**Paper 1: Cross–Platforming Web–Application of Electronic On–line Voting System on the Elections of Any Level**

The author presents a proposal for enhancing the architecture of web applications, specifically focusing on their application in secure voting systems. The main idea put forth is to utilize the Hierarchical Model-View-Controller (HMVC) modification, which offers several advantages in terms of the structure, maintainability, and security of web applications.

By incorporating the HMVC approach, the author aims to improve the overall design and functionality of web applications utilized in the voting process. This modification allows for a more organized and modular development approach, where the application components are divided into separate layers: the model, responsible for providing data and responding to controller commands; the view, responsible for presenting data to users and reacting to changes in the model; and the controller, acting as the link between the model and view, facilitating user interactions and notifying the model accordingly.

In addition to the HMVC modification, the proposal suggests the implementation of digital signatures to ensure the integrity and authenticity of voting results. Digital signatures serve as a means of verifying that the selected candidate by each voter remains unchanged and untampered with. By applying digital signatures, the author intends to provide an additional layer of security, preventing any potential compromise of the electronic voting system and instilling trust in the accuracy of the results.

The proposed enhancements to web application architecture aim to create a more robust and reliable platform for conducting secure elections. By leveraging the benefits of HMVC and incorporating mechanisms such as digital signatures, the author seeks to enhance the transparency, integrity, and trustworthiness of the voting process in electronic systems.

**Paper 2: IRJET- A Study on Decentralized EVoting System Using Blockchain Technology**

The author is discussing the issues present in the current election voting systems worldwide and proposing the use of electronic voting (e-voting) models based on blockchain technology to address these problems. They highlight that trust in the election system is a major concern in modern democracies, even in countries like India, the United States, and Japan. The major issues in the current voting system include vote rigging, hacking of electronic voting machines (EVMs), election manipulation, and polling booth capturing.

The paper aims to investigate the problems in the current voting systems and proposes the use of blockchain technology to create distributed electronic voting systems. It explores the application of blockchain as a service and discusses popular blockchain frameworks that offer solutions for electronic voting systems. The proposed system based on blockchain technology addresses the limitations of traditional voting systems while preserving participants' anonymity and allowing public inspection.

They emphasize that modern democracies rely on voting systems, and there is a growing need to attract young voters by adopting robust e-voting schemes. They discuss the functional and security requirements for a reliable e-voting scheme, including transparency, accuracy, auditability, integrity, secrecy/privacy, availability, and distribution of authority.

While existing research explores how blockchain can improve e-voting schemes and meet the listed requirements, the author points out that these papers often overlook the implementation challenges and limitations of blockchain technology in large-scale voting schemes. Therefore, this paper aims to explore both the possibilities and challenges of implementing e-voting schemes using blockchain technology.

The author discusses the limitations of traditional e-voting systems, such as secure digital identity management, anonymous vote-casting, individualized ballot processes, ballot casting verifiability by the voter, high initial setup costs, increasing security problems, lack of transparency and trust, and voting delays or inefficiencies related to remote/absentee voting.

They argue that blockchain technology can address many of these issues and make e-voting cheaper, easier, and more secure to implement. They explain the basic concepts of blockchain, its decentralized nature, and its immutability, which make it suitable for e-voting systems.

The working of the proposed e-voting system using blockchain is described, highlighting the steps of requesting to vote, casting a vote, encrypting votes, and adding the vote to the blockchain. The author also discusses the opportunities and benefits of blockchain in e-voting, such as secure and transparent voting records, increased voter participation, improved identity verification, faster vote tallying, elimination of ambiguities, greater transparency and clarity to voters, and improved security compared to outdated electronic voting platforms.

The author conveys the importance of addressing the trust and security issues in current voting systems by adopting e-voting models based on blockchain technology.

**Paper 3: Design and Development of Voting Data security for electronic voting**

The author's main objective is to present a comprehensive and secure e-voting system that maintains voter privacy and guarantees the accuracy and integrity of the voting process. The proposed system aims to address the shortcomings of traditional paper-based voting methods and provide a robust electronic alternative.

To achieve this, the author introduces a sophisticated cryptographic framework that combines several techniques to ensure the confidentiality, authenticity, and verifiability of voting data. The system utilizes cryptographic hash functions like SHA256 to securely store and retrieve sensitive information. Digital signatures are employed to authenticate the identity of voters and prevent tampering with their votes.

Additionally, the system employs RSA asymmetric encryption, which involves the use of public and private keys, to protect the transmission of voting data across various levels of the voting hierarchy. Each level, including voting places, districts, cities, states, and the country, follows a similar process to verify and count the votes. The focus of the paper is primarily on the district level, as it represents a fundamental unit of the voting system.

At the voting places, a client application is used to record and count the votes. Once the votes are encrypted and verified for confidentiality and integrity, they are transmitted to the higher levels. This process continues until the voting data reaches the country level, where the final tally is determined. By employing cryptographic measures at each stage, the system aims to thwart potential attacks, such as replay attacks, where recorded votes are maliciously reused, and packet sniffing, where an attacker intercepts and manipulates voting data.

They acknowledge the significance of prior research in the field of e-voting and highlights the key areas of concern, such as data encryption, voter privacy protection, and ensuring the verifiability of the vote counts. Several existing methods are discussed in relation to these concerns, emphasizing the importance of secure database design to uphold privacy and maintain data integrity.

In conclusion, the author argues that their proposed e-voting system effectively addresses the security issues associated with electronic voting. By leveraging cryptographic techniques and following a multi-level verification process, the system offers enhanced privacy protection for voters while ensuring the accuracy and trustworthiness of the voting results. The paper presents the proposed system as a potential replacement for traditional voting methods, offering a more efficient, secure, and transparent approach to democratic processes.

**Paper 4: Anonymous Remote Voting System**

In this paper, the author delves into the intricacies of a cryptographic protocol designed for anonymous remote voting. The primary goal is to address the shortcomings of traditional voting methods, which heavily rely on the human factor and are susceptible to manipulation. By leveraging cryptographic protocols, the author argues that it is possible to create a secure and reliable digital voting system.

The paper provides an overview of the specific cryptographic protocol implemented in a real-world voting system developed at the Institute of Computational Technologies SB RAS. This protocol employs a "blind" signature algorithm, originally introduced by David Chaum in 1982, which allows participants to generate and sign voting ballots without disclosing their choices to the server. The algorithm is based on the RSA protocol but can be adapted to other digital signature algorithms as well. The step-by-step process of the algorithm is outlined, emphasizing the generation of secret and open parameters, the creation of data for signature, and the signing process itself.

In addition to the blind signature algorithm, the paper also explores the establishment of an anonymous data transfer channel to ensure the privacy and security of the voting process. Various approaches are mentioned, including decentralized anonymous networks, hybrid networks, TOR, and VPN. The paper proposes a specific protocol within the voting system that probabilistically guarantees the anonymity of the original sender of voting ballots. By incorporating a random selection of participants and the server as potential recipients of the ballots, the protocol enhances the difficulty of determining the origin of each ballot.

They go on to discuss the potential integration of blockchain technology into the voting system. Blockchain, a popular method for storing and protecting information, offers cryptographic security and immutability. The author suggests that by recording voting transactions as blocks in a blockchain, the system can ensure the integrity of the data and prevent tampering. The openness of the blockchain database allows participants to verify the correctness of their votes and confirm the total number of voters, thus promoting transparency and accountability.

They aim to demonstrate the feasibility and advantages of an anonymous digital voting system backed by cryptographic protocols. The paper provides insights into the specific protocol utilized in a real-world voting system and highlights the benefits of incorporating an anonymous data transfer channel and blockchain technology. The presented system serves as a practical example that adheres to the security requirements of such voting systems, showcasing its potential to overcome the limitations of traditional voting methods.

**Paper 5: SecEVS : Secure Electronic Voting System Using Blockchain Technology**

The author is presenting a research paper that focuses on the implementation of blockchain technology in digital e-voting systems to address security issues and fulfill system requirements. The paper emphasizes the shift from paper-based voting systems to digital systems and highlights the advantages of digital e-voting, such as transparency, decentralization, irreversibility, and non-repudiation.

The abstract discusses the growth of digital e-voting systems, which has led to increased security and transparency concerns. To tackle these issues, the author proposes the use of blockchain technology in e-voting systems, offering a decentralized and secure solution. The blockchain is described as a distributed ledger containing voting results in the form of "bit-coins" stored across different locations.

The abstract also references previous research on electronic voting systems that have utilized blockchain technology, highlighting the limitations and vulnerabilities of some existing solutions. Examples of electronic voting systems from Estonia, Norway, and Scytl are mentioned, pointing out issues such as transparency, cyber attacks, and compromised confidentiality.

The proposed electronic voting system is specifically designed for university elections and aims to provide a secure and robust solution. The abstract mentions the participants in the system, including voters, election organizers, and inspectors. It outlines the framework of the digital voting system, which involves voter registration, authentication, candidate selection, encryption, signing, and the generation of blockchain blocks.

The security analysis of the proposed system includes considerations such as privacy of data transmission, voter confidentiality, prevention of duplication and forgery, and protection against system-level threats and attacks. The abstract asserts that the proposed system addresses these security concerns through the use of encryption, hashing, and other security measures.

The papers main objective is to introduce a secure and decentralized electronic voting system using blockchain technology, specifically targeting university elections. The abstract highlights the advantages of the proposed system and suggests that it offers improved security compared to existing solutions.

**Firebase Description**

The e-voting system we have created utilizes Firebase as the underlying technology stack. The Realtime Database serves as the backbone for the system's admin module, providing essential functionality for administrators. Within this module, administrators can add new users, capturing their phone numbers, election districts, constituencies, and district names. The module also includes a polling division feature, which encompasses candidates, a helpdesk with a helpline number and helpline email, registration locations, and voters' information. The Realtime Database efficiently stores crucial voter details, including names, passwords, village IDs, and voting choices (represented as "yes" or "no").

In addition to the Realtime Database, the e-voting system makes extensive use of the Firestore Database. This document-oriented database enables flexible and scalable data storage, ensuring efficient querying and seamless data synchronization. The Firestore Database is organized into various collections, each serving a specific purpose in the e-voting system's data management.

The "Answers" collection within Firestore captures responses to questions posed to candidates or voters, facilitating further analysis and evaluation. This collection plays a vital role in gathering insights and opinions from the participants.

To ensure the integrity of the voting process, the "Ballot Box" collection securely stores submitted votes. This collection guarantees the accuracy and confidentiality of each vote, maintaining the credibility of the electoral system.

Information about candidates participating in the election is stored in the "Candidates" collection. It includes profiles, credentials, party affiliations, and other relevant details, providing transparency and enabling voters to make informed choices.

The "Constituencies" collection contains specific details about constituencies, which are important subdivisions within election districts. This collection captures distinct geographic areas or demographic characteristics that influence the election process, aiding in efficient district-level management.

The "Districts" collection stores essential information about election districts, such as names, boundaries, and administrative details. It serves as a crucial reference for administrators and helps in organizing and overseeing the electoral process effectively.

The "Registrations" collection captures the registration details of voters, streamlining the process of verifying their eligibility to participate in the election. This collection helps maintain accurate voter records and facilitates authentication during the voting process.

The "Voters" collection stores comprehensive information about registered voters, including profiles, identification details, and other attributes necessary for authentication and verification. This collection serves as a central repository of voter data, ensuring accurate and up-to-date information for the election process.

The "Votes" collection records individual votes cast by registered voters. It ensures transparent and anonymous storage of each voter's choice, maintaining the privacy and integrity of the voting process.

The "Voting Station" collection stores information about designated voting stations, including locations, capacities, and logistical details. This collection assists in organizing and managing the physical voting locations efficiently.

Using Firebase and its Realtime Database and Firestore Database components offers a robust and scalable solution for modernizing the electoral process. By effectively utilizing these databases, the system streamlines administrative tasks, provides secure and efficient data storage, and ensures a transparent and reliable voting experience for administrators, candidates, and voters. The system's ability to handle user management, store voter information, facilitate candidate management, and enable efficient data querying makes it a valuable tool in revolutionizing the electoral process.