JCMM Journal of Computers, Mechanical and Management
Journal homepage: www.jcmm.co.in e-ISSN: 3009-075X
AAN PUBLISHING

Volume 2 Issue 3

Article Number: 23065

Enhancing Voting Security and Efficiency: An Electronic Voting Machine (EVM) System Integrated With Biometric Identifiers

Nikhil Ranjan [*]

Department of Computer Science Engineering, Galgotia University, Greater Noida, Uttar pradesh, India 201308

Abstract

This study explores developing and implementing a novel Electronic Voting Machine (EVM) system integrated with biometric identifiers to enhance voting security and efficiency significantly. Traditionally, voting processes relied on paper ballots, a system fraught with several challenges, including over-voting, the loss or misplacement of ballot papers, environmental harm due to paper consumption, and a lengthy result compilation process. An advanced EVM system is proposed to address these issues, leveraging unique biometric identifiers - facial recognition and fingerprints - for voter authentication and secure vote recording. Our EVM system effectively improves the security against bogus voting and vote repetition, which have been significant concerns in previous voting systems. This robust approach to voter authentication minimizes the likelihood of voting fraud, thus contributing to a more reliable and secure voting process. However, the transition to this advanced EVM system is challenging. The study identifies key implications, including the impact on employment due to automation, potential inaccuracies and biases associated with biometric technologies, and vital privacy concerns surrounding using sensitive biometric data. Despite these challenges, the proposed system provides a substantial foundation for future enhancements. Opportunities for further development include the integration of additional biometric identifiers like iris recognition, refining the accuracy of current biometric technologies, and strengthening data privacy measures.

Keywords: Electronic Voting Machines; Biometric Identifiers; Voting Security; Facial Recognition; Fingerprint Authentication

1 Introduction

Voting, in its most fundamental sense, is a means to express choice or preference from an array of options. It forms the backbone of democratic processes worldwide, deciding the leaders the populace entrusts with power [1, 2]. This fundamental democratic process has undergone various transformations throughout history, from traditional paper ballots to more advanced Electronic voting machines (EVMs). However, the shift from traditional paper ballot voting to EVMs has not been without challenges and consequences [3–6]. Originally, the voting process involved the physical presence of each voter, the use of ballot papers, and manual counting – a method proven to be time-consuming and prone to inaccuracies and manipulation. Issues such as over-voting, where voters accidentally stamp more than once, and ballot papers being lost or miscalculated were significant challenges. These systemic problems, compounded with the environmental concerns around using paper, underscored the need for a more efficient and secure voting mechanism, hence the adoption of EVMs [4, 7, 8]. Designed and developed in India, in collaboration with Bharat Electronics Limited, Bangalore, and Electronics Corporation of India Limited, Hyderabad, EVMs promised to alleviate many of these challenges.

[*] Corresponding author: nrcs008@gmail.com

Received: 06 July 2023; **Revised:** 14 July 2023; **Accepted:** 29 July 2023; **Published:** 31 August 2023

DOI: 10.57159/gadl.jcmm.2.3.23065.

Offering advantages such as efficient vote recording, quick result processing, enhanced voter-friendliness, and a reduction in the use of paper, EVMs marked a significant evolution in voting technology. However, adopting EVMs has also raised concerns [9–15]. The transition to an electronic voting system has reduced the need for manpower, potentially affecting employment during elections. Furthermore, questions about the security and integrity of the voting process in an electronic format remain. The present work aims to address these concerns and refine the current EVM system, utilizing biometric identifiers to strengthen security and integrity. By proposing the unique physical attributes of voters, such as facial recognition and fingerprint data, the study aims to establish an unhackable, accessible, and more reliable voting system. This paper details the methodology, discusses the outcomes and implications of the proposed system, and outlines future avenues for improving upon this novel application of biometric technology in voting systems.

2 Methods

The methodology of the proposed EVM system encompasses the use of biometric identifiers, namely facial recognition and fingerprint data, for enhanced security and reliability. The study aims to develop an unhackable voting system, reducing the instances of bogus voting and vote repetition.

2.1 Hardware and software requirements

The proposed EVM system requires the integration of specific hardware and software components. The hardware components included a fingerprint sensor for fingerprint-based authentication, an EVM controller, a global system for mobile communications (GSM) module, and a webcam for facial recognition. The chosen software for the proposed system was MATLAB 13 by MathWorks, which proved excellent in managing and processing biometric data [15, 16].

2.2 EVM architecture

The proposed EVM architecture comprises two main units - the ballot unit (BU) and the control unit (CU). The BU is operated by the voter and is placed in the election booth. It displays the voter's name, OTP, date, time, candidate party name, party symbols, submit buttons, and various buttons labeled with the party name. The CU, used by poll workers, is responsible for storing votes and controlling the polling process. Its functionalities are accessible only after a secure admin login, post which it offers access to the result of the voting, the EVM result, reset functions and the voter login panel. Figure 1 represents the block diagram of the proposed EVM architecture, illustrating the interaction between the BU and CU.

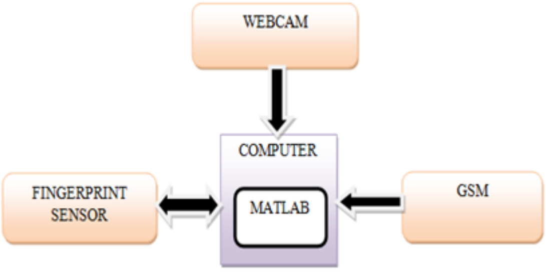


Figure 1: Block diagram of the proposed EVM architecture.

2.3 Biometric identifiers

The proposed EVM system leverages biometric identifiers for secure voter authentication. These identifiers are divided into two categories - physical and behavioral. The physical category includes face and fingerprint detection, while the behavioral category incorporates signature and voice detection. These identifiers provide a secure layer of verification, given their uniqueness to each individual [17–19]. In the proposed system, physical identifiers are used. The fingerprint detection technology uses the unique ridge and furrow patterns present on every individual's fingerprint [20, 21]. This uniqueness, coupled with the fact that fingerprints remain the same throughout an individual's life, makes them an effective tool for identification [22]. Figure 2 depicts a general fingerprint pattern that serves as a reliable biometric identifier. Face recognition, also known as automatic face recognition (AFR), uses the distinctive features of an individual's face for identification. This technology has advanced significantly and has numerous applications, such as personal identification and security systems [23, 24]. Combining these biometric technologies provides an enhanced security layer, facilitating a more secure and efficient voting process. However, it is worth noting that these technologies are not without their challenges and potential biases, which need to be continually addressed and improved upon to ensure an inclusive and accessible voting system.

Figure 2: A general fingerprint pattern of ridges and furrows.

3 Results

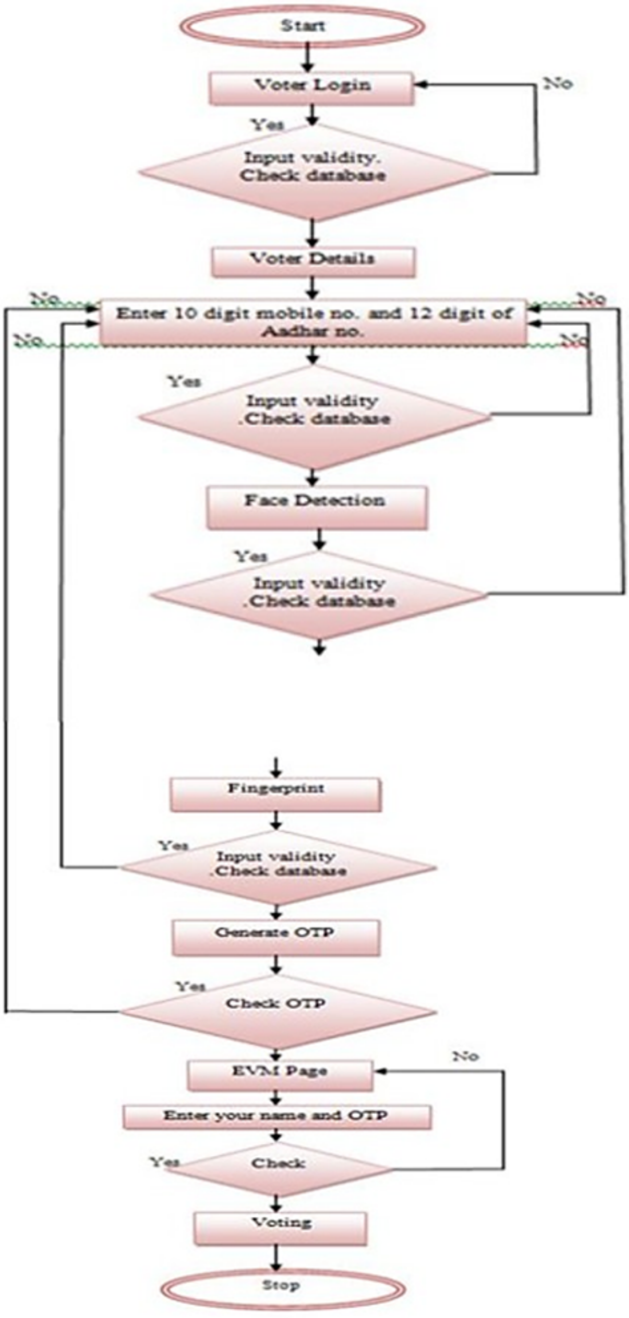


Figure 3: Flowchart of the proposed voting process

Implementing the proposed system resulted in marked improvements in security, efficiency and accessibility. Integrating biometric technologies with the EVM system enhanced the system's security against bogus voting and vote repetition. The system's process begins with the voter logging in. The voter is then prompted to enter their mobile and Aadhaar numbers, which must match the pre-stored information in the database. Once this step is completed, the system captures an image of the voter using the webcam. This image is then matched with the picture available in the database. Simultaneously, the voter's fingerprint is captured using the fingerprint sensor integrated into the EVM. The system matches this fingerprint with the data linked to the voter's Aadhaar number in the database. In cases where both image and fingerprint match the database records, the system generates a one-time password (OTP) sent to the voter's registered mobile number linked with their Aadhaar card. Following this, the voter enters the OTP, allowing them to cast their vote. Introducing fingerprint verification alongside facial recognition provides an additional layer of security to the voting process. It ensures a higher level of authenticity and prevents any potential identity fraud. Figure 3 depicts the flowchart of the proposed voting process, and Figure 4 represents the screen snapshot detailing each step from voter authentication to vote submission.

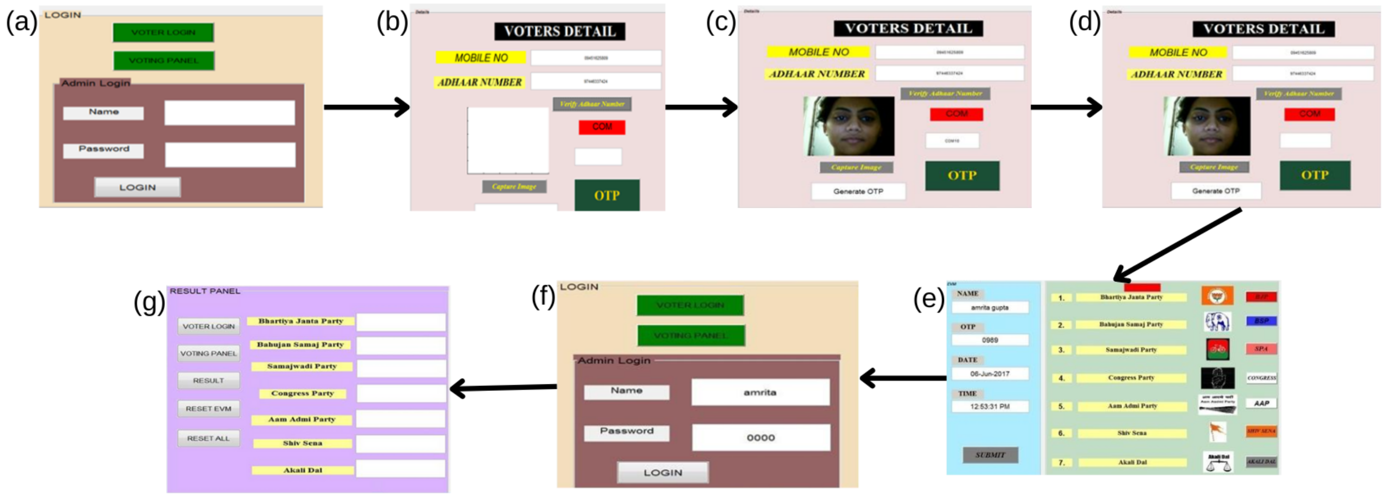
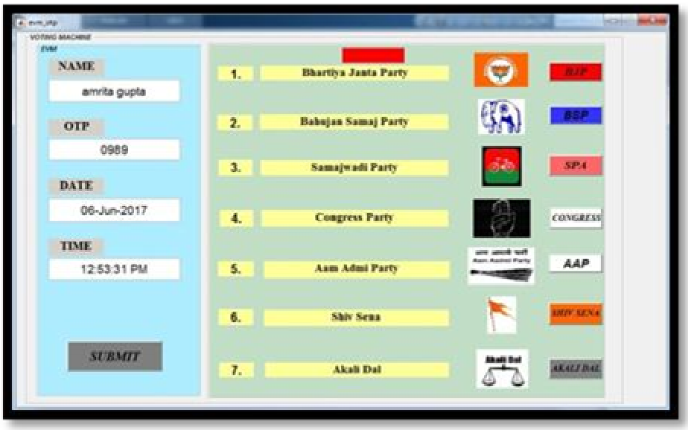


Figure 4: Flow process sequence: **(a)** Voter login interface; **(a)** Voter detail input page **(c)** Image capture and verification **(d)** COM Port Entry Stage **(e)** OTP verification and vote submission **(f)** Admin login stage **(g)** Result panel interface

Several key improvements became evident while comparing this implementation with the previous paper-based system:

- **Enhanced security**: Biometric identifiers substantially increased the voting process's security.
- **No misplacement**: Unlike ballot papers that could be lost or misplaced, votes can be securely stored in the EVM database.
- **Single-user single-vote**: The system ensures voters can vote only once, thus eliminating over-voting issues.
- **Accessibility for handicapped individuals**: The facial recognition feature allows physically challenged individuals to participate seamlessly in voting.
- **Efficiency**: The time consumed in the voting process can significantly reduce compared to the traditional ballot paper-based system.
- **Data recollection and recording**: The EVM system enables consistent and speedy recall and recording of voting data, which was not feasible with the previous system.

Regarding the EVM system's architecture, it was observed that the separation of functionalities into the BU and the Control CU streamlined the voting process. The BU, accessible to the voter, provided a user-friendly interface to cast their vote. Figure 5 depicts the proposed ballot unit having the user interface for the voter with the listed elements. The CU, operated by the poll workers, securely stored the votes and controlled the polling process. This architecture also allowed for real-time vote tallying, making the result compilation process faster and more efficient. Figure 6 represents the proposed control unit, highlighting the various functionalities available to the poll workers.



NAME: amrita gupta

OTP: 0989

DATE: 06-Jun-2017

TIME: 12:53:31 PM

1. Bhartiya Janta Party
2. Bahujan Samaj Party
3. Samajwadi Party
4. Congress Party
5. Aam Admi Party
6. Shiv Sena
7. Akali Dal

Figure 5: Proposed ballot unit.

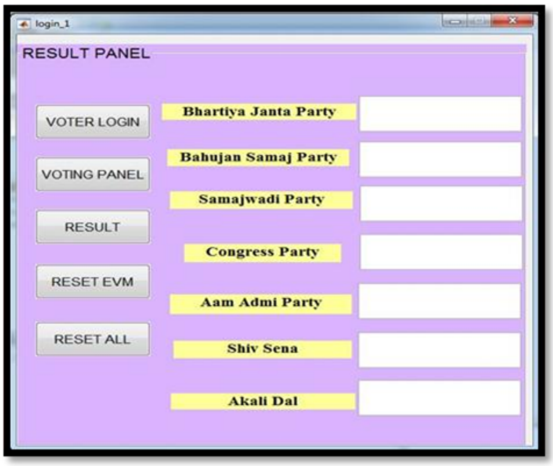


Figure 6: Proposed control unit.

4 Discussion

The present work has primarily focused on enhancing the security and efficiency of the voting process by incorporating biometric technologies into the EVM system. Using unique biometric identifiers such as facial recognition and fingerprints has shown a substantial improvement in the system's security against vote repetition and false voting, two significant issues with previous voting methods. While the shift from traditional paper ballots to EVMs has reduced many systemic problems, including over-voting and lost ballot papers, it has brought forth its own challenges. One such concern revolves around the reduction of manpower. As EVMs automate many tasks previously performed by humans, employment is impacted during elections. This concern is substantial and needs to be addressed in the context of technological progress, where automation is often seen as a job killer. Potential solutions might involve the re-skilling of workers or their integration into different stages of the election process where human intervention is still essential.

Additionally, while biometric identifiers have improved the security and efficiency of the voting process, their use is not devoid of potential inaccuracies and biases. These technologies must be continually refined to prevent false rejections or acceptances and ensure they do not unfairly favor or disadvantage any particular group of voters. Privacy concerns must also be considered, as biometric data is sensitive personal information. Moreover, the proposed system's success hinges upon the matching of voter details with a pre-existing database, a process that may encounter discrepancies or mismatches. Safeguards must address situations where valid voters cannot match their details, ensuring they are not denied their fundamental right to vote. As the system stands now, it significantly improves the voting process's security and efficiency. However, given the continuous advancement in biometric technology and the existing room for improvement, future enhancements could include more robust security features and the integration of additional biometric identifiers like iris recognition for more secure polling. It is also important to consider the technical and infrastructural challenges that come with the implementation of such an advanced system. Not all regions or voting demographics may have equal access to the technology required for EVMs, potentially leading to disparities in voting accessibility. Future work must make the technology universally accessible, ensuring no voter is left behind in the shift toward a more advanced voting process.

5 Conclusion

The exploration and implementation of an electronic voting machine (EVM) system equipped with biometric identifiers have presented a new paradigm in the evolution of voting processes. The present work has shown that integrating unique biometric features like facial recognition and fingerprints into EVMs greatly enhances the system's security against bogus voting and vote repetition, thus making the voting process more reliable and secure. The adoption of EVMs has helped eliminate many of the issues associated with traditional paper-based systems, such as over-voting, loss of ballot papers, and environmental concerns around the use of paper. In addition, using EVMs has led to significant improvements in the efficiency of the voting process, with real-time vote tallying and quick result compilation. However, as we acknowledge the advancements and improvements made, we also recognize the challenges and implications this shift entails. Concerns over the impact on employment due to reduced manpower and potential discrepancies in voter database matching are significant and require further attention. Moreover, using biometric identifiers while enhancing security opens discussions around potential inaccuracies, biases, and privacy concerns. Looking forward, the system presents considerable scope for further enhancement. Security could be bolstered through more robust measures and the integration of additional biometric identifiers, such as iris recognition.

Efforts should also focus on addressing the employment concerns raised by the adoption of EVMs and ensuring the universal accessibility of the technology, irrespective of regional or demographic disparities. In conclusion, while the proposed EVM system offers a substantial leap in the right direction, it is a continuous process of evolution and improvement to meet emerging challenges and ensure a secure, efficient, and inclusive voting process.

Declaration of Competing Interests

The author declares that he has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding Declaration

This research did not receive any grants from governmental, private, or nonprofit funding bodies.

Author Contribution

Nikhil Ranjan: Conceptualization, Methodology, Investigation, Visualization, Software, Writing - original draft, Writing - review and editing.

References

[1] M. Khosla, "The possibility of modern India," *Global Intellectual History*, 2021.

[2] A. Shah, "What if We Selected our Leaders by Lottery? Democracy by Sortition, Liberal Elections and Communist Revolutionaries," *Development and Change*, vol. 52, no. 4, pp. 687–728, 2021.

[3] A. Kud, "Decentralized Information Platforms in Public Governance: Reconstruction of the Modern Democracy or Comfort Blinding?," *International Journal of Public Administration*, vol. 46, no. 3, pp. 195–221, 2023.

[4] D. Pawade, A. Sakhapara, A. Badgujar, D. Adepu, and M. Andrade, "Secure Online Voting System Using Biometric and Blockchain," *Advances in Intelligent Systems and Computing*, vol. 1042, pp. 93–110, 2020.

[5] T. M. A. Elven and S. A. Al-Muqorrobin, "Consolidating Indonesia's Fragile Elections Through E-Voting: Lessons Learned from India and the Philippines," *Indonesian Comparative Law Review*, vol. 3, no. 1, pp. 63–80, 2021.

[6] S. Agarwal, A. Haider, A. Jamwal, P. Dev, and R. Chandel, "Biometric based secured remote electronic voting system," *2020 7th International Conference on Smart Structures and Systems, ICSSS 2020*, 2020.

[7] A. Olumide, B. Olutayo, and S. Adekunle, "A Review of Electronic Voting Systems: Strategy for a Novel," *International Journal of Information Engineering and Electronic Business*, vol. 12, no. 1, pp. 19–29, 2020.

[8] A. K. Tyagi, T. F. Fernandez, and S. U. Aswathy, "Blockchain and Aadhaar based Electronic Voting System," *Proceedings of the 4th International Conference on Electronics, Communication and Aerospace Technology, ICECA 2020*, pp. 498–504, 2020.

[9] A. Shankar, P. Pandiaraja, K. Sumathi, T. Stephan, and P. Sharma, “Privacy preserving E-voting cloud system based on ID based encryption,” *Peer-to-Peer Networking and Applications*, vol. 14, pp. 2399–2409, jul 2021.

[10] S. Risnanto, Y. B. A. Rahim, N. S. Herman, and A. Abdurrohman, “E-Voting readiness mapping for general election implementation,” *Journal of Theoretical and Applied Information Technology*, vol. 98, no. 20, pp. 3280–3290, 2020.

[11] Z. Desai and A. Lee, “Technology and protest: the political effects of electronic voting in India,” *Political Science Research and Methods*, vol. 9, pp. 398–413, apr 2021.

[12] Y. B. Hamdan and A. Sathesh, “Construction of Efficient Smart Voting Machine with Liveness Detection Module,” *Journal of Innovative Image Processing*, vol. 3, no. 3, pp. 255–268, 2021.

[13] A. C. Sheela and G. F. Ramya, “E-voting system using homomorphic encryption technique,” *Journal of Physics: Conference Series*, vol. 1770, no. 1, 2021.

[14] I. Arora, “Election Commission of India: Institutionalising Democratic Uncertainties,” *Asian Affairs*, vol. 52, no. 1, pp. 228–230, 2021.

[15] K. A. Alnajjar and O. Hegy, “Attendance System Based on Biometrics and RFID,” in *2019 Fifth International Conference on Image Information Processing (ICIIP)*, vol. 2019-Novem, pp. 596–599, IEEE, nov 2019.

[16] S. Jabin, S. Ahmad, S. Mishra, and F. J. Zareen, “iSignDB: A database for smartphone signature biometrics,” *Data in Brief*, vol. 33, p. 106597, dec 2020.

[17] J. Mason, R. Dave, P. Chatterjee, I. Graham-Allen, A. Esterline, and K. Roy, “An Investigation of Biometric Authentication in the Healthcare Environment,” *Array*, vol. 8, p. 100042, dec 2020.

[18] S. M. J. Amali, M. D. C., and R. G., “Evolution of Deep Learning for Biometric Identification and Recognition,” in *Handbook of Research on Computer Vision and Image Processing in the Deep Learning Era*, pp. 147–160, oct 2022.

[19] S. Dargan and M. Kumar, “A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities,” *Expert Systems with Applications*, vol. 143, p. 113114, apr 2020.

[20] M. A. Bhimrao and B. Gupta, “An empirical study of dermatoglyphics fingerprint pattern classification for human behavior analysis,” *Social Network Analysis and Mining*, vol. 13, p. 79, apr 2023.

[21] J. K. Appati, P. K. Nartey, E. Owusu, and I. W. Denwar, “Implementation of a Transform-Minutiae Fusion-Based Model for Fingerprint Recognition,” *International Journal of Mathematics and Mathematical Sciences*, vol. 2021, pp. 1–12, mar 2021.

[22] N. Kaushal and P. Kaushal, “Human Identification and Fingerprints: A Review,” *Journal of Biometrics and Biostatistics*, vol. 02, no. 04, 2011.

[23] R. S. Ghiass, O. Arandjelovic, H. Bendada, and X. Maldague, “Infrared face recognition: A literature review,” in *The 2013 International Joint Conference on Neural Networks (IJCNN)*, pp. 1–10, IEEE, aug 2013.

[24] Y. Kortli, M. Jridi, A. Al Falou, and M. Atri, “Face Recognition Systems: A Survey,” *Sensors*, vol. 20, p. 342, jan 2020.