International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6136
***Article Received**: 20 December 2022 **Revised**: 10 January 2023 **Accepted**: 27 January 2023*

Role of Digitalization in Election Voting Through Industry 4.0 Enabling Technologies

Musheer Vaqur[1], Rajesh Kumar[2], Rajesh Singh[1,3], Umang[4], Anita Gehlot[1,3], Shaik Vaseem Akram[1*], Kapil Joshi[1]
[1]Uttaranchal Institute of Technology,
Uttaranchal University, Dehradun, 248007, India
musheervaqur@uttaranchaluniversity.ac.in;
drrajeshsingh004@gmail.com; dranitagehlot@gmail.com;
vaseemakram5491@gmail.com*; kapilengg0509@gmail.com
[2]Meerut Institute Of Technology, Meerut, 250103, India.
rajesh.Kumar1 @mitmeerut.ac.in
[3]Department of Project Management, Universidad Internacional Iberoamericana, Campeche 24560, CP, Mexico
[4]Department of computer applications, D.S.B campus kumaun University Nainital, 263002, India.
Anilumang@yahoo.co.in

Abstract— The election voting system is one of the essential pillars of democracy to elect the representative for ruling the country. In the election voting system, there are multiple areas such as detection of fake voters, illegal activities for fake voting, booth capturing, ballot monitoring, etc., in which Industry 4.0 can be adopted for the application of real-time monitoring, intelligent detection, enhancing security and transparency of voting and other data during the voting. According to previous research, there are no studies that have presented the significance of industry 4.0 technologies for improving the electronic voting system from a sustainability standpoint. To overcome the research gap, this study aims to present literature about Industry 4.0 technologies on the election voting system. We examined individual industry enabling technologies such as blockchain, artificial intelligence (AI), cloud computing, and the Internet of Things (IoT) that have the potential to strengthen the infrastructure of the election voting system. Based upon the analysis, the study has discussed and recommended suggestions for the future scope such as: IoT and cloud computing-based automatic systems for the detection of fake voters and updating voter attendance after the verification of the voter identity; AI-based illegal, and fake voting activities detection through vision node; blockchain-inspired system for the data integrity in between voter and election commission and robotic assistance system for guiding the voter and also for detecting disputes in the premises of election booth.

Keywords- Election voting; blockchain; IoT; Artificial intelligence; cloud computing; industry 4.0.

I. INTRODUCTION

Election is the process that is the backbone any democratic country through which leaders are chosen by the people among the competing candidates through paper ballots or E-voting to brings desired societal changes. Especially in biodiversity country like India it is very sensitive. Electoral processes are critical because they enable voters to influence the potential future policies of elected governments. Voter_ registration, voter verifications, polling, counting, information broadcasting, and result posting are essential part of the electoral process [1]. The Indian Election Commission adopted digital Electronic Voting Machines (EVM) for the Parliament election on the theme of digital India in 2014. This traditional election system required massive administration staff and polling re-sources as shown in figure 1.

Rapid developments in information technology with 5G have accelerated great enhancement in adopting the new generation of technology, resulting in the creation of Industry 4.0. Such technologies emerge from a variety of fields, incorporating enterprise architecture, industrial information integration with IoT, business management process, cloud computing [2]. Understanding Industry 4.0, which emphasizes automation with minimal manpower involvement, is crucial. Sensors, actuators, digital verification, and communication between them would allow the entire election process to take place without human intervention. the idea of industry 4.0 leads to automate system with minimum manpower.

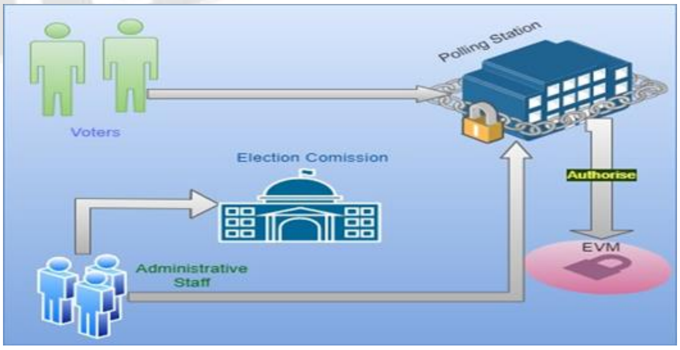

Fig. 1: Traditional voting process.

A secure mobile Internet voting architecture is proposed, which is based on the NFC technique, the internet, mobile devices, GPS location services, and speech biometric security [3]. Voting via the internet from any remote location in the world is made possible by the implementation of a secure e-voting application with Azure Service Fabric and micro service architecture [4]. Creating an e-voting system that ensures verifiability, anonymity and openness is a difficult job. Blockchain is a technology capable of constructing transparent and decentralized networks that ensure only authorized voters can vote through the use of Enigma-based smart contracts [5]. The entire voting process takes place autonomously without human intervention through Industry 4.0 technologies, sensors, actuators and various forms of communication between them. From the above aspects, it is concluded the integration of industry 4.0 enabling technologies plays a vital role in enhancing the infrastructure and connectivity of different elements of electronic voting system on virtual world with sustainability. The researchers have individually covered the implementation of blockchain, AI, and IoT technology for electronic voting in previous studies. As a result, there is a need for research that can present the application and implementation of all of these technologies in a single article to assist academicians in obtaining scientific information that will be useful for future research work. The contribution of the study is as follows:

- The study discussed the overview of election voting system with inclination towards to the industry 4.0 technologies.
- The integration of industry 4.0 technologies such as blockchain, AI, cloud computing, and the IoT for election voting system are detailed presented with architecture.
- Finally, the study made significant recommendations for the wide deployment of Industry 4.0 for automating election voting with intelligence, real-time monitoring, and security.

Section 2 addresses the overview of voting system and industry 4.0; Section3 covers contribution of IoT, cloud computing, blockchain, and Machine Learning & Artificial Intelligence in electronic election voting system. Section 4 presents the recommendations for future work.

II. Overview of Election voting system and Industry 4.0

The paper-based polling method accelerated people 's credibility in the dominant voting process. It has contributed to the democratisation of the electoral system and democratic procedure for electing governments. In 2018, 167 nations have democracy, out of around 200 that are either completely faulty or hybrid [6]. The secret voting model has been employed to boost trust in democratic institutions ever since commencement of the system of voting. A recent study revealed that the conventional voting procedure raising various questions, including fair-ness, equality, and the desire of the people [7]. Recent electronic voting methods and approaches [8] are crucial and have posed substantial difficulties to the democratic system [9]. Compared to traditional voting methods, it has improved both the integrity and efficiency of the process. Along with this there are problems in the voting system such as lack of evidence for electoral fraud with the effect of bribes. They are no fraud resistance as the qualified voter needs to vote only once throughout the country and detect the fake voter. Along with this, there are chances of manipulating votes and creating violence for postponing the election. For this activity, the election system uses booth capturing through the cameras, however the intelligence needs to be integrated in the camera for detecting the illegal activities and suspicious activities.

Currently the adoption of Industry 4.0 revolution has transformed various applications with its advanced enabling technologies (Fig. 2). Industry 4.0 is termed as the fourth Industrial revolution, where the exchange of data and automation in between the manufacturing activities. Industry 4.0 is the amalgamation of various technologies including IoT, AI, big data analytics, AR/VR, blockchain [10], [11]. These are the key technologies that have driven industry 1.0 in various applications to industry 4.0 with automation. The interface between IoT and CPS enables communication between physical things and virtual networks through sensors and wireless communication.

a) IoT: IoT is the interconnection of physical things with a virtual world via Internet Protocol (IP) connectivity, and GSMA intelligence forecasts that there will be 25 billion IoT connections globally by 2025 [12]. IoT transforms conventional things into smart things by utilizing actuators and sensors that can track and act together on the Internet. IoT enables machine-to-machine communications by constantly accumulating data, recognizing relationships, and recommending solutions.

b) Cloud computing: In today's ever-changing environment, organisations must invest significantly in handling their on-premises IT infrastructures, such as software, hardware, and services, in order to meet the market's varying expectations [13]. Cloud computing technology provides compute and storage services by distributing IT infrastructure across the Internet to meet changing needs.

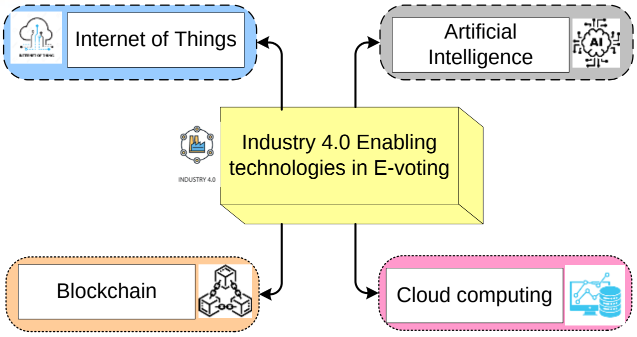

Fig. 2: Industry 4.0 enabling technologies for E-voting.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6136
***Article Received**: 20 December 2022 **Revised**: 10 January 2023 **Accepted**: 27 January 2023*

c) AI: AI is the study of parts of human behaviors in order to construct a specific intelligent system that will allow computers to do occupations that only humans could do in the past, and to reproduce the underlying using computer hardware and software. AI uses computers and technology to imitate the problem-solving and decision-making abilities of the human mind [14]. AI uses data to automate repetitive learning and discoveries. AI uses neural networks with numerous hidden layers to interpret more and deeper data.

d) Blockchain: A blockchain is a collection of blocks that is utilized to share and store data in a transparent, distributed, and tamper-proof manner. Blockchain 4.0 focuses on real-time services like public ledgers and distributed databases [15], and this tier effortlessly incorporates Industry 4.0 assisted apps. Its employs smart contracts, which eliminate the need for paper-based contracts the network by consensus.

III. IoT and Cloud Computing in Electronic Election Voting System

IoT plays a vital role in the developing county to automate the administrative task. IoT provides efficient and optimized add on services in order to address societal challenges. It's important to provide interoperability among different devices [16]. Protecting voter privacy, ensuring secrecy, anonymity, integrity, uniqueness, and legitimacy of votes, while making e-Voting as trustworthy as voting, remains the key challenges of e-Voting. a secure open-source e-voting system is introduced that uses cryptographic techniques to separate the both voter identification and voting phases [17]. The Election system is one of essential parts of democratic country that in-volves the several procedures. But these traditional procedure leads to massive manpower resources. Electronics voting machine can be control via Internet of Things (IoT) to automate the process of voting using biometrics that would reduce the time, expenses, and human resources, moreover it is more secure with the help of two step verification using OTP [18].

On one hand, remote e-voting provides easier access to voters, while on the other it makes it easier for election bodies to count votes and generate reports, but it required significant improvement in terms of security and integrity [19]. Aadhar card, fingerprint and facial recognition can be incorporated with voting machine and fetch data will be stored in the secure database [20]. The Aadhar card and voter id can be verified via fingerprint sensor and Node MCU ESP8266, to ensure the user's vote, MCU ESP8266 also display through Voter-verified paper audit trail (VVPAT) [21]. Against the voter card id RFID can be used with IoT so that system can scan the tag and match with the fingerprint that improvise the overall security [22]. To generate a trustworthy communication environment by separating the malicious IoT devices from the legal ones using social optimizer to compute their trust levels and to maintain the transparency all transaction is visible to election bodies at each level [23].

A decentralized multirole e-voting protocol over the cloud computing where each user independently shared, each subset of users creates a separate access structure and only shares a single target secret with a short secret share [24]. The E-Voting Cloud System (ECS) system verifies vote data via cloud computing and is highly secure with a cube data structure and a user differentiated system model that encrypts voter data using an encrypted model and ECSe [25]. Using a cloud computing infrastructure, electronic government services can become more sophisticated and inclusive. When looking at the election process and the digitalization of government transactions from the standpoint of information and communication security, a structured analysis is used to pinpoint weaknesses. This context-specific research also explores the concepts of trust and transparency [26].

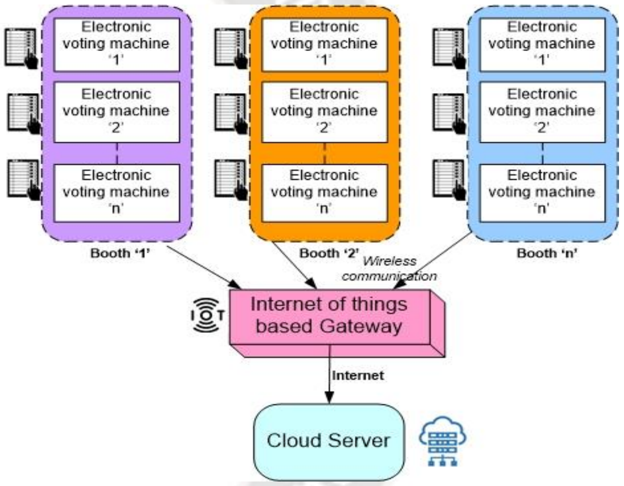
Electronic voting machine '1'
Electronic voting machine '2'
Electronic voting machine 'n'
Booth '1'
Booth '2'
Booth 'n'
Wireless communication
Internet of things based Gateway
Internet
Cloud Server

Fig. 3: IoT and cloud server-based Booth wise EVM monitoring system.

Fig. 3 illustrates an architecture that can be applied in the booth for monitoring the EVMs through wireless communication and IoT. Every election voting machine (EVM) is integrated with the controller unit and wireless communication protocol, the updating of every vote will be logged in the cloud server. Moreover, the controller unit can be updated through firmware, that is able to transmit the information regarding the malfunction of EVM. IoT based gateway in the architecture enables connecting the EVM to the cloud server via wireless communication and internet connectivity.

IV. Machine Learning & Artificial Intelligence in Voting

Machine learning performs a significant role in managing and automating the election. Cyber security techniques and AI pattern recognition for data decryption and encryption were used to assist the Independent National Electoral Commission (INEC) in resource allowance [27]. AI has generated AI technologies that aid political campaigns in achieving observable integrity inside their election cycles, hence increasing trust in the society institutions tasked with maintaining free, fair, and open election environments [28]. An AI-based early warning system that tracks the effects of online material manipulation, including changed images, violence conflict, and societal unrest in the real world so that election bodies can aware how fake content is spreading [29]. An important step toward perceptual user interfaces with autonomous perception of persons is the reliable detection of ordinary facial expressions despite individual variability and face appearances [30].

In general, fourteen cities in the United States use currently ranks option voting, as do six states for special elections and overseas ballots [31]. Ranked choice voting allies argue that it is more elected because it involves the victor to receive a popular vote [31], [32]. Proponents of this type of voting as well argue that it eradicates the demand for costly runoff polls because it confirms a contestant receives a greater part of the vote with only a single ballot. Critics contend that many municipalities lack the necessary infrastructure to execute this kind of voting [33], [34]. While modeling the impact of executing instant run-off polling in the 2016 presidential poll, analytical modelling is employed to establish exactly how votes would be divided up whenever a contestant is excluded.

V. Blockchain-Based E-Voting

A new form of electronic voting scheme has also been proposed with the development of emerging Blockchain technology. As technology improves it may lead to several security threats that required to be addressed. In order to identify and address the numerous hazards brought on by an intrusion at multiple levels, a safe and faire E-voting system integrated with digital devices and Blockchain technology is being adopted. Through the help of secure time stamp and three-layer of authentication OTP, QR codeshare and blockchain, voter can safely vote with the, and as hash-code identify malicious attack on the server [35]. A Blockchain is maintained in the linked blocks where all valid transactions are stored that guard against future alterations of data collected by smart devices in order to keeps the system transparent for every voter while giving better understanding to higher authorities [36]. Suggested design will be built on a blockchain-based secure system for electronic voting application, where users can create accounts and have their identity properly verified using voter identification number along with biometric techniques on a smart device [37]. A candidate can be verified with each transaction made through their registered account. Response time, resource use, and request processing are only a few of the characteristics used to assess and verify the given Blockchain system for electronic polling with smart devices [38]. All voters and independent observers have access to the voting records kept in these systems, the key complex problems, including integrity, consensus, and privacy are addressed by the blockchain [39]. SLR made it possible to identify patterns in the application of blockchain technology, planned use cases, testing procedures, are the key advantages, but maintaining the identity of the voters on the large scale is Still major issue [40].

Trust between election commission and voters is the main issue in any democratic country and that is the major cause of failure of tradition voting system [41]. The blockchain technology enables significant transparency, integrity, reliability, and Security Algorithm adopted in the electronic voting system to secure the voting transaction. By encrypting transactions using cryptographic hashes and preventing 51 percent of attacks on the blockchain, A node cannot be changed or deleted once it is added and if node is being attacked, the linked node recognized and reconstruct the faulty node while maintaining system the latency via flexible consensus algorithms [42]. Although self-tallying voting system is alternative solution for traditional IoT based decentralized system, it may lead some serious transparency issues caused by faulty voters. blockchain based self-tallying voting system decentralized framework that fulfils maximum securities requirement while maintaining the transparency [28]. An electronic voting protocol based on blockchain technology and self-tallying, that balance anonymity and accountability with full traceability of defaulter voter’s and at the same time, it optimizes computation efficiency, voting scale. And can be deployed practically in real world applications [43]. Blockchain electronic voting can reduce the risk of numerous security breaches, internal vote tampering, and increase accountability. Voter validity and blockchain architecture security are two potential flaws that will require a lot of attention. The architecture trade-off analysis method could be used to help electoral partners recognize the possible consequences, problems, and opportunities of blockchain in electoral polling through a participating architectural evaluation and docu-mentation process [39].

Blockchain technology may be able to deal with challenging problems facing in electoral processes. Privacy and transaction speed are the most frequent issues with legitimate, accurate, safe, and convenient blockchain applications [44]. Decentralized voting is recognized as the key idea that blockchain focuses on to make the right choice and provide an adequate level of security with IoT. A novel decentralised based on the Weighted Majority Consensus Algorithm (WMCA) is implemented to enhance the blockchain voting process in IoT [45], [46]. Secure large-scale E-voting system founded on blockchain contracts that uses distributed storage and a hybrid consensus model are utilised to create a safe computing environment and a reliable public bulletin [47].

***Article Received**: 20 December 2022 **Revised**: 10 January 2023 **Accepted**: 27 January 2023*

Designed and tested a sample e-voting application for the Ethereum network utilizing solidity programming language and Ethereum wallets. The Ethereum blockchain will store ballots and polling results. Voting requests are conducted with the consensus of all Ethereum nodes, and users can cast their votes actively from their Ethereum wallets [48]. An IoT embedded device with a decentralized e-voting implementation that provides thorough voter confidentiality and edge security for all involved parties in the electronic election system [49]. Data security is ensured by an adaptable blockchain framework using powerful hashing methods. Block creation and sealing as a concept makes the blockchain adaptable to meet the challenges of data management and security for the polling process [50]. An end to end (E2E) verifiable electronic voting system via voter's unique identification and bio-metric features provides mobility to a voter and allows to cast their vote from the remote location. Privacy and polling status using short signature Boneh-Lynn-Shacham scheme [51]. The implementation of blockchain for various purposes of voting. For detailed discussion, different parameters such as model, authentication, platform, voter verification, decentralized and blockchain type. From the table different models are implemented for voting and model named as permissioned blockchain, vote book, and bronco vote. In the majority study, it has been observed that the Ethereum blockchain is integrated for secure voting.

VI. Recommendation and Discussion

The traditional voting system consumed enormous time, massive resources, and human interventions. Different digital devices and technologies like smart sensor, biometric sensor, RFIDs, E-voter ID, Node MCU ESP8266, Arduino UNO, Raspberry pi e.tc. are incorporated with the IOT that automate the voting system. These innovative capable for solving complex conflict in validation and duplication of votes. Maintaining system transparency in order to gain the voter's trust is an intrinsic challenge in this digital era. These emerging technology leads to series privacy, integrity, authentication issues. There is a need for extensive research in order to address above stated issues so that E-voting techniques can be adopted on the real ground. IoT devices can be integrated with cloud computing and big data that enables the election commission identify conflict and take futuristic decision. Electronic services can be made more sophisticated and inclusive by utilizing a cloud computing infrastructure. A systematic analysis is utilized to identify vulnerabilities while examining the election process and the digitalization of government transactions from the perspective of information and communication security. During the election process besides of polling system number of challenges and conflict were faces like dispute, tempering of voting devices and spreading fake news.

The significant work has not been done yet in the area of e-voting with big data, cloud computing, and AI with ML. So, there is need to explore the insight e-voting system with stated technology. Although Blockchain Technology successful to controlling numerous hazards like integrity, transparency and security with these emerging techniques internet voting can be done at any location that increase the voting percentage and reduced time and massive resources consumed during the election. But in current scenario internet voting leads to complex conflict as voting can be manipulated or biased and administration not able to gain trust with political parties. A transparent, secure, trustworthy decentralized smart election mechanism is suggested that allows election bodies to conduct not only polling smoothly but also control stated conflict arises during election process. In order to manage election efficiently our suggested mechanism goes through several phases with different technology.

- We have suggested IoT and cloud computing-based systems that manage and control polling. The first stage is the initialization phase in which the election commission announces the date and related information regarding election and uploads the voting list on the server. On the day of polling, voters register themselves on the electronic voting machine (EVM). Three layers of Voter's authentication (as depicted in fig. 4) are done with the Aadhar card, fingerprint and retina scan.

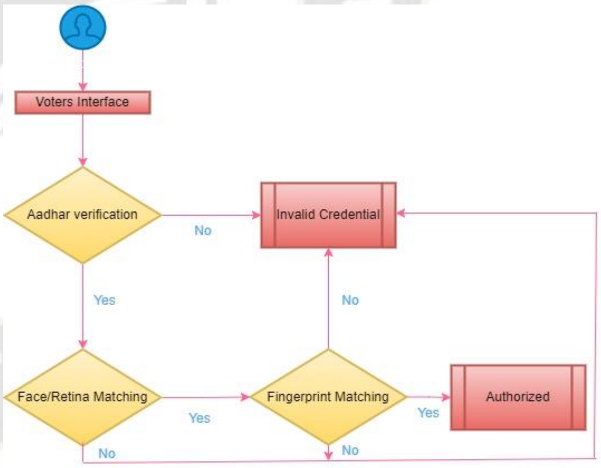

Fig. 4: Tree layer Authentication system

- This automated system fetches the data from voters via proposed device and map with the predefine dataset stored on the cloud. As highlighted in fig. 5, Once the voter's authorization is done, a unique token is generated, and voter's is applicable for the vote subsequently message will flush on screen and process get completed and id of voter will be blocked to avoid duplicity. All the voting transactions will be stored on the cloud for further processing.

DOI: https://doi.org/10.17762/ijritcc.v11i2.6136
***Article Received**: 20 December 2022 **Revised**: 10 January 2023 **Accepted**: 27 January 2023*

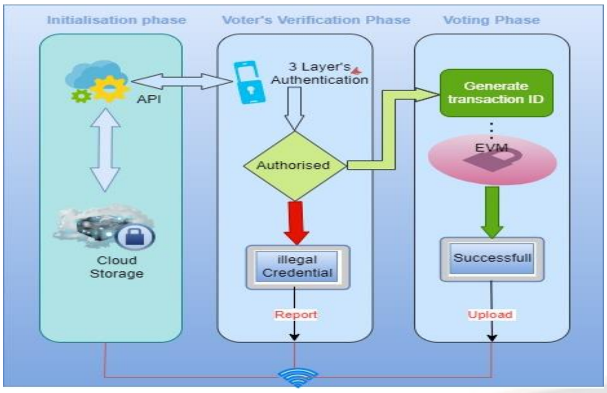

Fig. 5: IoT & Cloud Based voting system.

- During the election process besides of polling system number of challenges and conflict were faces like dispute, tampering of voting devices and spreading fake news. We need to surveillance polling booth and social media. The AI/ML model equipped with smart sensor and camera is suggested that analyses facial expressions, dispute or conflict on polling booth and report to controlling center for further action. An AI/ML-based early warning expert system track on social media that measures the impacts of online material modification in the real world, such as changing pictures, violence, conflict, and social discontent, so that electoral bodies are conscious.
- An interactive Robot assistant is deployed in premises of polling both that provides that is capable of communicating with the voter and provides basic information about registration and voting procedure. The robot connects with the suggested AI/ML model that generates voice alarm and inform to controlling center if illegal voting, tempering machine, and conducting misbehave or dispute.
- Emerging technology like Blockchain provides solutions to the main challenging issues like integrity, transparency and security. Making a trust and transparency between voter's and election commission is an intrinsic challenge in biodiverse country like India. A private blockchain will be integrated with the above suggested IoT and AI model as depicted in fig. 6. On the authentication of voter's unique id as per above stated system, a random number is generated with hashing algorithm. The voting transaction is stored along random numbers by using the SHA-256 hashing algorithm with the hash into the linked block chain in order to maintain the integrity of whole system.

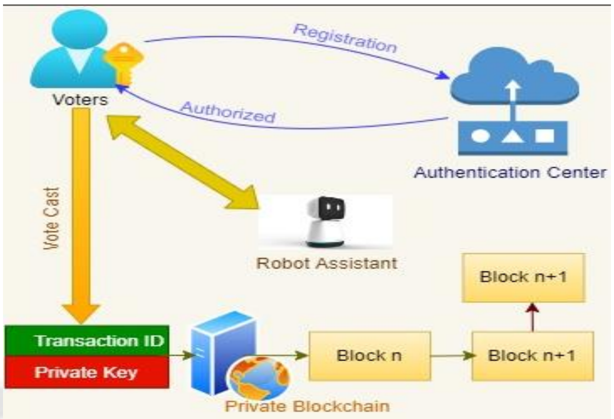

Fig. 6: Secure electronic voting system

VII. CONCLUSION

The election voting system is one of the essential pillars of democracy to elect the representative for ruling the country. The impact and usage of Industry 4.0 in the election voting system is yet to be explored. Based on these facts this study examined the integration of blockchain, AI, cloud computing, IoT, in the election voting system for real-time monitoring, intelligent detection, enhancing security and transparency of voting and other data during the voting. The study suggested few vital recommendations such as IoT and cloud computing-based automatic systems for the detection of fake voters and updating voter attendance after the verification of the voter identity; AI-based illegal, and fake voting activities detection through vision node; blockchain-inspired system for the data integrity in between voter and election commission and robotic assistance system for guiding the voter and for detecting disputes in the premises of election booth.

REFERENCES

[1] S. Yadav and A. K. Singh, "A biometric traits based authentication system for indian voting system," *Int. J. Comput. Appl.*, vol. 65, no. 15, pp. 28–32, 2013.

[2] L. Da Xu, E. L. Xu, and L. Li, "Industry 4.0: state of the art and future trends," *Int. J. Prod. Res.*, vol. 56, no. 8, pp. 2941–2962, 2018.

[3] S. Thakur, E. Adetiba, O. O. Olugbara, and R. Millham, "Experimentation using short-term spectral features for secure mobile internet voting authentication," *Math. Probl. Eng.*, vol. 2015, 2015.

[4] R. Johari, A. Kaur, M. Hashim, P. K. Rai, and K. Gupta, "SEVA: Secure E-Voting Application in Cyber Physical System," *Cyber-Physical Syst.*, vol. 8, no. 1, pp. 1–31, 2022.

[5] A. Fernandes, K. Garg, A. Agrawal, and A. Bhatia, "Decentralized online voting using blockchain and secret contracts," in *2021 International Conference on Information Networking (ICOIN)*, 2021, pp. 582–587.

[6] R. Cullen and C. Houghton, "Democracy online: an assessment of New Zealand government web sites," *Gov.*

Inf. Q., vol. 17, no. 3, pp. 243–267, 2000.

[7] C. Schinckus, “The good, the bad and the ugly: An overview of the sustainability of blockchain technology,” *Energy Res. Soc. Sci.*, vol. 69, p. 101614, 2020.

[8] R. Taş and Ö. Ö. Tanrıöver, “A manipulation prevention model for blockchain-based e-voting systems,” *Secur. Commun. Networks*, vol. 2021, 2021.

[9] L. Hang and D.-H. Kim, “Design and implementation of an integrated iot blockchain platform for sensing data integrity,” *Sensors*, vol. 19, no. 10, p. 2228, 2019.

[10] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, and M. Hoffmann, “Industry 4.0,” *Bus. Inf. Syst. Eng.*, vol. 6, pp. 239–242, 2014.

[11] M. Ghobakhloo, “Industry 4.0, digitization, and opportunities for sustainability,” *J. Clean. Prod.*, vol. 252, p. 119869, 2020, doi: 10.1016/j.jclepro.2019.119869.

[12] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, “Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios,” *Ieee Access*, vol. 8, pp. 23022–23040, 2020.

[13] J. W. Rittinghouse and J. F. Ransome, *Cloud computing: implementation, management, and security*. CRC press, 2017.

[14] M. Haenlein and A. Kaplan, “A brief history of artificial intelligence: On the past, present, and future of artificial intelligence,” *Calif. Manage. Rev.*, vol. 61, no. 4, pp. 5–14, 2019.

[15] U. Bodkhe *et al.*, “Blockchain for industry 4.0: A comprehensive review,” *IEEE Access*, vol. 8, pp. 79764–79800, 2020.

[16] R. Fooprateepsiri and W. Kurutach, “A fast and accurate face authentication method using hamming-trace transform combination,” *IETE Tech. Rev.*, vol. 27, no. 5, pp. 365–370, 2010.

[17] D. R. Ibrahim, J. Sen Teh, and R. Abdullah, “Multifactor authentication system based on color visual cryptography, facial recognition, and dragonfly optimization,” *Inf. Secur. J. A Glob. Perspect.*, vol. 30, no. 3, pp. 149–159, 2021.

[18] R. Krimmer, D. Duenas-Cid, and I. Krivonosova, “New methodology for calculating cost-efficiency of different ways of voting: is internet voting cheaper?,” *Public money Manag.*, vol. 41, no. 1, pp. 17–26, 2021.

[19] M. Kumar, S. Chand, and C. P. Katti, “A secure end-to-end verifiable internet-voting system using identity-based blind signature,” *IEEE Syst. J.*, vol. 14, no. 2, pp. 2032–2041, 2020.

[20] R. P. Prasad, S. K. N. Kumar, R. Gatti, M. Pranav, G. Rahul, and M. Yatheesh, “TOUCHLESS ELECTRONIC VOTING MACHINE WITH AN AI-FACIAL RECOGNITION,” in *2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT)*, 2021, pp. 951–955.

[21] B. Ahlgren, M. Hidell, and E. C.-H. Ngai, “Internet of things for smart cities: Interoperability and open data,” *IEEE Internet Comput.*, vol. 20, no. 6, pp. 52–56, 2016.

[22] V. Agate, A. De Paola, P. Ferraro, G. Lo Re, and M. Morana, “SecureBallot: A secure open source e-Voting system,” *J. Netw. Comput. Appl.*, vol. 191, p. 103165, 2021.

[23] B. Vignesh, P. P. Sricharan, S. Shankrith Chokkalingam, J. Bhuvana, and B. Bharathi, “E-Biometric Voting Machine,” in *Futuristic Communication and Network Technologies: Select Proceedings of VICFCNT 2020*, 2022, pp. 505–516.

[24] H. Alamleh and A. A. S. AlQahtani, “Analysis of the design requirements for remote Internet-based E-voting systems,” in *2021 IEEE World AI IoT Congress (AIIoT)*, 2021, pp. 386–390.

[25] K. Srikrishnaswetha, S. Kumar, and M. Rashid Mahmood, “A study on smart electronics voting machine using face recognition and aadhar verification with iot,” in *Innovations in Electronics and Communication Engineering: Proceedings of the 7th ICIECE 2018*, 2019, pp. 87–95.

[26] A. Gehlot, R. Singh, K. Rastogi, and J. Gupta, “Design and Development of Industrial Internet of Things-Based Polling Booth for Voting,” in *Advances in Industrial Safety: Select Proceedings of HSFEA 2018*, 2020, pp. 323–332.

[27] P. M. B. Mansingh, T. J. Titus, and V. S. S. Devi, “A secured biometric voting system using RFID linked with the Aadhar database,” in *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2020, pp. 1116–1119.

[28] G. Rathee, R. Iqbal, O. Waqar, and A. K. Bashir, “On the design and implementation of a blockchain enabled e-voting application within iot-oriented smart cities,” *IEEE Access*, vol. 9, pp. 34165–34176, 2021.

[29] J. Li, X. Wang, Z. Huang, L. Wang, and Y. Xiang, “Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing,” *J. Parallel Distrib. Comput.*, vol. 130, pp. 91–97, 2019.

[30] 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 Netw. Appl.*, vol. 14, pp. 2399–2409, 2021.

[31] C. M. Burnett and V. Kogan, “Ballot (and voter)‘exhaustion’ under Instant Runoff Voting: An examination of four ranked-choice elections,” *Elect. Stud.*, vol. 37, pp. 41–49, 2015.

[32] R. Richie, “Instant runoff voting: what Mexico (and others) could learn,” *Elect. Law J.*, vol. 3, no. 3, pp. 501–512, 2004.

[33] S. Bowler and D. M. Farrell, “Voter strategies under preferential electoral systems: a single transferable vote mock ballot survey of London voters,” *Br. Elections Parties Yearb.*, vol. 5, no. 1, pp. 14–31, 1995.

[34] P. Dunleavy, H. Margetts, and B. O’Duffy, *Making votes count: replaying the 1990s general elections under alternative electoral systems*. Democratic Audit of the United Kingdom, 1997.

[35] D. Zissis and D. Lekkas, “Securing e-Government and e-Voting with an open cloud computing architecture,” *Gov.*

Inf. Q., vol. 28, no. 2, pp. 239–251, 2011.

[36] H. Mora, J. C. Mendoza-Tello, E. G. Varela-Guzmán, and J. Szymanski, "Blockchain technologies to address smart city and society challenges," *Comput. Human Behav.*, vol. 122, p. 106854, 2021.

[37] E. Zaghloul, T. Li, and J. Ren, "d-BAME: distributed blockchain-based anonymous mobile electronic voting," *IEEE Internet Things J.*, vol. 8, no. 22, pp. 16585–16597, 2021.

[38] K. Lee, J. I. James, T. G. Ejeta, and H. J. Kim, "Electronic voting service using block-chain," *J. Digit. Forensics, Secur. Law*, vol. 11, no. 2, p. 8, 2016.

[39] R. Taş and Ö. Ö. Tanrıöver, "A systematic review of challenges and opportunities of blockchain for E-voting," *Symmetry (Basel).*, vol. 12, no. 8, p. 1328, 2020.

[40] U. Jafar, M. J. Ab Aziz, Z. Shukur, and H. A. Hussain, "A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems," *Sensors*, vol. 22, no. 19, p. 7585, 2022.

[41] S. Mozaffar and A. Schedler, "The comparative study of electoral governance—introduction," *Int. Polit. Sci. Rev.*, vol. 23, no. 1, pp. 5–27, 2002.

[42] G. Megala, P. Sevugan, and R. Venkatesan, "Blockchain-Based Secured Voting Using Multi-Level Authentication," in *Blockchain Technologies for Sustainable Development in Smart Cities*, IGI Global, 2022, pp. 187–195.

[43] R. Krishnamurthy, G. Rathee, and N. Jaglan, "An enhanced security mechanism through blockchain for E-polling/counting process using IoT devices," *Wirel. Networks*, vol. 26, no. 4, pp. 2391–2402, 2020.

[44] M. Pawlak and A. Poniszewska-Marańda, "Trends in blockchain-based electronic voting systems," *Inf. Process. Manag.*, vol. 58, no. 4, p. 102595, 2021.

[45] M. S. Farooq, U. Iftikhar, and A. Khelifi, "A framework to make voting system transparent using blockchain technology," *IEEE Access*, vol. 10, pp. 59959–59969, 2022.

[46] Y. Li *et al.*, "A blockchain-based self-tallying voting protocol in decentralized IoT," *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 1, pp. 119–130, 2020.

[47] H. Li, Y. Li, Y. Yu, B. Wang, and K. Chen, "A blockchain-based traceable self-tallying E-voting protocol in AI era," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1019–1032, 2020.

[48] O. Daramola and D. Thebus, "Architecture-centric evaluation of blockchain-based smart contract e-voting for national elections," in *Informatics*, 2020, vol. 7, no. 2, p. 16.

[49] U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system—review and open research challenges," *Sensors*, vol. 21, no. 17, p. 5874, 2021.

[50] M. M. Alhejazi and R. M. A. Mohammad, "Enhancing the blockchain voting process in IoT using a novel blockchain Weighted Majority Consensus Algorithm (WMCA)," *Inf. Secur. J. A Glob. Perspect.*, vol. 31, no. 2, pp. 125–143, 2022.

[51] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," *Futur. Gener. Comput. Syst.*, vol. 105, pp. 13–26, 2020.