IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 11, November 2025

DOI: 10.17148/IARJSET.2025.121126

Blockchain-Enabled Secure E-Voting Using Wallet-Based Voter Authentication and Smart Contracts

Sudha M[1], Samarth R Hegde[2], Dhanush C[3], Hrishikesh Gangatkar[4], Pradyumna VG[5]

Assistant Professor, Dept of AIML, KS Institute of Technology[1]

Student, Dept of AIML, KS Institute of Technology[2]

Student, Dept of AIML, KS Institute of Technology[3]

Student, Dept of AIML, KS Institute of Technology[4]

Student, Dept of AIML, KS Institute of Technology[5]

Abstract: This paper presents a comprehensive analysis of blockchain-enabled electronic voting systems, focusing on how decentralization, smart contracts, and advanced cryptographic techniques can enhance trust, security, and transparency in modern elections. By examining key research contributions—including Ethereum-based protocols like Ques-Chain, decentralized systems such as the Open Vote Network, permissioned blockchain evaluations using Hyperledger Fabric, and cutting-edge privacy solutions employing zero-knowledge proofs and zk-SNARKs—the work highlights both the promise and limitations of blockchain as an e-voting foundation. The study explains how wallet-based voter authentication, Merkle tree validation, and self-tallying mechanisms can enforce one-time voting, preserve voter anonymity, and eliminate reliance on central authorities. At the same time, the analysis acknowledges persistent challenges: scalability constraints, governance complexities, and the critical vulnerability posed by insecure end-user devices. The paper concludes that while blockchain provides a mathematically robust and auditable architecture for secure e-voting, achieving a truly trustless, large-scale national implementation requires addressing real-world security issues, performance bottlenecks, and user-centric barriers that remain unresolved today.

Keywords: Blockchain, E-Voting, Smart Contracts, Zero-Knowledge Proofs, zk-SNARKs, Merkle Tree, Wallet-Based Authentication, Decentralization, Cryptographic Voting, Hyperledger Fabric, Election Security, Self-Tallying Protocols1. Introduction: The Imperative for Secure E-Voting in the Digital Age

I. INTRODUCTION

1.1. The Evolving Landscape of E-Voting and Its Challenges

The transition from traditional paper-based ballots to electronic voting systems is motivated by the desire to enhance accessibility, increase voter participation, and streamline the election process to produce faster results. However, this evolution has introduced a new and complex set of challenges, particularly concerning authentication, data privacy, integrity, and the verifiability of results. These concerns have led to a significant lack of public trust, with many voters questioning the security and reliability of centralized e-voting platforms.[1] The global health crisis during the COVID-19 pandemic further underscored the urgent need for a secure, impartial, and confidential remote voting solution that could operate without the risks associated with physical gatherings.[1]

The vulnerabilities of centralized e-voting systems, such as the potential for data tampering and electoral fraud, have a direct and measurable impact on public confidence. When the integrity of a system is in doubt, voters may lose faith in the democratic process itself, reinforcing a reliance on paper ballots and other traditional, albeit less efficient, methods.[1] The move toward blockchain-based solutions is a direct response to this crisis of confidence. The core value proposition is not merely to introduce a new technology, but to employ cryptographically-enforced trust mechanisms that can fundamentally address the deficit in public confidence. By leveraging features such as immutability, transparency, and decentralization, blockchain technology offers a viable pathway to rebuild and strengthen trust in the electoral process.

1.2. Report Scope and The Foundational Promise of Blockchain

This report provides an expert-level analysis of the application of blockchain technology to address the critical challenges of electronic voting. It examines how the core properties of blockchain—decentralization, immutability, and transparency—can be leveraged to create a tamper-proof and auditable platform.[3] The analysis focuses specifically on

 This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 11, November 2025

DOI: 10.17148/IARJSET.2025.121126

the roles of smart contracts and wallet-based authentication in this context, with a particular emphasis on the cryptographic solutions employed to ensure a "one-time vote" and to protect voter privacy.[2]

II. CORE CONCEPTS: THE BUILDING BLOCKS OF A SECURE E-VOTING FRAMEWORK

2.1. Blockchain's Foundational Role: Immutability, Transparency, and Decentralization

At its core, a blockchain is an append-only, distributed ledger. This fundamental architecture provides three properties that are uniquely suited for the requirements of a secure voting system.

- **Immutability and Durability:** Once a vote is recorded as a transaction on the blockchain, it is unalterable and cannot be lost. This cryptographic permanence ensures the finality of the vote and creates a robust, tamper-proof record.[3] The durability of the data ensures that the election records are permanent and resistant to data loss.
- **Transparency and Auditability:** The inherent design of public blockchains encourages open and auditable voting procedures. All vote transactions are visible to participants and can be independently verified.[3] This facilitates public verifiability, allowing anyone to confirm that their vote was recorded and counted correctly, while also enabling independent audits of the entire election process.[3]
- **Decentralization:** By distributing the ledger across a peer-to-peer network, blockchain-based systems remove the reliance on a single, centralized entity that could become a single point of failure or a target for manipulation. This decentralized consensus mechanism is a promising solution to mitigate the risk of electoral fraud and data tampering.[1]

2.2. The Mechanics of Smart Contracts: Automation and Enforcement

A smart contract is a self-executing program that runs on the blockchain and automatically carries out a transaction when specific, predefined conditions are met.[4] In the context of e-voting, smart contracts are used to enforce every aspect of the voting protocol, from voter registration and eligibility checks to the secure aggregation of ballots.[2] This automation eliminates the need for a central authority or an intermediary to manage the election, significantly reducing the potential for human error or malicious interference.[4]

The use of smart contracts, particularly when combined with a robust consensus mechanism like Ethereum's, represents a fundamental shift in the trust model of an election. Historically, elections have relied on human or institutional trust, where voters must believe that a "trusted third party," such as an election commission, will properly manage the ballot boxes and accurately tally the votes.[2] Blockchain-based protocols, such as the Open Vote Network, explicitly do not rely on any trusted authority to compute the tally or protect voter privacy.[6] Instead, the protocol's correct execution is mathematically enforced by the blockchain's consensus mechanism.[6] This means the code itself becomes the trusted authority, transparently and immutably executing the rules of the election. This decentralization of trust is a core contribution that addresses a major historical vulnerability.

2.3. Wallet-Based Voter Authentication and the Prevention of Double Voting

Centralized e-voting systems traditionally rely on a single database for voter authentication and to prevent double voting. Blockchain-based systems offer a decentralized alternative using digital wallets and cryptographic keys.

- **Smart Contract Wallets:** These wallets represent an advancement over traditional wallets, as they are programmable and can enforce complex rules defined within a smart contract.[5] This allows for superior security features, such as multi-signature access, which can require multiple confirmations to authorize a vote transaction.[5] This programmability provides enhanced security and automation that traditional wallets lack.
- **Zero-Knowledge Proofs (ZKPs):** A critical cryptographic technique for e-voting is the use of Zero-Knowledge Proofs. ZKPs allow a "prover" (the voter) to demonstrate to a "verifier" (the smart contract) that a statement is true (e.g., "I am an eligible voter with a valid ticket") without revealing any additional information, such as the voter's identity or their vote.[9] This is a powerful solution for maintaining voter anonymity while simultaneously ensuring a one-time vote and preventing fraud.
- **The Merkle Tree and zk-SNARKs:** A common and effective approach to preventing double voting is the use of a Merkle tree to store a hash of each voter's ticket.[11] During the vote casting process, a voter generates a zk-SNARK proof that they possess a valid ticket that is a leaf in this Merkle tree.[11] The smart contract then verifies this proof against the Merkle root stored on the blockchain. This process ensures both the authenticity of the voter and that the ticket is used only once, all without revealing the voter's personal information. The system can confirm the integrity of the votes without disclosing the voters' privacy.[11]

The application of ZKPs and other advanced cryptographic techniques addresses what has historically been a fundamental paradox in e-voting: the conflict between voter anonymity and election verifiability. A voter wants to ensure that their choice remains private, but for the election to be trustworthy, the process must be verifiable by all. These

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 11, November 2025

DOI: 10.17148/IARJSET.2025.121126

cryptographic solutions resolve this conflict by allowing for the public verification of a vote's validity and its correct inclusion in the final tally without revealing the voter's choice.[9] The trust is no longer placed in a central entity to protect sensitive information but in the mathematical guarantees of the cryptographic protocol itself.

2.4. Key Security and Privacy Requirements for E-Voting

For an e-voting system to be considered secure and trustworthy, it must satisfy a number of critical requirements. The following table provides a summary of the most important of these, based on a review of the research literature.[3]

Requirement	Definition	How Addressed by Blockchain
Integrity	Holistic assurance that votes are not altered after they are cast.	The cryptographic hash chain and consensus mechanism ensure that once a vote is recorded, it cannot be changed.
Immutability	A vote, once recorded, cannot be altered or removed.	Blockchain's append-only ledger and distributed nature make it nearly impossible to retroactively alter data.
Transparency	The voting, recording, and counting procedures are open and verifiable to all participants.	The public ledger allows all transactions (votes) to be visible and verifiable by anyone.
Privacy (Anonymity & Confidentiality)	The voter's personal information and voting choices are protected.	Cryptographic techniques like zero-knowledge proofs and pseudo anonymity mask the voter's identity while confirming their eligibility and vote validity.[3]
Verifiability	The ability to confirm that votes have been cast, stored, and counted as intended.	Individual verifiability allows each voter to confirm their vote was correctly recorded. Public verifiability allows all observers to audit the entire process.[3]
Auditability	The process ensures the accuracy and truthfulness of the final election results.	The transparent and immutable nature of the blockchain facilitates independent audits and recounts.[3]
One-time Vote/Uniqueness	The system prevents voters from casting more than one vote.	Smart contracts and cryptographic techniques like Merkle trees and ZKPs can programmatically enforce this rule.[11]

III. CASE STUDIES: A DEEP DIVE INTO KEY RESEARCH PAPERS

3.1. The Ques-Chain Protocol: An Ethereum-Based Approach

The paper, *An Ethereum based E-voting Protocol with High Security and Anonymity Using Blind Signature*, proposes an Ethereum-based protocol known as Ques-Chain.[2] This protocol is designed to ensure a high degree of security and anonymity. Its primary contribution is the use of blind signatures to decouple voter authentication from ballot content, ensuring that anonymity is protected without sacrificing the ability to prevent fraud.[2] The process is a four-stage protocol: Setup, Sign, Vote, and Count. It uses an Ethereum smart contract as a "judge" function to validate ballots and store valid votes in a decentralized "BallotBox" database, making the entire process transparent and verifiable.[2] A unique UUID is used as a technical mechanism to prevent multiple voting, which the smart contract checks during the voting stage.[2]

 This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 11, November 2025

DOI: 10.17148/IARJSET.2025.121126

3.2. The Open Vote Network: Decentralized Privacy in Boardroom Voting

A Smart Contract for Boardroom Voting with Maximum Voter Privacy presents the Open Vote Network, which is noted as the first implementation of a decentralized and self-tallying internet voting protocol on a blockchain.[6] A key contribution is its complete elimination of any trusted authority for tallying or protecting voter privacy.[6] The protocol is a two-round process—Voter Registration and Vote Casting—which is enforced by the Ethereum blockchain's consensus mechanism. The system employs zero-knowledge proofs (specifically, Schnorr and Cramer, Damgård, and Schoenmakers methods) to prove a voter's eligibility and the validity of their vote without revealing their identity or choice.[6] The "self-tallying" feature allows any voter or third party to compute the final result, further reinforcing the decentralized and trustless nature of the system.[6]

3.3. Performance Evaluation of Hyperledger Fabric

The study, *Performance Evaluation of E-Voting Based on Hyperledger Fabric Blockchain Platform*, shifts focus from a public blockchain like Ethereum to a permissioned one, Hyperledger Fabric.[7] This paper provides a crucial empirical analysis of a blockchain-based e-voting system's practical performance. The findings indicate a direct correlation between key architectural parameters and system performance metrics such as latency and throughput.[7] Specifically, the study found that high transaction rates and large block sizes led to better performance, while increasing the number of organizations in the network negatively impacted latency and throughput.[7] This research highlights the critical importance of architectural design choices when deploying such systems, particularly for large-scale applications where performance is paramount.

3.4. Advanced Cryptography: The Role of Zero-Knowledge Proofs

A paper proposing a *Secure and Privacy-Preserving Voting System Using Zero-Knowledge Proofs* highlights the use of advanced cryptography to address core security and privacy challenges.[9] The system uses a combination of ZKPs and homomorphic encryption to ensure integrity, confidentiality, and voter anonymity. ZKPs are used to verify a voter's eligibility without revealing their personal identity, and to prove the validity of an encrypted vote without disclosing the choice.[9] The use of homomorphic encryption allows for the secure aggregation of votes while they remain encrypted, ensuring that individual choices are never revealed, even during the tallying process.[9] This multi-layered cryptographic approach is presented as a robust solution for large-scale elections.

3.5. A Proof of Concept: Zk-SNARKs and Ticket-Based E-Voting

The *ZkSNARKs and Ticket-Based E-Voting: A Blockchain System Proof of Concept* paper proposes a system that uses zk-SNARKs and a Merkle tree to ensure voter authenticity and prevent double voting.[11] The system begins with the creation of a Merkle tree during the registration phase, where each voter's ticket hash is stored as a leaf.[11] The Merkle root is then registered on the blockchain. When a voter casts a vote, they submit a zk-SNARK proof that they possess a valid ticket that is a leaf in the tree, without revealing which specific ticket they hold.[11] The smart contract validates this proof against the Merkle root, ensuring a one-time vote while preserving the voter's anonymity.

IV. THE NUANCED PERSPECTIVE: BENEFITS, CHALLENGES, AND CRITICISMS

4.1. The Primary Benefits of Blockchain E-Voting: A Unified View

Based on the synthesis of multiple systematic reviews, the primary benefits of blockchain-based e-voting are multifaceted.[1] These systems offer heightened security and integrity through immutability and decentralization, which prevent fraud and data tampering.[3] The public and transparent nature of the ledger allows for robust verifiability and auditability, empowering voters and third-party observers to independently confirm the election results.[3] Furthermore, advanced cryptographic techniques ensure voter privacy and anonymity, protecting the confidentiality of voting choices.[3] The automation provided by smart contracts also has the potential to increase the efficiency and reduce the cost and time associated with traditional elections.[3]

4.2. Persistent Challenges and the Scalability Trilemma

Despite the technological promise, significant challenges remain. The most frequently cited concerns are privacy, transaction speed, and scalability.[1] Blockchain technology is known to face the "Scalability Trilemma," a fundamental trade-off between scalability (high transaction speed), decentralization (involvement of a vast number of participants), and security (cost of gaining control over the network).[1] A system can typically only achieve two of these three properties, which presents a major barrier to the adoption of blockchain for national-level elections where high throughput is critical.[1] The performance evaluation of a Hyperledger Fabric-based system further confirms these bottlenecks, demonstrating that performance is heavily influenced by factors such as block size and the number of participating organizations.[7]

 This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 11, November 2025

DOI: 10.17148/IARJSET.2025.121126

Furthermore, while decentralization is often lauded as a core benefit, a critical analysis of blockchain-based voting systems reveals a complex trade-off. A paper from the MIT Digital Currency Initiative points out that blockchain protocols, by their very nature, require governance and coordination among a multitude of actors.[12] This introduces a new set of management challenges that are often difficult to handle. The trust problem is not so much solved as it is transformed from relying on a single, centralized entity (e.g., a government election commission) to a more complex, multi-stakeholder governance model. This new model has its own unique risks, such as collusion or political disputes among the validators, which can be even more complex to manage than the vulnerabilities of a single, central authority.

4.3. A Contrarian View: The MIT Critique

A major paper from the MIT Digital Currency Initiative, *Going from bad to worse: from Internet voting to blockchain voting*, presents a strong and nuanced critique of blockchain e-voting.[12] The paper argues that internet- and blockchain-based voting would "greatly increase the risk of undetectable, nation-scale election failures".[12]

A primary point of contention is that blockchain does not solve the most critical security threat to remote electronic voting: the end-user's device.[12] Standard cybersecurity threats like malware and zero-day attacks can compromise a voter's personal computer or smartphone before a vote is even cast. If a malicious actor alters a vote on the user's device before it is encrypted and sent to the blockchain, the immutability of the chain is irrelevant.[12] The blockchain will simply record the tampered but cryptographically valid vote. This highlights a crucial disconnect between the technical perfection of an e-voting protocol and its real-world application. A mathematically sound system is rendered vulnerable by the weakest link in the chain, which is the insecure personal device of the average citizen.

The MIT critique also points out that, beyond pre-existing cybersecurity risks, blockchains introduce additional problems related to governance and coordination among multiple actors.[12] The report suggests that these systems fail to meet the unique needs of a political election, where universal accessibility, end-to-end security, and a provably auditable outcome are paramount. The technical novelty of the blockchain solution, while significant, does not address the most common and difficult-to-solve security problems of remote electronic voting.

V. COMPARATIVE ANALYSIS AND FUTURE OUTLOOK

Paper/Protocol	Primary Platform	Voter Authentication Method	Double Voting Prevention	Key Cryptographic Techniques	Primary Contribution	Application Scale
Ques-Chain	Ethereum	Blind Signatures	UUID/Smart Contract	Blind Signatures	Anonymity with separation of authentication and ballot content	E-voting, surveys
Open Vote Network	Ethereum	ZKPs/Schnorr Proofs	ZKPs	ZKPs, Fiat-Shamir Heuristic	First decentralized, self-tallying protocol with maximum privacy	Boardroom
Hyperledger Study	Hyperledger Fabric	Not specified	Not specified	Not specified	Empirical performance evaluation of a permissioned blockchain	Not specified
ZKP System	Not specified	ZKPs	ZKPs	ZKPs, Homomorphic Encryption	Secure and private system for large-scale elections	Large-scale
Zk-SNARKs POC	Blockchain	Ticket-Based	ZKPs/Merkle Tree	Zk-SNARKs, Merkle Tree	Proof of concept for ticket-based authentication and one-time vote	Not specified

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 11, November 2025

DOI: 10.17148/IARJSET.2025.121126

5.1. Comparative Analysis of Reviewed Systems

The papers reviewed in this report highlight a variety of approaches to blockchain-based e-voting. A comparative analysis reveals key distinctions across different systems.

The reviewed systems show a clear divergence in their architectural and cryptographic choices. The Open Vote Network and Ques-Chain protocols use the public Ethereum blockchain, leveraging its decentralized consensus. In contrast, the Hyperledger Fabric study focuses on a permissioned, private blockchain, highlighting the trade-offs in performance and decentralization. A critical difference lies in the authentication and privacy mechanisms: Ques-Chain uses blind signatures to hide ballot content, while systems leveraging ZKPs and Merkle trees achieve a more robust form of anonymity by separating voter identity from eligibility proof.[2]

5.2. Future Research Directions

Based on the challenges and critiques identified in this report, future research must address a number of critical areas to move the field forward. First, continued work on **scalability solutions** is paramount, as current systems are not yet capable of handling the volume of a national-scale election without sacrificing decentralization or security.[1] Second, there is a clear need for research into
end-to-end verifiability that can address the issue of client-side malware and ensure a vote is not tampered with on the voter's local device before it is cast.[12] Third, as the MIT critique highlights, a focus on
robust governance models for decentralized protocols is essential. Finally, simplifying the complex cryptographic processes to make them **accessible and usable** for the general public, including the elderly and disabled, is a critical step for real-world adoption.[1]

VI. CONCLUSION

The application of blockchain technology to electronic voting presents a compelling, cryptographically-enforced solution to many of the vulnerabilities of traditional e-voting systems. By leveraging the inherent properties of immutability, transparency, and decentralization, along with advanced cryptographic techniques like smart contracts, zero-knowledge proofs, and Merkle trees, researchers have proposed systems that can address issues of fraud, data tampering, and a lack of voter trust. These systems can provide a self-tallying, auditable, and privacy-preserving framework for elections.

However, as the analysis has shown, significant and complex challenges remain. The fundamental trade-offs of the scalability trilemma mean that a truly decentralized and secure national-scale e-voting system remains an elusive goal. Moreover, the most profound critique is that blockchain does not solve the primary security risk of remote voting, which is the vulnerability of the voter's personal device. The elegance of a cryptographically perfect protocol is diminished if the integrity of the vote can be compromised at the endpoint before it even reaches the blockchain. The path forward for blockchain-enabled e-voting requires not only continued technological innovation but also a more nuanced understanding of the real-world security, governance, and human-centric challenges that must be overcome for such systems to be a viable and trustworthy alternative for modern democracies.

REFERENCES

[1]. A Systematic Literature Review and Meta-Analysis on Scalable ..., accessed on September 13, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC9572428/
[2]. QUES-CHAIN: AN ETHEREUM BASED E-VOTING SYSTEM, accessed on September 13, 2025, https://csitcp.org/paper/9/98csit03.pdf
[3]. Blockchain-Based E-Voting Systems: A Technology Review - MDPI, accessed on September 13, 2025, https://www.mdpi.com/2079-9292/13/1/17
[4]. Smart Contracts on Blockchain: Definition, Functionality, and Applications - Investopedia, accessed on September 13, 2025, https://www.investopedia.com/terms/s/smart-contracts.asp
[5]. Smart Contract Wallets: The Future of Secure and Automated Transactions - Metana, accessed on September 13, 2025, https://metana.io/blog/smart-contract-wallets-the-future-of-secure-and-automated-transactions/
[6]. This is a repository copy of A Smart Contract for Boardroom Voting ..., accessed on September 13, 2025, https://eprints.whiterose.ac.uk/117996/1/e_voting_over_ethereum.pdf
[7]. (PDF) Performance Evaluation of E-Voting Based on Hyperledger ..., accessed on September 13, 2025, https://www.researchgate.net/publication/364032940_Performance_Evaluation_of_E-Voting_Based_on_Hyperledger_Fabric_Blockchain_Platform
[8]. Blockchain-Based E-Voting Mechanisms: A Survey and a Proposal - MDPI, accessed on September 13, 2025, https://www.mdpi.com/2673-8732/4/4/21

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

DOI: 10.17148/IARJSET.2025.121126

[9]. (PDF) Secure and Privacy-Preserving Voting System Using Zero ..., accessed on September 13, 2025, https://www.researchgate.net/publication/372823212_Secure_and_Privacy-Preserving_Voting_System_Using_Zero-Knowledge_Proofs

[10]. Zero-Knowledge Proof In Voting Systems - Meegle, accessed on September 13, 2025, https://www.meegle.com/en_us/topics/zero-knowledge-proofs/zero-knowledge-proof-in-voting-systems

[11]. (PDF) ZkSNARKs and Ticket-Based E-Voting: A Blockchain System ..., accessed on September 13, 2025, https://www.researchgate.net/publication/385250516_ZkSNARKs_and_Ticket-Based_E-Voting_A_Blockchain_System_Proof_of_Concept

[12]. Going from bad to worse: from Internet voting to blockchain voting ..., accessed on September 13, 2025, https://www.dci.mit.edu/projects/going-from-bad-to-worse-from-internet-voting-to-blockchain-voting

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License