Survey on Secure E-Voting Platform

Miss. Sadhana Prakash Khade.
Government Polytechnic, Kolhapur.
khadesadhana8@gmail.com

ABSTRACT:

E-voting systems are being developed to replace traditional paper-based voting, offering benefits like efficiency, accessibility, and reduced costs. These include DRE machines, internet-based voting, and blockchain-enabled solutions. However, challenges like security, voter privacy, system reliability, and scalability remain significant. This survey looks at the current state of e-voting systems and the research around their design, use, and evaluation. It covers topics like security issues in DRE and internet voting, protecting voter privacy and confidentiality, making e-voting platforms accessible and easy to use for everyone, and how blockchain technology can create secure and transparent voting. The survey highlights gaps in current research and suggests future steps to improve the integrity, transparency, and trust in e-voting systems. By solving these challenges, e-voting could make democratic processes better and encourage more people to vote.

INDEX TERMS :

Online voting, safe voting system, verifying voters, OTP (one-time password) check, sending SMS, data protection, building web apps, showing voting results, and managing elections.

I. INTRODUCTION

Electronic voting (e-voting) systems are a big step forward in making elections better by using technology to increase efficiency, accessibility, and accuracy. Traditional methods like paper ballots can have problems such as human errors, fraud, and logistical issues. E-voting systems solve these problems by digitizing the voting process. They include tools like DRE machines used at polling stations and internet-based systems that let people vote from anywhere.

E-voting systems can help more people vote by making it easier, especially for those with disabilities, people living abroad, or those in remote areas. It can also save time by counting votes faster and giving more accurate results.

Setting up e-voting systems has big challenges, like ensuring security, protecting privacy, and gaining public trust. It's important to keep them safe from hacking, protect voter privacy, and make sure results are accurate. They also need to be easy to use, accessible for people with disabilities, and simple enough for everyone to understand, so all voters can take part easily.

This paper looks at how e-voting systems are built, used, and the challenges they face, focusing on security, ease of use, and accessibility. It reviews current systems, related research, and future possibilities, discussing both the advantages and risks of updating the voting process.

II. ASSOCIATED WORK

The development of e-voting systems has been shaped by the use of new technologies to improve how elections are run. From early DRE machines to modern ideas like blockchain, these advancements show a strong effort to fix the problems with traditional paper voting. This section looks at the history and latest progress in e-voting research, focusing on key security innovations and the challenges that still need to be solved.

Direct Recording Electronic Systems:

DRE systems were among the first to be broadly implemented in relation to e-voting technologies. In these systems, voters can directly submit their votes into an electronic system, without their vote being recorded on a paper-based ballot and then counted manually [1]. Early DRE systems aimed to reduce human error and speed up the tallying process to provide a more efficient solution compared to older methods. However, it did not take long for concerns about security and transparency to arise. Subsequently, studies began to show that DRE machines were susceptible to various types of malicious attacks, including the deployment of harmful software capable of altering vote counts without detection [2]. In response, numerous research efforts have been conducted to improve the security measures of DRE systems, such as incorporating voter-verified paper audit trails that produce a physical record of every vote cast [3].

1. Internet Voting:

Another method of voting that emerged was internet voting. It aimed to enhance accessibility by allowing voters to cast their votes from any location via the internet. This was especially attractive to absentee voters, military personnel stationed overseas, and individuals with disabilities [4]. Despite its convenience and potential to boost voter participation, internet voting has also faced several significant security issues. Among the major threats to the integrity of internet voting are DDoS attacks, phishing schemes, and man-in-the-middle attacks [5]. This prompted researchers to investigate the use of advanced cryptographic methods, such as end-to-end encryption and secure multi-party computation, to protect voter data and ensure the confidentiality and integrity of votes [6]. Often, implementing such security

measures involves balancing system complexity with user accessibility.

1. Blockchain-Based E-Voting Systems:

Among the groundbreaking solutions suggested to tackle the challenges of e-voting, blockchain technology has been remarkable, providing a fully decentralized and transparent vote record that is resistant to manipulation [7]. Blockchain based e-voting systems utilize blockchain's inherent security features, such as cryptographic hashing and consensus protocols, to achieve end-to-end verifiability and greater trust from voters in the process [8]. These systems allow voters to independently confirm that their votes have been recorded and counted accurately without compromising their privacy. In fact, pilot programs and numerous academic studies have already demonstrated the practicality of blockchain-based voting. However, scalability remains significant hurdle, particularly for nationwide elections involving millions of voters [9]. Additionally, issues related to the computational and energy demands of blockchain transactions limit its widespread adoption for election purposes [10]

2. Biometric Authentication in E-Voting:

Other advancements have incorporated biometric technologies like fingerprint scanning, facial recognition, and iris detection to further improve voter authentication and minimize fraud in e-voting [11]. Biometric verification can help create a strong identification system for voters, ensuring that only eligible individuals participate in an election. However, biometric verification involves sensitive personal information, raising concerns about the potential misuse of such data if it is exposed or compromised in a security breach [12]. Experts have emphasized the necessity for strict data protection policies and regulations to oversee the use of biometric data in voting systems [13].

3. End-to-End Verifiable Voting Systems:

One of the most important features of modern e-voting systems is end-to-end verifiability, which allows voters to confirm that their vote has been correctly cast, recorded, and counted without revealing their personal choice. Systems like Prêt à Voter, Scantegrity, and Helios use various cryptographic techniques, such as homomorphic encryption or mix-nets, to achieve this goal [15]. These systems can even provide voters with a receipt or verification code, enabling them to confirm that their vote has been included in the final tally, thereby enhancing transparency and trust in the process. While these systems are generally robust from a theoretical perspective, in practice, many face challenges with voter comprehension and usability because the verification processes are often complicated and not easily understood by the average voter [16].

4. Legal and Regulatory Issues:

The implementation of e-voting systems must also address various legal and regulatory considerations. The validity of e-voting relies on its adherence to the standards established by national and international electoral bodies. Legal frameworks must address issues such as data security, system certification, and post-election audits to ensure the process upholds its integrity [17]. Some researchers have emphasized the need for detailed guidelines and best practices to steer the deployment of e-voting systems, ensuring that security, transparency, and accessibility align with the required standard criteria for use [18].

5. Comparative Studies and Pilot Programs:

Various pilot projects and comparative studies on different e-voting technologies have been conducted in numerous countries and regions. For example, Estonia has been a pioneer in internet voting, first using it during national elections in 2005 [19]. Comparative studies of the Estonian system have provided valuable insights into both the practical challenges and advantages of internet voting, such as the significance of voter education and confidence in the technology [20]. Other nations, like Brazil and India, have adopted DRE systems, achieving mixed results that highlight the varying approaches to e-voting and the need for solutions tailored to specific contexts [21].

Overall, research on e-voting remains dynamic and evolving, with significant efforts directed at modernizing electoral processes while addressing critical issues of security, privacy, and accessibility. Despite notable advancements, the large-scale deployment of such systems still relies on further studies and innovations to enhance reliability, transparency, and public trust.

This related work in the field of e-voting has greatly contributed to the development of secure and efficient voting systems. However, implementing these systems on a larger scale has proven challenging in terms of security, usability, and accessibility. Building on the practical lessons learned from earlier systems, this paper proposes an e-voting solution that is accessible, secure, and efficient to address these challenges.

III. LITERATURE SURVEY

The literature on e-voting systems is highly diverse, covering the progressive evolution of voting technologies, concerns related to security and privacy, system usability, the application of blockchain and other emerging technologies, and biometrics. This paper provides a comprehensive review of existing studies, focusing on key advancements, challenges, and future prospects within the field of e-voting.

1. Vulnerability to Cyberattacks

E-voting systems are highly prone to cyberattacks, particularly internet-based voting and DRE systems. These typically include:

- **Malware and Virus Infections**: Attackers might inject harmful malware into the voting machines to alter vote counts or subtly disrupt the voting process in undetectable ways. Research has revealed that most DRE systems are incapable of defending against such malware, making them vulnerable to vote tampering [1].
- **DDoS Attacks**: Online voting systems are susceptible to DDoS attacks, where overwhelming traffic blocks the server, rendering the system inaccessible to voters. This can disrupt the entire election process and raise doubts about its credibility [2].
- **Phishing and Social Engineering**: Attackers may carry out phishing schemes, tricking voters into sharing their credentials or redirecting them to fake voting portals. This compromises voter authentication and leads to fraudulent votes [3].
- **Man-in-the-Middle Attacks**: In internet voting, this type of attack occurs when malicious actors intercept data transmitted between the voter and the voting server and manipulate it. This allows them to alter or steal votes without the voters' awareness [4].

2. Ensuring Voter Privacy and Anonymity

Voter privacy and anonymity are crucial for safeguarding voter choices and preventing coercion. However, several challenges emerge in e-voting systems related to these aspects:

- **Reconstruction Attacks**: These occur when attackers exploit system vulnerabilities to reconstruct voters' choices from voting data, leading to a breach of voter anonymity [5].
- **Voter Activity Tracking**: Many e-voting systems, particularly those using internet-based platforms, unintentionally monitor voter activities through IP addresses, cookies, or other uniquely identifying data. Such tracking can have serious consequences for voter privacy [6].
- **Transparency vs. Privacy in Blockchain**:

  Blockchain-based voting systems ensure transparency but struggle to maintain voter anonymity due to the immutable and traceable nature of blockchain transactions [7]. Striking a balance between transparency and privacy in this context requires advanced cryptographic methods,

  such as zero-knowledge proofs, which add complexity to the system [8].

3. System Integrity and Tamper-Resistance

Integrity ensures that the e-voting system accurately captures each voter's choice and records and counts it correctly. Maintaining the integrity of the system is a significant challenge due to the following:

Software and Hardware Tampering: E-voting systems are vulnerable to interference with both software and hardware, such as the modification of components within a voting machine. A key challenge is ensuring that both software and hardware remain secure against tampering.

Insider Threats: These involve individuals with access to the electronic voting system, such as administrators or developers. If they act maliciously or if their accounts are compromised, they can pose severe risks. Insider threats are particularly hard to counter because they involve individuals with elevated access privileges.

Secure Audit Trails: An e-voting system must provide secure audit trails to enable the verification of election results [11]. Ensuring these trails are tamper-proof and accurately reflect the election outcome is challenging, particularly when balancing transparency with the need to protect voter privacy.

4. End-to-End Verifiability

Integrity ensures that the e-voting system properly captures each voter's selection and accurately records and tallies it. Preserving the system's integrity poses a considerable challenge due to the following:

- **Software and Hardware Manipulation**: E-voting systems are at risk of tampering with both software and hardware, such as altering components within a voting device. A critical challenge is ensuring that both software and hardware are safeguarded against interference.
- **Insider Risks**: These refer to individuals with privileged access to the e-voting system, like administrators or developers. If they turn malicious or their accounts are compromised, they can present serious risks. Insider risks are particularly challenging to mitigate because they involve individuals with privileged access.
- **Reliable Audit Trails**: An e-voting system must provide reliable audit trails to support the verification of election results [11]. Making these trails tamper-resistant and reflective of the actual election outcome is difficult, especially when balancing transparency with protecting voter confidentiality.

.

5. Secure Voter Authentication

Voter authentication is essential to ensure that only eligible individuals are allowed to vote and that no voter casts more than one ballot. Security challenges in voter authentication include:

- **Weak Authentication Mechanisms**: Some e-voting systems rely on weak authentication methods, such as passwords or PINs [15], which can be compromised through phishing, guessing, or brute-force attacks.
- **Risks in Biometric Authentication**: While biometric methods, such as fingerprint or facial recognition [16], offer stronger authentication, the risks associated with storing and safeguarding sensitive biometric data are significant. A breach of biometric data can have severe privacy repercussions and, unlike passwords, cannot be changed or replaced.
- **Usability of Advanced Authentication**: Stronger authentication techniques, like multi-factor authentication, enhance security but may pose usability difficulties, particularly for voters who are less familiar with technology or those with disabilities [17].

6. Scalability and Performance

Scalability and performance are key factors in the effective deployment of e-voting systems, especially during large-scale elections. The challenges include:

- **Large Voter Numbers**: E-voting systems must be capable of accommodating hundreds, thousands, or even millions of voters at once without experiencing performance issues. Poor scalability can lead to slow system responses or even crashes, potentially disrupting the voting process and discouraging voter participation.

- **Blockchain Scalability**: Although blockchain-based voting systems offer significant security benefits, they often face scalability challenges due to the substantial computational and storage requirements needed to operate a decentralized ledger [19]. This typically results in slow transaction processing speeds, making their use impractical for large-scale national elections.

7. Regulatory and Compliance Challenges

E-voting systems must adhere to specific legal and regulatory standards designed to protect voter rights and ensure fair elections. The challenges include:

- **Adhering to Diverse Legal Frameworks**: Each country and region has its own legal requirements regarding elections. Designing a single e-voting solution that suits all nations can be highly challenging [20]. It is particularly difficult to ensure compliance with these varied legal frameworks while respecting local laws and regulations.
- **Certification and Standardization**: E-voting systems need to undergo rigorous testing and certification to validate their security and functionality [21]. However, the lack of standardized testing protocols often leads to inconsistent evaluation results, producing systems with varying levels of security.

Successfully implementing an e-voting system requires overcoming these security-related challenges. Only through ongoing research and innovation in cryptographic methods, system architecture, and voter education can these obstacles be addressed, allowing e-voting to become a reliable and credible alternative to traditional voting methods.
.

B) Accessibility and Usability in E-Voting Systems

Accessibility and ease of use are key factors in determining the overall efficiency, inclusiveness, and user experience in the voting process. Guaranteeing that individuals with disabilities, limited technological proficiency, or language barriers can easily utilize an e-voting system lies at the core of fostering democratic participation. This section outlines the primary challenges and factors to consider in designing accessible and user-friendly e-voting systems, along with potential solutions and recommended practices.

1. Accessibility Challenges

One of the critical issues of e-voting, accessibility, refers to all voters being able to participate autonomously in the voting process in private. Major challenges in accessibility include:

Voter Disabilities: Voters with physical disabilities, such as limited mobility, idea enhancements, or hearing loss may find difficult to use the interface of conventional e-voting. Traditional methods of voting require hand-based fine motor skills or clear vision for which these voters cannot participate in the process.

E-voting systems are daunting for those people who are unfamiliar with the digital world. Examples include elderly voters and those that have limited contact with technical devices [2]. Lack of technological literacy may result in voter errors, frustration, and/or a refusal to take part in the voting process.

Language barriers, attributed to the multicultural nature of societies, may severely obstruct the potential for accessibility in e-voting. If the interface of e-voting is availed in one language only, then non-native speakers cannot comprehend the commands and thus may not be able to complete their votes accurately.

Remote access to absentee voters: Voters who are overseas, in remote locations, or otherwise unable to access the polling stations can cast a vote using internet-based e-voting [4]. Ensuring secure, reliable, and user-friendly access to such systems is one of the major challenges.

2. Usability Challenges

Usability refers to how easily and effectively voters can engage with the e-voting system. Poor usability can deter voters from voting successfully or erode their confidence in the system. Some key challenges related to usability include:

Complexity in User Interfaces: If the user interfaces of e-voting systems are too complex or not intuitive, this may confuse voters [5]. Confusion can lead to errors, such as voting incorrectly or failing to complete the voting process. Poorly designed interfaces can especially impact voters with disabilities or those who are unfamiliar with technology.

Cognitive Overload: The more complex the instructions given by the system or the greater the number of screens voters must navigate, the more information they need to process [6]. This creates difficulties for individuals with cognitive impairments, limited literacy, or similar challenges, increasing the likelihood of errors or incomplete ballots.

Lack of Feedback: Feedback at various stages of the voting process is essential to assure voters that their actions, such as casting a vote, have been successfully completed [7]. Systems that fail to provide adequate feedback can leave voters uncertain about whether their votes were recorded.

3. Designing Accessible and Usable E-Voting Systems

These challenges can only be overcome by making access and usability of paramount importance in the development or design process of an e-voting system. Here are some strategies that might go a long way toward fulfilling that:

Integrating Assistive Technologies: Screen readers, Braille displays, voice recognition, switch devices, and the like-are examples of assistive technologies to be incorporated into the system in order to make voters with a disability use such a system independently [8]. For example, screen readers can convert text to speech for visually impaired voters, while switch devices can allow those with limited mobility to navigate the system.

Easy-to-Use and Simplified Interfaces: The design of user interfaces should be made simple, clear, and intuitive; they should require as few steps as possible to finish the process. In this regard, large buttons, high contrasts in colors, and fonts can enhance readability and facilitate ease of use [9]. Also, there is a place for visual and audio cues that will help voters navigate the process.

Multilingual Support: Availability of e-voting interface in multiple languages would support voters speaking different languages. Instructions and info can be made available to voters in their preferred language, and this approach reduces confusion and hence errors.

Accessible Verification: Systems that include verification steps on the part of the voter should provide confirmation of the cast vote in an available manner [11]. This may include audio confirmations, visual checks, or other accessible verification methods that do not compromise voter privacy.

User-Centered Design and Testing: The involvement of various types of voters in the design and testing stages helps a lot in the identification of and finding a solution to the problem of accessibility and usableness concerning the e-voting system. The user-centered design practices, such as usability tests conducted with people with disabilities, can provide critical insight into just how such a system could be made more inclusive.

Clearly, Providing Instructions and Help: There should be clear instructions displayed that explain each step to the voter [13]. Providing help options, both on-screen and through help hotlines that are accessible, will provide additional support for voters who may need additional assistance during a vote.

3. Real-World Implementations and Case Studies

A few countries and organizations have been able to realize some accessible and user-friendly e-voting systems which offer some lessons and best practices:

Estonian Internet Voting System: Estonia has been at the forefront of providing internet voting with a system that is accessible to different sets of voters even from abroad [14]. Some of the major features that distinguish it from other elections are an intuitive interface, multilingually, and high security; hence, it has been a model in terms of accessible e-voting.

U.S. Accessible Voting Systems: According to HAVA, all the voting systems in the United States should provide accessibility for voters with disabilities [15]. Due to this reason, numbers of accessible voting solutions are being implanted, including ballot-marking devices that accommodate a wide range of disabilities while maintaining

privacy and independence for all voters.
Accessible Features in Brazil's DRE Systems: Brazil has implemented features to make the DRE voting machines more accessible, [16]. such as audio instructions and Braille keypads for visually impaired voters. This allows all voters to participate independently in the process.

4. Future Directions in Accessibility and Usability

The ongoing development of e-voting systems will provide for continued advancement of systems in terms of accessibility and usability. Research and development in this area should be directed toward the following areas of concern:

Innovative Assistive Technologies: Investigations into new assistive technologies, such as haptic feedback devices and augmented reality interfaces, may further improve the accessibility of e-voting systems.
Improved User Testing and Feedback: Involving various groups of voters in usability testing on a continuous basis and integrating their feedback into the design of systems will be helpful in keeping e-voting systems accessible and user-friendly.
Standardization and Best Practice: Standard guidelines and best practices can be developed for accessible e-voting, making it easier for various countries and organizations to design systems that are accessible to all types of voters [19]. International collaboration and sharing will be of immense value in encouraging accessibility and usability in e-voting of the future.

In this manner, electoral bodies ensure, through design for accessibility and usableness, the full participation by and self-governing engagement of all eligible voters in the democratic process. This not only increases the inclusiveness of voters but also improves the overall integrity and legitimacy of elections conducted using electronic voting technologies.

IV. FUTURE WORK

In the field of e-voting systems, future research should be directed to enhancement in security, accessibility, and scalability due to various challenges arising in the usage of digital voting. For instance, there will be the need for developing more secure cryptographical protocols, such as post-quantum cryptography, against emerging threats like quantum computing. Similarly, further explorations of blockchain can enhance the transparency and trust of e-voting systems, although research needs to take into consideration the issues of scalability and privacy concerns related to blockchain.
Improvement of accessibility and serviceability does remain a critical research direction, with a particular focus on interface design that caters to access needs for all voters, not excluding those with disabilities or limited digital literacy. This integrates advanced assistive technologies like voice recognition and gesture control, making e-voting more inclusive.

It is also very relevant to conduct research on the use of artificial intelligence and machine learning and improve voter authentication and fraud detection so that only eligible voters can have a say in elections, and the system is resilient against sophisticated attacks.

There is a need for comprehensive studies on voter behavior, trust, and the social impact of e-voting technologies. These will be fundamental in formulating systems that would meet not just the technical requirements but also make gains in confidence among the electorates

E-voting systems are increasingly being explored with the aim of taking over from traditional paper-based voting and may offer several advantages, including efficiency, accessibility, and cost-cutting. These systems include DRE machines, internet-based voting, to even blockchain-enabled voting solutions. However, this shift toward e-voting is attended by a raft of significant hurdles on security, secrecy in voting, dependability of the systems, and scalability. This survey paper covers the current status of e-voting systems and related work and literature regarding the design, implementation, and evaluation. These topics will range from security vulnerabilities regarding DRE and Internet voting to privacy and anonymity concerns with respect to maintaining confidentiality of voters, accessibility and usability of e-voting platforms for the diverse voter population, and the increasingly emerging blockchain technology that provides secure and transparent processes toward voting. The survey underlines important gaps in present research and points to a number of future directions that might help in building up integrity, transparency, and trustworthiness in e-voting systems. In overcoming the challenges lying ahead, e-voting has the potential to significantly improve democratic processes and enhance voter participation.

V. CONCLUSION

In this overview of the general status of e-voting systems, we have presented an overview from multiple angles: the technological developments, security challenges, users' acceptance, and the general feasibility for introducing electronic voting within different contexts. Our results clearly show that while e-voting systems do have some crucial potential advantages-increasing voter access, lowering the costs, and processing results in less time-they also make a raising of important critical trials, particularly regarding security, privacy, and public trust.

The analysis has shown that security remains an elusive dream because susceptibilities in the software, hardware, and network infrastructure undermine the integrity of the process. Also, privacy issues such as those related to voter coercion and those ascribed to ensuring ballot secrecy add complexity to the broad base adoption of the E-voting systems. It also underlined a important breach in public trust, with the key drivers of this being characterized by scares over riding, fraud, and possible misuse of data.
However, in spite of these problems, the potentiality of e-voting systems cannot be discarded. In those few jurisdictions where it has been conducted successfully, it has

emerged that with proper security provisions, transparency in their processes, and education of the voters, the e-voting system can work to increase democratic participation and make the conduct of elections easier.

In this regard, it is advisable that, in the future, research efforts be targeted at evolving more secure and user-friendly systems to address these identifications of the survey-in the areas of cryptographical techniques, better methods of voter authentication, testing, and auditing. Further efforts should also be made to enhance public trust through transparency and education of the general public on security issues, involving them in development and evaluation processes.

However, the successful implementation of the e-voting system also depends on whether these technical and social challenges are surmounted. The way forward will call for continued research, innovation, and collaboration among technologists, policymakers, and the general public in a move to build secure, reliable, and trusted systems for e- voting.

VI. ACKNOWLEDGEMENT:-

I would like to convey my heartfelt gratitude to everyone who contributed to the successful completion of this research paper, "Enhancing Electoral Integrity: Survey of a Secure E-Voting Platform." My profound appreciation goes to my mentor, [Mr. Prashant Patil], whose knowledge, guidance, and motivation have been indispensable throughout the research journey. I also wish to thank my colleagues and peers for their thoughtful discussions and unwavering support. Furthermore, I am grateful for the resources and aid provided by [Miss. Komal Parit]. Lastly, I am sincerely thankful to my family for their unwavering encouragement and backing.

REFERENCES:-

1. Adida, B. (2008). Helios: Web-based open-audit voting. In *Proceedings of the 17th USENIX Security Symposium*.

2. Halderman, J. A., & Teague, V. (2015). The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election. In *Proceedings of the 5th International Conference on E-Voting and Identity.*

3. Rivest, R. L., & Wack, J. P. (2006). On the notion of "software independence" in voting systems. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 366(1881), 3759-3776.

4. Kulyk, O., Volkamer, M., Kobsa, A., & Hughes, S. (2015). Providing voters with responsible explanations for their choices to enhance their trust in voting systems. In *Proceedings of the 14th International Conference on Trust, Security and Privacy in Computing and Communications*.

5. Benaloh, J., Rivest, R. L., Ryan, P. Y., Stark, P. B., Teague, V., & Vora, P. (2014). End-to-End Verifiability. In *Handbook of Financial Cryptography and Security*.

6. Goodman, N., Volkamer, M., & Ryan, P. Y. (2014). Usability and accessibility of the Prêt à Voter e- voting system. In *Proceedings of the 6th International Conference on Electronic Voting: Verifying the Vote*.

7. Estonian National Electoral Committee. (2020). *E-Voting in Estonia: Overview*. Estonian Ministry of Interior.

8. Dini, G., & Martinelli, F. (2006). A secure and usable e-voting system based on blind signatures and k-anonymity. In *Computer Security Applications Conference*.

9. Gjøsteen, K. (2011). Analysis of an internet voting protocol. In *International Workshop on Security Protocols*.

10. Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, P., & Halderman, J. A. (2014). Security Analysis of the Estonian Internet Voting System. In *Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS)*.

Author's:

Miss. Sadhana Prakash Khade is currently pursuing a Diploma in Electronics & Telecommunication at Government Polytechnic, Kolhapur. She has helps in conducting a comprehensive survey on e-voting system.