International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Advancing Electoral Processes: A Novel E-Voting Model Integrating Iris Scans, Raspberry Pi, and Blockchain Technology

RIJOY GN, VARADA ANIL, SANDRA S BAIJU, RAHANA HARIDAS, AISWARYA C

Abstract:

The amalgamation of an e-voting system with blockchain technology represents a significant advancement in the electoral process, streamlining voting procedures. However, concerns persist regarding the security and auditability of the system. While blockchain provides robust security and transparency to safeguard the integrity of votes, it faces potential resistance from tech-agnostic users. In response to these challenges, a novel e-voting model is proposed, leveraging iris scans through Raspberry Pi technology, offering a promising avenue for enhanced security and user acceptance. Moreover, this biometric approach introduces a seamless and user-friendly authentication process, potentially mitigating the resistance faced by tech-agnostic voters in adopting advanced e-voting technologies. The integration of iris scans through Raspberry Pi into the e-voting system, coupled with blockchain technology, presents a comprehensive and forward-thinking solution to the challenges posed by security, auditability, and user acceptance. This multifaceted approach not only addresses existing concerns but also sets the stage for a more inclusive and secure electoral process in the digital age.

Introduction:

In recent years, the amalgamation of electronic voting (e-voting) systems with blockchain technology has garnered considerable attention as a means to revolutionize the electoral process. While blockchain offers robust security and transparency, concerns persist regarding the system's overall integrity and user acceptance. These concerns are particularly pronounced among individuals who are hesitant to embrace advanced technological solutions.

In this context, this paper presents a novel e-voting model that seeks to address these challenges by integrating biometric authentication, specifically iris scans, through Raspberry Pi technology. By leveraging biometrics, this approach enhances the security and reliability of e-voting systems while also simplifying the authentication process for users. Moreover, the use of Raspberry Pi technology offers a cost-effective and accessible solution that can be easily deployed across diverse electoral environments.

This paper explores the rationale behind integrating iris scans with Raspberry Pi and blockchain technology in e-voting systems. It examines the potential benefits of this multifaceted approach, including enhanced security, auditability, and user acceptance. Furthermore, it discusses the implications of such a system for the future of electoral processes, emphasizing the importance of inclusivity and integrity in the digital age. Through this exploration, the paper aims to contribute to ongoing discussions surrounding the development of more secure and accessible e-voting systems.

EXISTING SYATEM

Electronic voting systems, while offering advantages such as increased efficiency and faster results, are not without significant drawbacks. Security concerns are paramount, with the potential for hacking and manipulation of electronic voting machines posing a serious threat to the integrity of elections. Vulnerability to malware adds another layer of risk, as malicious software can compromise the confidentiality and accuracy of recorded votes. Lack of transparency, often stemming from the use of proprietary software, undermines public trust, making it difficult for independent parties to verify the technology's accuracy and security. Accessibility issues for voters with disabilities, technical glitches, and the high cost of implementation further contribute to the challenges. The dependence on electricity and infrastructure, coupled with the absence of a paper trail in some systems, raises concerns about reliability and verifiability. To address these disadvantages, it is essential to implement robust security measures, ensure transparency in system design, and consider the accessibility needs of all voters. Thorough testing, reliable power sources, and the incorporation of paper trails are crucial steps toward building trust and safeguarding the democratic process in electronic voting.

PROPOSED SYSTEM

The proposed system represents a forward-looking approach to the electoral process, leveraging advanced technology to address the limitations of traditional paper-based voting systems. Key features of the proposed system include electronic voting, where voters use secure electronic devices to cast their ballots, eliminating the complexities of paper ballots and offering user-friendly interfaces. Biometric authentication methods such as fingerprint recognition and facial recognition are incorporated to ensure the integrity of the voting process by verifying the identity of voters, virtually eliminating the possibility of fraudulent voting. Real-time results tabulation enables swift announcements of election outcomes. Accessibility features cater to individuals with disabilities, and enhanced security measures, including robust encryption and digital signatures, safeguard vote data from tampering or hacking. The system also supports remote voting, promoting higher turnout and convenience while maintaining security. Detailed audit trails ensure transparency, and its scalability allows customization for various election sizes. The electronic nature of the system facilitates data analytics, offering valuable insights into voter behavior and preferences. By eliminating paper ballots and printed materials, the proposed system significantly reduces its environmental footprint, contributing to sustainability efforts. In summary, the proposed electronic voting system aims to enhance the efficiency, security, accessibility, and transparency of the electoral process, ultimately strengthening the foundations of democracy in the digital age.

BLOCK DIAGRAM

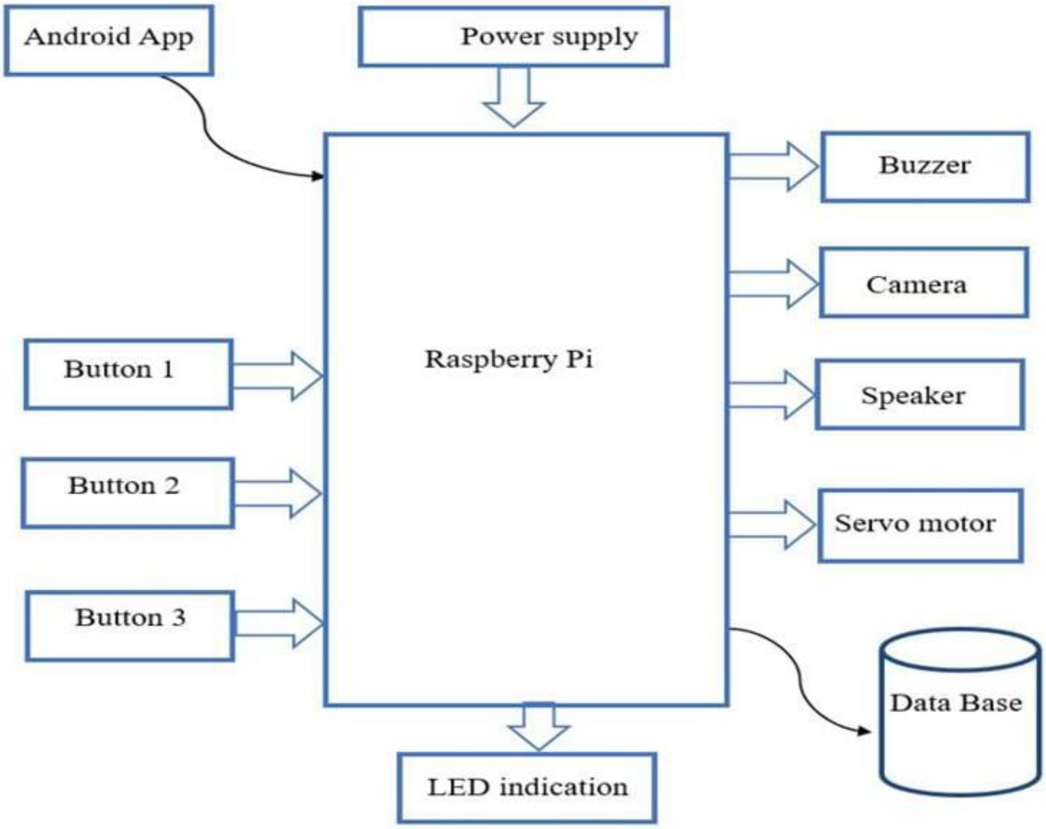
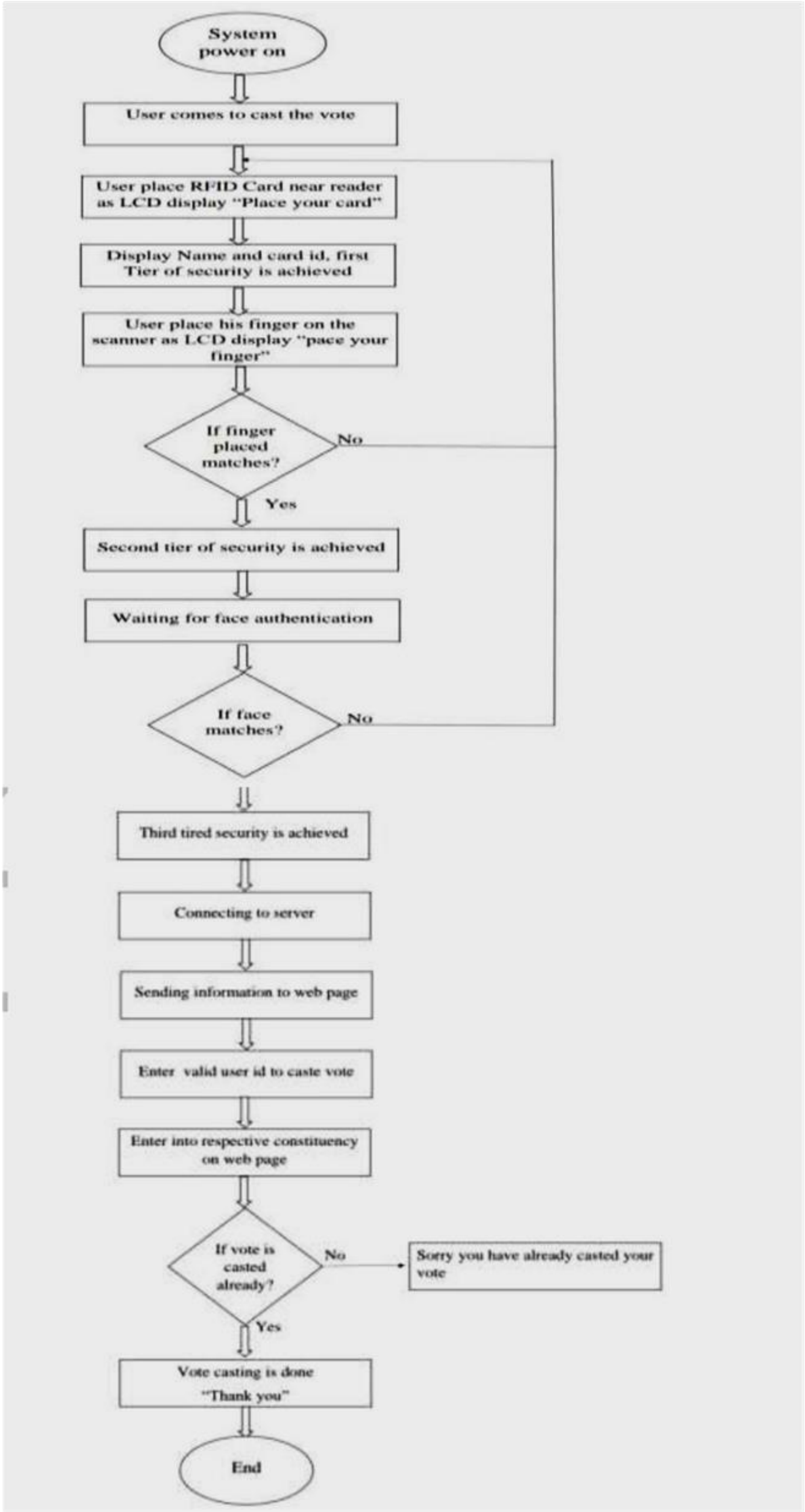


Figure 1: Block diagram of EVM model.

The core element of this innovative project is the Raspberry Pi, serving as the central processing unit for an electronic voting machine that embraces cutting-edge technology. Integrated with a high-quality Pi camera, the system leverages sophisticated facial recognition algorithms to validate voters. This process involves cross-referencing captured facial features with the extensive Aadhar database stored in MySQL, ensuring a secure and accurate identification process. To enhance security and regulate access to the private voting room, a servo motor is strategically employed. This motor acts as a gatekeeper, allowing only one person at a time to enter the voting area after successful facial recognition. This meticulous control ensures the integrity and confidentiality of each vote cast. The entire system is orchestrated through Android Studio, a powerful development environment, ensuring a seamless and user-friendly interface. The utilization of Android Studio not only streamlines the user experience but also facilitates smooth interaction with the electronic voting machine. This comprehensive integration of advanced technologies, from facial recognition to secure database management and controlled access mechanisms, positions the project at the forefront of modern electronic voting systems, offering an efficient, secure, and user-centric approach to the democratic process.

The electronic voting system employs a comprehensive approach to person authentication by integrating face recognition and fingerprint identification. The process initiates with the Face Recognition Module, capturing unique facial features through a camera and processing them using advanced algorithms to generate a distinct biometric signature. Simultaneously, the Fingerprint Identification Module analyzes fingerprint patterns from a scanner. Both sets of biometric data are forwarded to the Biometric Matching Unit, which compares them with details stored in the Aadhar card database.

The Microcontroller, powered by a 5V supply, acts as the system's core, receiving and processing matched biometric data. The User Interface, comprising an LED Screen and Speaker, guides the user through placing their face and fingerprint for identification. If successful, the Gate Control Module is triggered, opening access to a Private Voting Room to ensure voter privacy. Within this room, the voter engages with a secure electronic voting mechanism to cast their vote. The process concludes with a confirmation, and the Gate Control Module ensures the voter exits the voting area. This integrated system not only enhances security and minimizes identity fraud but also prioritizes a user-friendly and private voting experience.


System power on
User comes to cast the vote
User place RFID Card near reader as LCD display "Place your card"
Display Name and card id, first Tier of security is achieved
User place his finger on the scanner as LCD display "pace your finger"
If finger placed matches?
No
Yes
Second tier of security is achieved
Waiting for face authentication
If face matches?
No
Third tired security is achieved
Connecting to server
Sending information to web page
Enter valid user id to caste vote
Enter into respective constituency on web page
If vote is casted already?
No
Sorry you have already casted your vote
Yes
Vote casting is done "Thank you"
End

The electronic voting system begins its operation with the initiation of the system power, setting the stage for a secure and streamlined voting process. As users approach to cast their votes, the first layer of security unfolds through RFID card authentication. Placing their card near the reader prompts an LCD display instructing them to "Place your card," simultaneously presenting their name and card ID. This initial tier of security ensures the legitimacy of the voter. Subsequently, the system progresses to fingerprint authentication, instructing users to place their finger on the scanner. If the fingerprint matches, the second layer of security is achieved, marking a critical step in the verification process. In cases where fingerprint verification falls short, the system seamlessly transitions to face authentication, constituting the third tier of security. If the facial recognition process succeeds, the user gains access to the voting privileges; otherwise, the system proceeds to connect to the server. if so: "Sorry, you have already casted your vote." In the absence of a prior vote, users proceed to cast their votes on the web page. The culmination of this process is marked by a confirmation message on the LCD display: "Vote casting is done. Thank you." As the entire voting journey concludes, the electronic voting system stands as a testament to the integration of multiple security layers and technological components, ensuring the integrity and efficiency of the democratic process. The deatailed flow of the program is shown in figure 2. Establishing a connection with the server, the electronic voting system sends user information to a dedicated web page. Users are then prompted to enter a valid user ID to proceed with casting their vote, gaining entry into their respective constituency on the web page. The system meticulously checks whether the vote has already been casted, displaying a message.

Methodologies

1. Raspberry Pi: The Raspberry Pi serves as the central computing platform, coordinating and managing all components of the electronic voting system.

2. Facial Recognition (Pi Camera): Capture images with the Pi Camera, analyze facial features, and compare against a pre-trained model for voter identification.

3. Aadhar Database Integration: Establish a connection to the Aadhar database using secure protocols. Implement a query system to verify voter identity based on Aadhar details, ensuring a unique and valid voter.

4. Servo Motor for Entry Control: Program the servo motor to control the physical entry to the private voting room. Enable entry only after successful authentication via facial recognition and Aadhar verification.

5. MySQL Database Management: Design a MySQL database schema to store voter information, vote records, and other relevant data securely.

Implement database transactions to maintain data consistency and integrity.

6. Android Studio Interface: Develop an Android Studio application for voters to interact with the electronic voting system. It also enables voters to initiate the identification process, cast their vote, and receive confirmation through a user-friendly interface.

Electrical Architecture

The electronic voting system's electrical architecture revolves around a central Raspberry Pi, which serves as the core processing unit and orchestrates the interaction among various components. The Pi Camera, responsible for facial recognition, interfaces with the Raspberry Pi through the Camera Serial Interface (CSI), utilizing GPIO pins for power supply and control. Similarly, the Servo Motor, employed for entry control to the private voting room, connects to specific GPIO pins on the Raspberry Pi, requiring a dedicated power source and ground connection.

The Aadhar Database integration involves the Raspberry Pi establishing a secure connection to the Aadhar database server, ensuring the authentication and verification of voters. This communication relies on secure protocols like HTTPS to safeguard the exchange of sensitive information. Additionally, the system interacts with a MySQL Database, where the Raspberry Pi connects to a MySQL server, utilizing a combination of GPIO pins and network connectivity to manage and store voting data securely.

The Android Studio Interface facilitates communication between the voter and the Raspberry Pi. The Android device communicates with the Pi via either Wi-Fi or Bluetooth, employing a secure protocol to ensure the integrity of data transfer. In summary, this comprehensive electrical architecture underscores the interconnectedness of the Raspberry Pi with components such as the Pi Camera, Servo Motor, Aadhar Database, MySQL Database, and the Android Studio Interface, collectively forming a robust and secure electronic voting system.

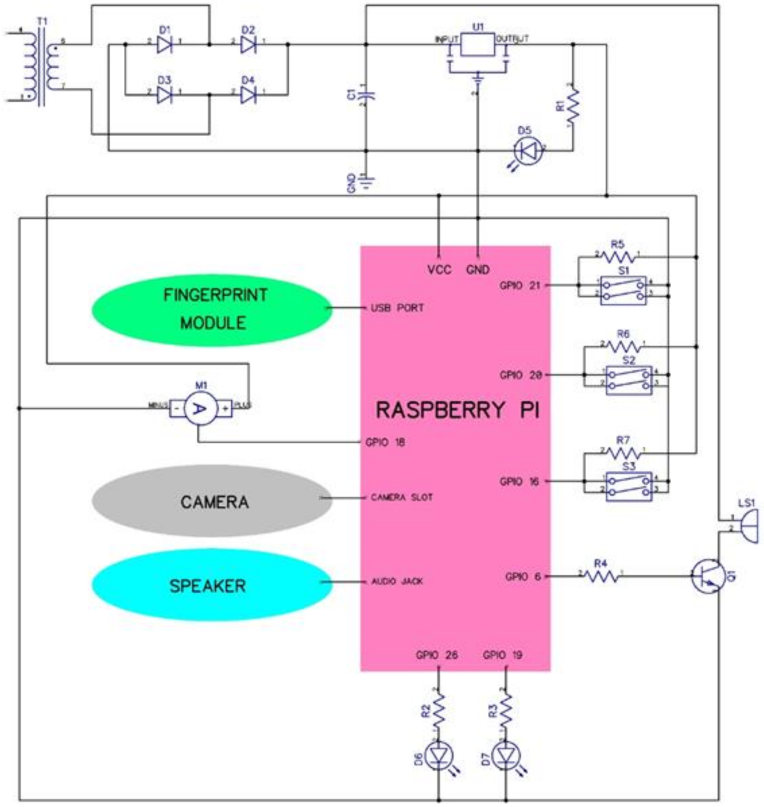


Figure 3: Circuit Design

An electronic voting system incorporating biometric components is designed to ensure secure and efficient voting processes. The system comprises essential components including a Fingerprint Scanner Module, Camera, Speaker, Microcontroller (such as Raspberry Pi), Display Device (like a Touchscreen LCD), and optionally, a Keypad.

In this configuration, the Fingerprint Scanner Module is linked to the microcontroller via GPIO 21, while the Camera is connected to GPIO 18. The Speaker is integrated through GPIO 6, and the Display Device is connected to GPIO 19. If a Keypad is utilized, it is connected to GPIO 26.

The Microcontroller, typically a Raspberry Pi, orchestrates the entire voting procedure. It begins by authenticating the identity of the voter through fingerprint comparison with a pre-existing database. Once authenticated, the system displays the ballot on the Touchscreen LCD for voter selection. Optionally, a Keypad can be employed for candidate selection and vote casting.

Data encryption is a pivotal aspect of the system's security. The Microcontroller encrypts each vote before securely storing it. Subsequently, the encrypted votes are transmitted to a central server for tallying and analysis.

Power is supplied to the circuit via a 5V source. This power supply is connected to the VCC and GND pins of the Raspberry Pi, ensuring continuous operation of the integrated system.

Overall, this integrated system, centered around a Raspberry Pi microcontroller, ensures a robust and streamlined electronic voting process. By managing authentication, ballot display, data encryption, and transmission, it guarantees the integrity and efficiency of the electoral process. The delineation of GPIO connections provides clarity on the circuit configuration, elucidating the role of each component in facilitating a secure and user-friendly voting experience.

EHICAL CONSIDERATIONS

The development and implementation of an electronic voting system incorporating facial recognition, Aadhar integration, and secure entry control through a servo motor necessitate careful consideration of various ethical aspects. Privacy is a paramount concern, particularly in the context of facial recognition technology accessing individuals' biometric data. Safeguards must be in place to ensure that facial images are used solely for voter identification and are securely stored and managed, mitigating the risk of unauthorized access or misuse. Integrating Aadhar data raises ethical concerns related to consent, as individuals' personal information is linked to voting records. Transparent communication and obtaining explicit consent for the use of Aadhar data are imperative to uphold ethical standards. Additionally, ensuring the security and integrity of the entire system is crucial to prevent tampering or unauthorized access to the voting process. Ethical considerations also extend to the accessibility of the system, ensuring it accommodates all voters, regardless of technological proficiency or disabilities. Striking a balance between technological innovation and ethical responsibility is essential to build public trust and uphold the integrity of the democratic process.

CONCLUSION AND FUTURE TRENDS

The introduced voting system leveraging Raspberry Pi, iris data, Aadhar ID verification, and QR code isolation marks a significant step towards a secure and user-friendly electoral process. The incorporation of iris scan technology enhances authentication, ensuring a robust and reliable voter identification system. The integration of Aadhar ID adds an additional layer of validation. The use of QR codes for isolated room setup not only minimizes the risk of tampering but also enhances the overall transparency of the voting process. As technology evolves, continuous improvements in biometric authentication methods, including iris scanning, may further enhance the system's security and accuracy. Exploring the integration of blockchain technology could provide an immutable and transparent ledger for storing voting records, adding an extra layer of security and ensuring the integrity of the electoral process. With the increasing use of smartphones, future systems could explore mobile-based voting solutions, enabling convenient and accessible participation in the electoral process. Implementing machine learning algorithms could help detect and prevent fraudulent activities, ensuring the system remains resilient against evolving security threats also the consideration for accessibility features to accommodate a diverse range of voters, including those with disabilities, could be a key aspect for future enhancements.

In summary, the proposed voting system lays the foundation for a secure and user-friendly electoral process, and future trends may focus on leveraging emerging technologies to further enhance security, transparency, and accessibility in the voting system.

REFERENCES

1. M. -V. Vladucu, Z. Dong, J. Medina and R. Rojas-Cessa, ”E-Voting Meets Blockchain: A Survey,” in IEEE Access, vol. 11, pp. 23293-23308, 2023, doi: 10.1109/ACCESS.2023.3253682.
2. Rahil Rezwan, Huzaifa Ahmed, M.R.N.Biplop ”Biometrically secured electronic voting system,” in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 36, no. 6, pp. 1120-1133, June 2014, doi: 10.1109/TPAMI.2013.234.
3. A. C. Weaver, ”Biometric authentication,” in Computer, vol. 39, no. 2, pp. 96-97, Feb. 2006, doi: 10.1109/MC.2006.47.
4. P.Sreekala, V.Jose, J.Joseph, ”Human embedded system and its application insecurity system of car,” 2017 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA), Poznan, Poland, 2017, pp. 263-268, doi:

5. A.M.Jagtap, V.Kesarkar and A.Supekar "EVM using biometrics, raspberry Pi and TFT module," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 21-30, Jan. 2004, doi: 10.1109/TCSVT.2003.818350.
6. S. Kulshrestha and S. Sachdeva, "Performance comparison for data storage - Db4o and MySQL databases," 2014 Seventh International Conference on Contemporary Computing (IC3), Noida, India, 2014, pp. 166-170, doi: 10.1109/IC3.2014.6897167.
7. A. Jamkar, O. Kulkarni, A. Salunke and A. Pljonkin, "Biometric Voting Machine Based on Fingerprint Scanner and Arduino," 2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT), Jaipur, India, 2019, pp. 322-326, doi: 10.1109/ICCT46177.2019.8969034..
8. Z. Kunik, A. Bykowski, T. Marciniak and A. Dabrowski, ”Raspberry Pi based complete embedded system for iris recognition," 2017 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA), Poznan, Poland, 2017, pp. 263-268, doi:
9. J. Daugman, "How iris recognition works," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 21-30, Jan. 2004, doi: 10.1109/TCSVT.2003.818350.
10. Daugman JG: High confidence visual recognition of persons by a test of statistical independence. IEEE Transactions on Pattern Analysis and Machine Intelligence 1993, 15(11):1148-1161. 10.1109/34.244
11. Ives R.W., Bonney B.L., Etter D.M., Effect of Image Compression on Iris Recognition, IMTC 2005 – Instrumentation and Measurement Technology Conference, Ottawa, Canada, 2005.
12. Marciniak, T., Dąbrowski, A., Chmielewska, A., Krzykowska, A., Selection of parameters in iris recognition system, Multimedia Tools And Applications, January 2014, Volume 68, Issue 1, pp 193–208.
13. F. R. G. Cruz et al., "Iris Recognition using Daugman algorithm on Raspberry Pi," 2016 IEEE Region 10 Conference (TENCON), Singapore, 2016, pp. 2126-2129, doi: 10.1109/TENCON.2016.7848401.
14. Ives R.W., Bonney B.L., Etter D.M., Effect of Image Compression on Iris Recognition, IMTC 2005 – Instrumentation and Measurement Technology Conference, Ottawa, Canada, 2005.
15. Marciniak, T., Dąbrowski, A., Chmielewska, A., Krzykowska, A., Selection of parameters in iris recognition system, Multimedia Tools And Applications, January 2014, Volume 68, Issue 1, pp 193–208.