

ABSTRACT

A cloud-based e-KYC system provides a more efficient and flexible authentication method compared to the host based e-KYC authentication method where documents need to be validated via the centralized host. Essentially, the security and privacy of e-KYC related documents stored in the cloud becomes the crucial issue. Existing e-KYC platforms generally rely on strong authentication and apply traditional encryption to support their security and privacy requirement. In this model, the KYC system owner encrypts the file with their host's key and uploads it to the cloud. This method induces encryption dependency and communication and key management overheads. In this paper, we introduce a novel blockchain-based e-KYC scheme called e-KYC Trust Block based on the ciphertext policy attribute-based encryption (CP-ABE) method binding with the client consent enforcement to deliver trust, security and privacy compliance. SQL Server 2008 supports having a wide range of users access it at the same time. An instance of SQL Server 2008 includes the files that make up a set of databases and a copy of the DBMS software. Applications running on separate computers use a SQL Server 2008 communications component to transmit commands over a network to the SQL Server 2008 instance. When an application connects to an instance of SQL Server 2008, it can reference any of the databases in that instance that the user is authorized to access.

ABSTRACT

The consumption of enormous time in the election booth paves a vital role in reducing the voting percentage of a country. This can be overcome with the help of online voting system which provides you a user friendly and secured environment where user can easily vote from their location. For some years, online voting has emerged as a substitute for paper-based elections to reduce redundancies and anomalies. The recent point of view adopted in the past two decades shows that it has not been as successful for some period because of the cloud encryption and privacy observed. In our project we use cooperative blockchain to maintain information protection. We use cooperative blockchain, which means that an administrating entity owns the block chain (e.g., election commission), so therefore no unapproved access may be created from outside. This system requires a good internet connection of any private network sectors of an android operating system or an iOS operating system in mobile phones, laptops and tablets. Further the system collects the unique primary identification card, voter id and mobile number with respect to the voter's country to ensure no fraud or malpractice while voting. It professes to catch the protection and details the problems confronting the executive in block chain, and gives a better explanation of the online voting process. Through internet via voting the voter's time is minimized and the voting can be done quicker. Thus, the rate of voting can be increased by this online voting system.