometric authentication technology in a number of settings, including call centres. Adopting this biometric technology enables the service to be expedited while also simplifying and improving the job of the agents. Use cases for this technology include teleconferencing, forensic analysis, credit card verification, and security systems.

Voice identification can be used in conjunction with another authentication technique, such as fingerprint scanning, in bigger projects, particularly where the requirement to secure sensitive information is high [5].

Advantages of Voice Recognition

- When being authorised, there is no need to memorise and then enter a password.
- Voice is a typical form of human engagement and communication.
- Both consumers and agents benefit from time savings, especially when passive voice biometrics are used.
- The voice is a distinctive quality that is very challenging to fake.
- Users are accustomed to this approach because it is extensively utilised.

Disadvantages of Voice Recognition

- Users could be concerned about their privacy and not know where their data is stored.
- Places with a lot of noise might make authentication fail.
- The success rate of verification may be lowered by severe respiratory sickness.

Iris Recognition

Ophthalmologist Frank Bursch originally suggested iris scanning technology in 1936. (source). John Dufman of Iridian Technologies developed an algorithm for spotting variations in the iris at the start of the 1990s. This biometric identification technology, which uses specialised iris scanners, now ranks among the most accurate.

The technology operates as follows: Finding the pupil comes first, then locating the iris and eyelids. The remaining portion of the eye, the iris, is then separated into blocks and transformed into numerical values describing the picture after extraneous components like the eyelids and eyebrows are removed. Finally, identification is confirmed by comparing newly obtained data with previously gathered data using the same techniques.

Advantages of Iris Recognition

ISBN 978-81-962236-1-8

- Iris is an internal organ that has a very transparent and delicate membrane protecting it from harm. Therefore, it's doubtful that small injuries will affect scanning technology.
- The iris is an invariant organ that varies greatly from person to person.
- There's no need to learn long passwords.

Bibliography

[1] M. Al Rousan and B. Intrigila, "A Comparative Analysis of Biometrics Types: Literature Review," *J. Comput. Sci.*, 2020, doi: 10.3844/jcssp.2020.1778.1788.

[2] S. Mekruksavanich and A. Jitpattanakul, "Biometric user identification based on human activity recognition using wearable sensors: An experiment using deep learning models," *Electron.*, 2021, doi: 10.3390/electronics10030308.

[3] S. Shin, M. Kang, J. Jung, and Y. T. Kim, "Development of miniaturized wearable wristband type surface emg measurement system for biometric authentication," *Electron.*, 2021, doi: 10.3390/electronics10080923.

[4] A. Mishra, "Multimodal Biometrics it is: Need for Future Systems," *Int. J. Comput. Appl.*, 2010, doi: 10.5120/720-1012.

[5] M. O. Oloyede and G. P. Hancke, "Unimodal and Multimodal Biometric Sensing Systems: A Review," *IEEE Access*. 2016. doi: 10.1109/ACCESS.2016.2614720.

CHAPTER 9

DISADVANTAGES OF IRIS RECOGNITION

Dr. Mohammed Aarif K. O.
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- mohammed.aarif@presidencyuniversity.in

This technology is currently under development and is still rather fresh. It's a technique that necessitates being close to the user's eye with the gadget. The likelihood of iris recognition is quite low in dim lighting.

Facial Recognition

The automated location of a human face within an image or video is known as facial recognition. A face image saved in a database as numerical code can be utilized by facial recognition technology, if necessary, to verify a person's identification using the information at hand. Because this technique can be used in videoconferencing, there is a lot of interest in this technology [1].

Advantages of Facial Recognition

- Minimal contact with the gadget is necessary.
- People are accustomed to this form of technology since it is so extensively utilized.
- When used in conjunction with other biometric techniques, very successful.
- Complex passwords are not necessary to remember [2].

Disadvantages of Facial Recognition

- The system's performance may be impacted by variations in lighting.
- The way the face appears to the system can be affected by facial expressions.
- It could be challenging to identify the user if face accessories are being worn.
- Some users could feel embarrassed by having to often glance at their phone to unlock it [3].

Handwriting Recognition

Dynamic signature confirmation can be used in workflow-intensive domains like banking or legal systems. Since a group of points might indicate a signature, the recognition of signatures is dependent on algorithms for pattern recognition or mathematical techniques for curve analysis. As a result, these systems frequently employ curve approximation or time series decomposition.

Advantages of Handwriting Recognition

- For millennia, identities were verified via signatures. This technology so inspires confidence.
- The technology doesn't need sophisticated equipment to function.
- It doesn't take a lot of explanation because it is obvious and natural.

Disadvantages of Handwriting Recognition

- Inconsistent signatures are common.

ISBN 978-81-962236-1-8 March 2023

- It could be tough to utilise this technology if you have injuries like broken fingers or arms.
- Only low-level security activities should use this technique.

Biometric Characteristic's Requirements

In contrast to conventional methods of personal identification that depend on what you have, biometrics as a method of identifying focuses on who you are. Both knowledge-based authentication (password or PIN) and token-based identification (passports, licences, ID cards, keys, and badges) have glaring drawbacks. Any one of them might be taken, shared and forgotten, or guessed by a fraudster. On the other hand hand, modern biometrics enable not only rapid and accurate identification but also the ability to distinguish between a fake and an authorised individual. Additionally, biometrics may do negative recognition, like blocking a terrorist in boarding an airline [4].

Biometrics: authentication or verification

Verification, in essence, is a biometric system function that does a one-to-one comparison to ascertain the veracity of an identification claim, such as "I am enrolled as subject X." In order to prevent countless individuals from using the same identity or, more particularly, to prevent unauthorised individuals from using someone else's identity, verification is frequently used for special reinforcement (see Positive identification). One-to-one comparison is another name for verification.

Biometric identification

In order to identify a specific individual, biometric identification is essentially a one-to-many procedure of comparing given biometric data against a particular or all database information. Identification offers a list of potential matches as candidates [5].

A comparison score from biometric authentication or verification, which is a 1:1 comparison, is combined with a threshold to create an access policy. A list of potential matching candidates is produced as a consequence of a 1: N comparison used for biometric identification.

Biometric information

Any physiological or behavioural property of a human being can be used as a biometric characteristic as long as it meets the criteria listed below:

Universality:

Every person ought to have a unique quality. Iris and Face are often accessible to everyone. In particular for manual labour, damage may make it difficult to gather fingerprints. As a result, fingerprints may not be as ubiquitous.

Uniqueness

Any two people ought to differ from one another in regard of their traits. Irises and fingerprints are quite distinctive for each individual. But at the other hand, faces are frequently comparable. Other distinct user-specific behavioral patterns, for instance the rhythm and cadence by which individuals typically write on their computer keyboard, are being investigated as a means of preventing online fraud. Handwriting, a certain gait, bodily gestures as a supporting method of personal identification, can be examined, as can event recognition.

ISBN 978-81-962236-1-8 March 2023

Permanence

A substantial amount of time should pass before the trait changes. Think about changing the comparison criteria. Because of this, even if a person's face changes significantly over the course of a lifetime, other traits do not change all that much and stay the same.After a few years, and during that they establish their permanent shape, fingerprints and iris stay steady [6].

Bibliography

[1] M. Andrejevic and N. Selwyn, "Facial recognition technology in schools: critical questions and concerns," *Learn. Media Technol.*, 2020, doi: 10.1080/17439884.2020.1686014.

[2] K. Wang and A. Kumar, "Cross-spectral iris recognition using CNN and supervised discrete hashing," *Pattern Recognit.*, 2019, doi: 10.1016/j.patcog.2018.08.010.

[3] W. K. Zhang and M. J. Kang, "Factors affecting the use of facial-recognition payment: An example of Chinese consumers," *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2927705.

[4] P. Nawrocki and W. Kubaty, "Assessment of the viability of a biometric characteristic in the context of biometric authentication on mobile devices," *Comput. Informatics*, 2021, doi: 10.31577/cai_2021_1_169.

[5] Y. Chen, C. Wu, and Y. Wang, "Whether normalized or not? Towards more robust iris recognition using dynamic programming," *Image Vis. Comput.*, 2021, doi: 10.1016/j.imavis.2021.104112.

[6] D. T. Nguyen, N. R. Baek, T. D. Pham, and K. R. Park, "Presentation attack detection for iris recognition system using NIR camera sensor," *Sensors (Switzerland)*, 2018, doi: 10.3390/s18051315.

CHAPTER 10

BIOMETRICS IN HEALTHCARE

Dr. Mohammed Aarif K. O.
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- mohammed.aarif@presidencyuniversity.in

Medical uses of biometrics aim to solve two main problems: patient matching and patient identification.

Patient Matching

The goal of patient matching is to guarantee that the appropriate patient data is entered into the appropriate medical record. It should come as no surprise that proper patient identification enhances treatment, lowers the chance of mistakes, and eliminates wasteful procedures like pointless testing [1].

Patient identification

Patient identification errors can result in mistakes with medication administration, unfavorable blood transfusion interactions, failure to treat a serious disease or illness, medical treatment for incorrect diagnostic testing results, and procedures being performed just on wrong patient, among other mistakes [2].

Patient misidentification has been a recurring issue in healthcare institutions as well, causing patients a great deal of distress and hospitals to face legal action. One instance included administering chemotherapy meant for another patient to a patient. Before starting the procedure, the accountable nurse checked the patient's ID on their bracelet. They had no idea that the hospital's database had another patient with the identical first and last name. Fortunately, the patient wasn't seriously hurt, but they still succeeded in their lawsuit against the hospital. The healthcare industry is seeking for a new reliable identification form in light of all these horrific incidents. Because they are permanently connected to the patient and cannot be "forgotten," biometrics are unquestionably unique identifiers [3].

Advantages of biometrics in healthcare

- a trustworthy form of identity that is unbreakable and unforgettably secure, unlike passwords
- Since no actual item needs to be carried, it is simple and practical to utilize
- Suitable for special needs individuals. According to one research, those who are illiterate are happy to use biometric scanners since it spares them from having to admit that they are unable to write.

Disadvantages of biometrics in healthcare

- Medical organisations must exercise caution when it comes to data security. The repercussions of exposing sensitive material may be dire. If someone's password was compromised, they can quickly change it. However, if biometric data was compromised, it

ISBN 978-81-962236-1-8

would be impossible to alter someone's fingerprints or eyes. Replacement of the identifying system or exclusion of the victim are likely requirements.

- Purchasing biometric identification technology is frequently expensive.
- The bodily component used in biometrics may become useless due to physical injury [4].

Biometrics healthcare applications

- In hospitals, biometrics are mostly used for patient and personnel identification. By doing this, the health system's workflow is enhanced, duplication is decreased, and patients are identified. Despite being a potential use case, patient matching among health providers is still not extensively used.
- Medical biometrics have already been adopted by numerous healthcare organisations. The University Of Pittsburgh Medical Center, for instance, has installed finger scanners. Palm vein scanning is used by Houston-based Harris Health System for identification. The use of facial and iris-based identification technologies is being tested by Northwell Health.
- Even a portable device exists to scan infants' fingerprints. The fingers of a baby are little and squishy, despite the fact that they are completely developed. For an accurate picture, this gadget uses sensors that are seven more sensitive than typical fingerprint scanners.

Medical biometrics in data security and cloud access

The digital transformation of many healthcare companies has resulted in the migration of their data onto the cloud. For instance, Imprivata has connected its OneSign solution with Microsoft Azure, enabling its healthcare customers to view their data in the cloud using biometric fingerprint screening as a way of identity.

Healthcare biometrics for regulated substance prescription

Electronic prescriptions for restricted drugs are subject to strict regulations and need a strong authentication method. The aforementioned business, Imprivata, created the Confirm ID system, which uses biometrics, to help healthcare institutions meet DEA regulations for computerised prescriptions of controlled medications.

Medical biometrics in telehealth

Since the pandemic, mhealth has grown in popularity since it enables people to obtain high-quality medical treatment while remaining in the comfort of their homes. Both patients and doctors can use biometrics-based authentication as a secure telehealth portal login technique [5].

Challenges and considerations of Biometrics in healthcare

Additional software, compatible with the hospital's EHR platform and other relevant apps, is needed for biometric authentication. Otherwise, technical problems could occur, such as those involving Windows Hello, a fingerprint authentication system for granting access to devices, applications, etc. Its restriction to Windows 10 and the fact that many clinics were still updating to the newest operating systems prevented it from being extensively implemented.

Examine the possible effects of the new fingerprints system on your current IT infrastructure, taking into account network capacity and system integration. Select a reputable healthcare biometrics supplier that will provide after-sales assistance and assist in resolving any issues the system may cause with your other apps. Additionally, it's great if the supplier is already acquainted with the healthcare industry and the rules that govern it. Conversant with the laws and regulations

that govern the healthcare industry.to keep biometric medical data secure. The category of protected data includes biometrics (PHI). Health Insurance Portability Act (HIPAA), Health Information Technology for Socioeconomic and Clinical Health (HITECH) Act, and other rules relevant in their nation of operations require medical facilities to protect this data. As of the time this article was written, the Biomedical Information Privacy Act (BIPA) had been approved by five US states. It is up for debate in other states. Watch the news closely to guarantee compliance by doing so [6].

Bibliography

[1] R. A. Naqvi, D. Hussain, and W. K. Loh, "Artificial intelligence-based semantic segmentation of ocular regions for biometrics and healthcare applications," *Comput. Mater. Contin.*, 2021, doi: 10.32604/cmc.2020.013249.

[2] D. Marohn, "Biometrics in healthcare," *Biometric Technol. Today*, 2006, doi: 10.1016/S0969-4765(06)70592-6.

[3] R. K. Mishra, "The Appropriated Body: Biometrics Regime, The Digital State and Healthcare in Contemporary India," *Glob. Policy*, 2021, doi: 10.1111/1758-5899.12945.

[4] J. W. Crampton, "Platform biometrics," *Surveill. Soc.*, 2019, doi: 10.24908/ss.v17i1/2.13111.

[5] A. Rattani and R. Derakhshani, "A Survey Of mobile face biometrics," *Comput. Electr. Eng.*, 2018, doi: 10.1016/j.compeleceng.2018.09.005.

[6] M. Leghari, S. Memon, L. Das Dhomeja, A. H. Jalbani, and A. Ali Chandio, "Deep feature fusion of fingerprint and online signature for multimodal biometrics," *Computers*, 2021, doi: 10.3390/computers10020021.

ISBN 978-81-962236-1-8 March 2023

CHAPTER 11

SECURED HUMAN HEALTH RECORD ACCESS USING BIOMETRIC SYSTEM

Dr. Sandhya Dass
Associate Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- sandhya.dass@presidencyuniversity.in

With the use of biometrics, cloud software, and intelligent wearables, Healthcare 4.0 has automated the traditional banking services provided by the healthcare system. After Healthcare 2.0, health systems also began electronically recording patient data. Digital techniques are more efficient and simpler to use than the conventional paper approach. Threats to security are the major problem with the digital system, though. An Electronic Health Record (EHR) that is accessed online and through cloud services is where a person's medical information is kept. Although data may be accessed anywhere by both patients and clinicians, data privacy has emerged as a top issue for people. Healthcare institutions started using biometrics to secure patient data after the broad use of biometric security technologies [1] .

Process to secure Electronic Health Record data

One of the most important pieces of data about a person is their health data. These data are necessary for the insurance and pharmaceutical sectors' business operations and evaluation. Biometric authentication is appropriate to safeguard data in this case. The following is a list of the applications for biometrics in EHR.

Authenticate doctor

Doctors who treat patients are frequently the data administrators. The doctor creates space inside the cloud or server and uses biometric sign-in to verify his patient's identification throughout the patient registration process. Only the designated doctor has access to the patient history thanks to biometric authentication. A patient needs log out of the system before the doctor can no longer access the patient's data after the patient departs the hospital or stops receiving treatment. After some time has passed, the patient must log in again to provide a doctor access access his information. The first time the patient was seen by the doctor, and a second visit need not be identical [2].

Identify the patient correctly

The most important part of therapy is identifying the patient. Misidentification is one of the primary causes of all unfavourable surgical outcomes and blood transfusion errors, according to several studies. By using biometrics can identify patients, issues like incorrect blood analysis identification and erroneous diagnostic outcomes can be reduced. The patient's biometric information is gathered throughout various medical exams and cross-referenced with the previously registered information to guarantee no misidentification [3].

Securing the electronic health record

Three tiers of security are required for the data: wearable technology, health records, and cloud services. Wearable technology connects to a physician's mobile device or a hospital's main device

ISBN 978-81-962236-1-8 March 2023

using wifi, Bluetooth, or NFC. These communication will be encrypted, and only authorised users will be able to access the devices thanks to biometric authentication. Only the user and system administrator will be able to access the electronic medical record or cloud where the data are kept using the bio-login technique. Whether the administrator requires access to a patient's data can be determined by the system's architecture. He or she must demand the patient's biometric authentication [4].

Electronic Health Record in detail

A patient's paper chart gets converted to digital form in an electronic health record (EHR). EHRs are patient-centered, real-time records that securely and promptly make information accessible to authorised users. An EHR system is designed to go beyond the typical clinical data collected in a provider's office and can be inclusive of a broader picture of a patient's care, even if it does contain full medical and treatment records of patients. An essential component of health IT, EHRs can:

- Contain a patient's medical history, diagnoses, prescriptions, treatment schedules, dates of vaccinations, allergies, radiological pictures, and results of lab and test work.
- Give professionals access to evidence-based instruments so they may decide how to treat patients.

A Problem-Oriented Medical Record, the first EHR prototype, debuted fifty years ago. It was made up of a database with a patient's whole clinical history, a list of the patient's medical complaints, an initial plan of treatment in which a doctor determines what to do about the condition, daily progress reports, and a discharge report that highlights any unresolved issues [5].

EHR software now goes beyond simple record management. The EHR is evolving into a complete clinic management system with useful practise and revenue management functions. It is a key premise, according to Nabil Manzoor, a specialist with more than 15 years of experience in healthcare advising and a founding member of the Healthcare Cryptocurrency Working Group INATBA: "EHR should control all the activities from the frontline care to the back office.

EHR Workflow

EHR was created to support the clinic's current workflow. It also suggests that everyone involved in patient care is connected to one another.

Patient

Patient is eager to visit a physician. Either at the front desk or through a self-service check-in kiosk, it can be done. A patient enters all of their information there, including past and present illnesses, allergies, treatments received, and payment information. A patient who registers receives an account so at patient portal where they may examine a summary of their visits, make appointment requests, etc.

Front office

A receptionist uses the centralised scheduling module to schedule a patient's appointment with a doctor. The system distributes patient queues based on several sources, including online booking, check-in counts, and reception desks, and automatically accommodates each doctor's workload.

Physician

The doctor is informed of the scheduled visit. The patient's characteristics, medical history, and symptoms are all accessible on the patient chart. After the actual or virtual consultation, a physician

records a clinical note from the appointment into the practice's electronic health record system (EHR) along with the diagnoses, prescription, and any other instructions. A nurse, counselor, or the other doctor can later consult the letter to do the required operations.

Insurance company

The billing component of the EHR then creates an insurance claim. Prior to sending the claim to the insurers to reimburse the costs, it is first checked for mistakes at the clearinghouse, then formatted to the insurer's specifications.

Bibliography

[1] J. Effah and E. Owusu-Oware, "From national to sector level biometric systems: the case of Ghana," *Inf. Technol. Dev.*, 2021, doi: 10.1080/02681102.2020.1818543.

[2] P. H. Pisani *et al.*, "Adaptive biometric systems: Review and perspectives," *ACM Comput. Surv.*, 2019, doi: 10.1145/3344255.

[3] W. Jia *et al.*, "A survey on dorsal hand vein biometrics," *Pattern Recognit.*, 2021, doi: 10.1016/j.patcog.2021.108122.

[4] A. S. Rathore, Z. Li, W. Zhu, Z. Jin, and W. Xu, "A Survey on Heart Biometrics," *ACM Computing Surveys*. 2021. doi: 10.1145/3410158.

[5] N. Garcelon, A. Burgun, R. Salomon, and A. Neuraz, "Electronic health records for the diagnosis of rare diseases," *Kidney International*. 2020. doi: 10.1016/j.kint.2019.11.037.

CHAPTER 12

INTEROPERABILITY AMONG DIFFERENT ELECTRONIC HEALTH RECORD SYSTEMS

Dr. Sandhya Dass
Associate Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- sandhya.dass@presidencyuniversity.in

The electronic exchange of patient data between various EHR systems and healthcare providers is made possible by interoperable electronic health records (EHR). The simplicity with which doctors can treat their patients is increased through healthcare interoperability, and it can also assist patients in navigating the healthcare environment [1].

Directed Exchange

An electronic health information exchange is required under the HIPAA Security Rule to guarantee the patient data's secrecy, integrity, and technical safety. As a result, healthcare providers can comply with HIPAA by using the Directed Exchange technique. DE is a secure email-based technology that can only be used with certified EHRs and always has a defined sender and recipient [2]. Physicians may exchange messages, attach files in compatible formats, handle referrals online, and more thanks to the Directed Exchange connection across EHRs [3].

Health information exchange organization

A secure central repository known as the HIE collects patient data from various hospitals and EHR systems. As a result, a participating practitioner can send a query to other connected EHRs to see if they have data on a particular patient.

Patient matching algorithms

EHR's automatic algorithms compare demographic data and ensure that records from multiple authorities pertain to the same patient. Accurate matching may be hampered by differences in the structuring of patient demographic data between systems. Because of this, ONC advises standardising demographic data and mandates the use of address, name, birthday, phone number, and sex as matching criteria. Using an email account or mother's maiden name can help improve matching precision [4].

Electronic Medical Record

A digitalized patient chart from a single doctor or clinic is an EMR. Making the appropriate diagnosis, giving the appropriate therapy, and keeping tabs on the patient's health are its three main objectives. An EMR system is not meant to be shared outside of the specific practise; instead, it is created to retain health information locally.

Electronic Health Record features and modules

HR is responsible for protecting patient data. It ought to identify the degrees of access by authenticating users and/or entities. With the help of automatic data backups, auto log-offs,

ISBN 978-81-962236-1-8 March 2023

encryption techniques, auditing, access control, secure communications systems, etc., EHR protects patient information from potential risks and data loss [5].

EHR scheduler

A tool that facilitates dental and medical patient schedule by directly connecting with an EHR system for quick access to patient data is known as an EHR scheduler or EHR scheduling software. Online patient scheduling allows you to manage appointments electronically while automating a lot of the procedure. Medical and dental firms in the healthcare sector rely on EHR integration for appointment scheduling to assure accurate data and improved patient care. When accessing their schedule, doctors and dentists may examine patient details, enhancing patient care and simplifying the medical professional's job [6].

Common features of an EHR appointment scheduler

Schedule management

Organize your practice's data, including patient information, inventory, and more, to make it simple to maintain and access as required.

Appointment setting:

Give your staff the authority to make appointment for your patients. Patients should be able to make their own online appointment bookings with a proper EHR schedule. Supports one-way or two-way contact with patients, allowing you to interact with them, get insightful feedback, and fill in for missed visits.

Appointment reaffirmation

Automatically notify appointment reminders to patients to help prevent cancellations and no-shows and to make sure they are informed of forthcoming appointments.

Physician support

Health information about patients is compiled in an electronic chart via EHR. A doctor can access a patient's chart to obtain a summary of information about that patient, including information on their demographics, immunisation records, allergies, medical history, lab but also test results, diagnostic tests, vital signs, prescription medications, and present health issues, as well as information on their insurance coverage and billing information.

Reports generation

A problem list, medication list, encounter summaries, clinical visit notes, a treatment plan, progress notes, instructions pertaining to both pre- and post-procedural and post-discharge needs, medical histories, patient care orders, etc. are all included in the typical patient-specific reports. Templates may be modified using a menu of choices based on the speciality and purpose of the visit.

ISBN 978-81-962236-1-8 March 2023

E-Prescribing

All prescription information is recorded by EHR and sent straight to the pharmacy's computer system while remaining on the patient's file. Additionally, based on the circumstances and features of the patient at the time of ordering the medicine, the system can review the prescription and signal drug interaction alerts or suitable dose suggestions.

Bibliography

[1] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K. K. R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," *Computers and Security*. 2020. doi: 10.1016/j.cose.2020.101966.

[2] E. K. Christiansen, E. Skipenes, M. F. Hausken, S. Skeie, T. Østbye, and M. M. Iversen, "Shared Electronic Health Record Systems: Key Legal and Security Challenges," *Journal of Diabetes Science and Technology*. 2017. doi: 10.1177/1932296817709797.

[3] M. I. M. Salleh, R. Abdullah, and N. Zakaria, "Evaluating the effects of electronic health records system adoption on the performance of Malaysian health care providers," *BMC Med. Inform. Decis. Mak.*, 2021, doi: 10.1186/s12911-021-01447-4.

[4] B. Middleton *et al.*, "Enhancing patient safety and quality of care by improving the usability of electronic health record systems: Recommendations from AMIA," *J. Am. Med. Informatics Assoc.*, 2013, doi: 10.1136/amiajnl-2012-001458.

[5] G. Yang, C. Li, and K. E. Marstein, "A blockchain-based architecture for securing electronic health record systems," 2021. doi: 10.1002/cpe.5479.

[6] J. M. Gesulga, A. Berjame, K. S. Moquiala, and A. Galido, "Barriers to Electronic Health Record System Implementation and Information Systems Resources: A Structured Review," 2017. doi: 10.1016/j.procs.2017.12.188.

Publisher
M/s CIIR Research Publications
B-17, Sector-6, Noida,
Uttar Pradesh, India.
201301
Email: info@ciir.in

March 2023
ISBN 978-81-962236-1-8