International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Cloud Database Security in E-Voting System using Blockchain Technology

Shakkeera L, Hem Prasanth K C, Sabareesh, Sumaiya Begum, Sharmasth Vali

Abstract: ***In today's era, the cloud database security is one of the main concerns for any of the real time data accessing web/mobile applications. The cloud database protection involves accessibility and vulnerability of data, data protection, storage space, integrity and confidentiality on sensitive data. Building an electronic voting system that tries to completely fulfill the needs of the people has always been a challenge to achieve. The existing E-Voting System (E-VS) is not that much compatible with that of the current trends and does not assure to provide more security A lot of distributed ledger technologies which has been an exciting approach during existing election voting process. If we take a look on the ways of implying E-VS in a distribute ledger then Blockchain would be the right choice. As we all know that nowadays, Blockchain is one of the emerging technologies in the field of Information Technology. It normally stores information in batches called blocks which are linked together in a chronological way or method to form chain of blocks using cryptography techniques. During online voting process, many fraudulent activities happens which corrupt the entire election process. One of the major problems faced are fake voting which is obviously done by unauthorized people, inconvenient to reach to the respective places, average security level which may lead to the chances of an electoral fraud or any other malpractices.. Our proposed E-Voting System is mainly to protect the cloud database for real time data and to reduce the time consumption in voting and vote counting processes. Instead of standing in the queue for casting the vote, people can cast their votes from anywhere they want through online. The E-VS gives complete privacy and security for the online voting and makes it an ease for every individual to access it and cast their votes from anywhere possible with full pronounced security. In our proposed E-VS, Blockchain security concept called Consensus algorithm is implemented which makes it impossible for any unwanted activities to occur during election process. The E-VS system also achieves a higher level of security. Hence, the proposed system achieves data integrity, data confidentiality, eliminates storage overhead, and reduces time consumption for overall electronic voting system.***

Keywords: ***BlockChain, Proof of Work, Consensus, Cloud Database.***

Manuscript published on January 30, 2020.
* Correspondence Author
Shakkeera L*, Department of Information Technology, B.S.Abdur Rahman Crescent Institute of Science & Technology, Chennai, India. Email: lshakeera@crescent.education
Hem Pransanth K C, Department of Information Technology, B.S.Abdur Rahman Crescent Institute of Science & Technology, Chennai, India. Email: hemprasanth@outlook.com
Sabareesh, Department of Information Technology, B.S.Abdur Rahman Crescent Institute of Science & Technology, Chennai, India. Email: saba.mahesh@gmail.com
Sumaiya Begum I, Department of Information Technology, B.S.Abdur Rahman Crescent Institute of Science & Technology, Chennai, India. Email: sumaiyaimthiaz@gmail.com
Sharmasth Vali Y, Department of Computer Science and Engineering, Dhanalakshmi College of Engineering, Chennai, India. Email: vali566@gmail.com

I. INTRODUCTION

It's a well-known fact that the world runs under the rule of democracy and in India this should hold a major role in ruling the country for the well-being of people. Keeping that in mind if we look onto the main criteria of establishing a democratic society which can be achieved only by selecting the best candidate to rule the place. Electing the most suitable candidate by the process of election done by the people living in the country is a way of electing the right one and for the elections to be held for voting the deserving candidate should be taken as a serious task which is to be fulfilled with correct planning. The election commission of India keeps the election for state or country ruler respectively and according to the needs of it, and there are a lot of candidates volunteered for the post to win and amongst them the candidate with the highest number of voting given by people will win the election. During this process, there are a lot of fraudulent activities been done knowingly or unknowingly by the people or by the ones who want to desperately win. And more over the elections in India are done in a method in which the people have to go to their assigned voting booths to cast their votes which doesn't make it convenient for most of them to vote because of travelling and other issues. Here looking onto the need that every individual above the age of 18 should cast their vote without any inconvenience is our goal to achieve. So for that we have intended to create an E-Voting System (E-VS) by which people can use their smart phones and vote from anywhere they want. The lead concern of our proposed is to protect the cloud database by using the Blockchain technology for giving high security of votes in the database.

A. E-Voting System

Online voting system [1] or also known as Electronic voting, is something that uses the net so that people can cast their votes during the election process. The online way of voting can also be implied in representing the democratic setup in a way that increases the voters number in every other national stream of elections(local or national) and it might also define the innovations of democracy like the referendums. More or less the online way of voting is supremely used around the policies of the political system/politics. Overall purpose of voting through online is to increase the participation of the people to vote from anywhere through online on particular voting date.

B. Blockchain

Blockchain [2] is one of the emerging technologies in the field of Information Technology it normally stores the information in a form of batches that are called as blocks which are in a linked manner joined together in chronological way or method that forms a chain of blocks.

These blocks are well managed in a network which is peer-to-peer one for adhering to a protocol so that it gets inter-node communication and which are connected using cryptography techniques [14]. Initializing with the creation of block which might be included in the chain, few of the things should be done: Firstly, there is a puzzle in a cryptographic manner that is to be solved, which further leads to creation of new block. Then, the computer or node that solutions the given puzzle and spreads the answers to other node/ computers in the given network. This is assigned as Proof-of-Work. The miners after verifying the proof-of-work, if it's right, then a new block adds on to the following chain. This combination of the complex mathematical puzzles and the verification by a lot of computers or nodes notes this, we actually can trust every other block in chain, because this network itself will do the trust building and thus we will further have the way to directly connect or interact with all the data in reality. A Blockchain is basically distributed, an incontrovertible which is also immutable with a public ledger. This technology tends to works in four main features: (i) The ledger is to be existed in many different other locations i.e. there are no single point of fault or failure in the maintenance of the distributed ledger. (ii) There is a distributed control over the way in which that can be able to append new transactions to the ledger. (iii) Any proposed or new block to the ledger should have the previous version or hash of the block, by which it creates an immutable chain and from this we can assume where the name Blockchain came from, and this also prevents tampering by integrating the previous entries. (iv) There is a thing that the majority of the network nodes must reach a consensus so that before any new block of entries tries to become a permanent part of the ledger. These technological features in Blockchain also operates by using advanced cryptography, and by that it provides a security level which is equal or greater than any of the previously known database. The Blockchain technology is now considered by a lot of them to be the ideal tool, which is to be used to create the new modern democratic online voting system.

C. Cloud Computing

The cloud computing [3] is something that is a way of an on demand kind of availability which includes the computer resources, that can be the storage of data and the computational power, without having the direct way of actively management of the user. This term is normally used to explain the data centers that are available to many people or users through the net. The larger clouds, are verily predominating today, are often having the functions which are distributed over the multiple or many locations through the central servers. If the user has relatively close connection, then it may be designed to the edge server. If we put cloud computing in a metaphor then it's a group of the networked objects that provides the services need not have to be addressed individually or managed by the people/users; instead, the hardware and software of the entire providers-management suite can also be addressed as the amorphously cloud.

D. Private Cloud Database

The main concept cloud database implies that it is nothing but the database which normally runs or access on the platform of cloud computing, also that the general access for database is always provided in the form of a service which is (DaaS - Database as a Service). By using the private cloud database [4] the storing, accessing and retrieving of data becomes more simple as it can be accessed anywhere. The user details are encrypted and stored in cloud database using md5 and it is decrypted while retrieving. The services of the database makes all underlying software stack typically clear to all users.

E. Cloud Data Storage Security

To describe cloud data storage security [5] is nothing but the data protection, the applications, and infrastructures which are involved in the cloud computing. An efficient way of the security architecture should be able to recognize all issues which might arise with the security of management, and lately the security management will address the issues certainly with the security controls. The controls will be put in the place to actually safeguard all sort of weaknesses occurring in the allotted system and will try to reduce all effects of any sort of attack.

F. Database Protection using Consensus Algorithm

The Proof-of-work which is generally also known as same as the Consensus Algorithm [6] in the Blockchain technology. The concept of proof of work is that it makes things difficult for the fraudulent nodes to catch up with the honest nodes. The concept proof of work is also used beyond the context of Blockchain, which is in various web based framework and various secured mail servers to prevent fraud or spam. Main benefit are that it does not allow Denial of Service (DoS) attack and also impact of low stake on the possibilities of mining. Defense of the Do attack: proof of work imposes some restrictions or limits in actions of network. It requires lots of possible way of efforts to be implemented. The attacks need lots of the computational or computing power and also lot of duration to apply the calculations.

II. RELATED WORK

Bhuvanapriya. R, Kalaiselvi.V. K. G, Sivapriya. P and Rozil banu.S [7] Smart Voting System, the paper proposes a system were the way of voting is generally based on finger-print application that gives people an easy way of voting which is to guarantee 100% voting. This digital way of voting gives the list of all voters in the state who are above age 18 retrieving it from the Aadhaar card database. From this list the system will automatically give a voter id for people. This system enhances a secured online way of voting by using the concept of Biometric and Steganographic authentication. The Homomorphic techniques are used to encrypt the votes stored and later decrypt it during the time of results. The advantages of this system are that an automated voter id is generated.

This way of Digital voting will reduce the manual work and it implies RSA algorithm for the encryption and decryption and the mechanism of biometrics is used here to know whether the voter's identity is correctly given. The disadvantages includes that it is time consuming and it's not hardware independent, where there can be lack of security issues that are not assured to be the best for the database protection. J. Deepika, Kaliselvi S, Mahalakshmi S, and Agnes Shifani. S [8] Smart Electronic Voting System Based On Biometric Identification-Survey, the paper discusses about the implementation of an Electronic or Online Voting machine which is based on the Biometric way of Identification by using the GSM mode, message is sent to the voter's mobile that they have successfully given the desired vote and it will be recorded further. According to it, there will be no storage allowed where the votes are casted. By applying the embedded method and Internet of things (IoT) Technology, they will be able to send the casted data through online to MASTER servers unit. Normally finger print is used to compare with Aadhaar cards linked database and this also checks if vote is already been submitted. If someone has already voted then a buzzer alarm is enabled and an error message is sent, if not the EVM (Electronic voting machine) button is enabled and the vote is counted as usual. This system holds the advantages in a way that gives a secure way of voting with accurate and fast results. The GSM module is used to mainly elevate the security and speed of system and by using the IoT is easily passed on to the server for the quick announcement of results. The demerits are that it can retain the data only for 2 years which is sometimes necessary or not necessary and it also takes a lot of cost with no full assurance of high security of the database.

Usmani Z.A, Ajay Nair, Mukesh Panigrahi, andKaif Patanwala [9] Multi- Purpose Platform Independent Online Voting System,the paper focuses on the system which is like user needn't have to do any kind of account registrations to vote, they can simply show their Aadhaar number for their recognition. The main admin which is the one who creates the ballot will have a serial code which is unique by system and the admin will broadcast it to the people voting. After the user votes, it will be further encrypted using the Data Encryption Standard (DES) or Advanced Encryption Standard (AES) that is visible to the admin alone in a decrypted manner. The main advantages of this type of voting is that it is one of the different ways of voting which makes it easy and comfortable for the public to vote and there are different levels of security given to the database that will secures the votes casted. And the disadvantages of this is that it is expensive, complexity, more power utilization and more advanced way of security can be given for each type of voting system.

Annadate M N, Nivita Ravi Kaniampal, Pushkar Satish Naral [10] Online Voting System Using Biometric Verification, the paper proposes the system in a method which is an electoral system that is unbiased, completely automated for easing the voting by increasing security and reducing the counting time. It contains voter registration phase and the actual voting phase. In registration the database of the voter will be saved in repository containing voter's unique identification number, finger prints info. A biometric device which will verify the user from the database saved in repository by the communication of Wi-Fi module i.e. esp8266. If the voter is identified then authorization will approve that voter at the same time in other section of repository to vote, after getting authority from repository voting signal will be send from VVB by using ZigBee to voting console, when the voter votes then that vote will send to repository with the help of esp8266 and then the voting console will be reset after the voting of each candidate. The advantages of this system are that it is easy to implement and has a usage of reliable wireless connection. This keeps a track on Rigging and other malpractices and it also has the flexibility to vote from any booth irrespective of all the process. The demerits include the cost of the system and it has chances of high complexity. Tabish Ansari , Niraj Kumar, Sonalii Suryawanshi , Nilesh Yadav and Brijesh Chaurasia [11] Online Voting System linked with Aadhaar card, the work focuses on a system where we already acknowledge know that in India, Aadhaar card Number is Unique for everyone and it has biometric info of the people who wants to vote or not. This system has an elevated security that the voter's password for higher security is to be confirmed before that the vote is actually accepted in the main cloud database. The user can also cross check their vote with reference of unique id, which was generated by ECI (Election Commission of India. In this system people who find it inconvenient to vote because they are outside their allotted place now can also vote by using this way of voting. The advantage is that voter can submit their votes through internet without any problem of travelling to the voting booth. The Proxy type of voting or double type of voting is not at all possible, because it is more secured and is really easy to store the data. This is a mechanism in which it will not require any geographical restrictions of the voters i.e. Soldier's overseas can take part by casting online votes. The demerits can include the cost which can be of a concern to take care here.

Aishatu Shuaibu, Abubakar Mohammed and Arthur [12] The Adoption of Electronic Voting System, the paper discusses about how the system generates a more convenient voter's and candidate registration interface, an efficient voting interface, vote storage and count plus immediate result compilation etc. The outputs from the application page showing a list of all the registered voters, a list of all qualified candidates, and the results of the total vote count for each candidate in the Faculty of Science. A functionality test is also carried out on the developed system where few registered students appraised the system by filling out an electronic questionnaire. The system was also designed for faculty level voting in universities but can be easily adapted for smaller or larger scenarios. By this way it removes the unwanted activities that are linked with manual system and also this drastically reduces the time during the elections thus, resulting in huge financial savings. It is thus recommended for use in any election if well-adjusted but is not assured to be given the best security for the vote.

III. EXISTING SYSTEM

In existing voting system, recently the Election Commission of India has introduced a system which is the (VVPAT), which shows the voter's choice of vote being printed on a physical paper or receipt that is displayed for few seconds before it's been dropped into a sealed box or container.

A. Drawbacks in Existing System

The demerits of existing system are as follows:

- People have to wait in long queues to vote.
- Some of them find it very inconvenient to go to the voting booth to vote
- The paper trail would be added to the counting process, unless, a huge number of the votes were to gone missing somehow.
- Being more depended on labor manual intensive counting process might not turn out to be the best way forward.
- The manual authentication way of identifying people physically in your registration is something that we should try to avoid.

IV. PROPOSED SYSTEM

Our proposed system mainly focuses on the giving security to the votes [13] which is stored in the private cloud database, that is secured by using Blockchain Technology [15] [16] and this type of security level is not mentioned in the existing system. The Blockchain the security is given by using the Consensus algorithm which makes it impossible for any unwanted or any kind of fraud activities to occur during the election process yet also making it easy for tallying and generating the votes in a very short period of time. This proposed system is a pronounced online voting system which has availability to store in cloud database and is secured with the highest security of using Blockchain algorithm.

A. Advantages in Proposed System

The advantages of our proposed system are as follows:

- It makes it easy for the people to cast their votes from anywhere possible without any inconvenience.
- It is less time consuming, as in that people needn't have to wait in queues to get their chance to vote.
- This is a cost efficient system which does not have any hardware to spend a lot on it which is just extra wastage of money.
- It will be more secured and well organized than that of the manual work or way of monitoring, voting and securing the votes.
- By just using your Id and password you can easily login the voting site and cast your vote.
- Accordingly by using the Blockchain concept for giving higher security it makes it more reliable than that of the existing system.

B. Architecture Diagram

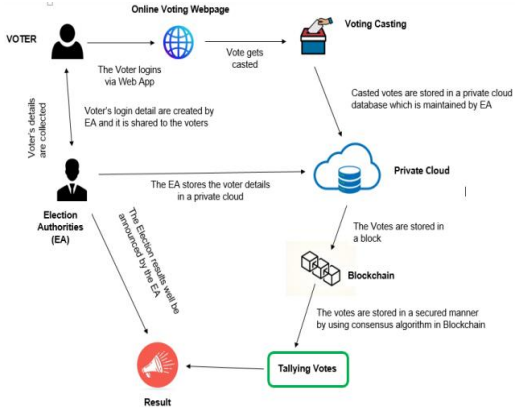

Fig. 1.Architecture Diagram

The Fig. 1 depicts the proposed architecture diagram of the E-Voting System which comprises of mainly the software that has an admin and the user which is the (voters) and the process starts with the user logs via web app then the admin (election authority) collects all the voters details two-three days before the election and then gives the voter its unique id and password which the voter will be using for logging in to caste the vote during the day of election. The voters then uses the id and password given by the admin in order to prove his authorization and then they casts the votes which are further on stored in a private cloud database which are maintained by Election Authority (EA). Later the votes are stored in a block. The votes are given higher security by using Blockchain consensus algorithm. The votes are further been tallied and then announced by the Election commission. The whole process is just to make the votes in the database more secured so that there are no unwanted activities held in the system during the online voting in election.

C. Block Diagram

The Fig. 2 depicts the proposed block diagram where the system is initialized with the creation of e-voting system user interface, then after the user finishes its voting these votes are stored a private cloud database which further leads to the method of pre-processing and storing of users votes in the database. This checks that there is no duplication of votes. All of this is secured using the Blockchain technology in which the consensus algorithm is used to give high security for the votes in the database. This block diagram explains the whole brief working the e-voting system.

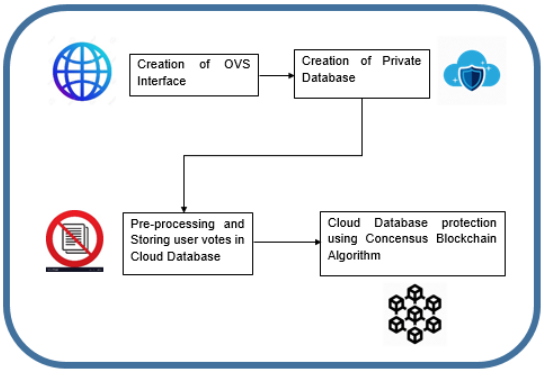

Fig. 2.Block diagram

D. Operational Workflow

The Fig. 3 depicts the proposed operational workflow diagram of the e-voting system which comprises of mainly the software that has an admin and the user which is the (voters) and the process starts with the user logs in via web app then the admin (election authority) collects all the voters details two- three days before the election and then gives the voter its unique id and password which the voter will be using for logging in to caste the vote during the day of election. The voters then uses the id and password given by the admin in order to prove his authorization and then they casts the votes which are further on stored in a private cloud database which are maintained by EA. Later the votes are stored in a block. The votes are given higher security by using Blockchain consensus algorithm.

The votes are stored in an encrypted manner using the SHA-256 algorithm for encryption. The votes are further been tallied and then announced by the Election commission.

The whole process is just to make the votes in the database more secured so that there are no unwanted activities held in the system during the online voting in election.

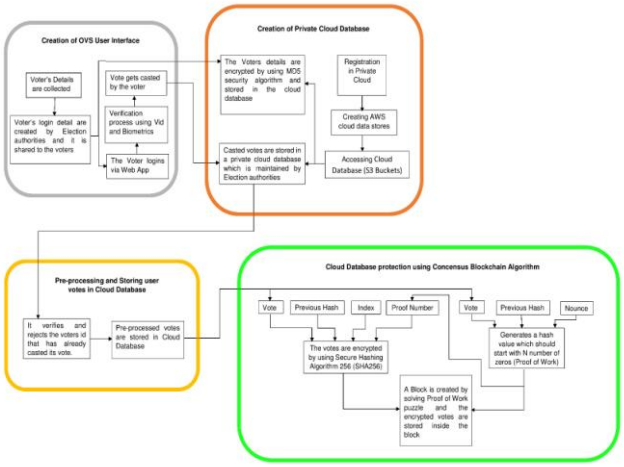

Fig. 3. Operational Workflow

V. MODULE IMPLEMENTATION

A. Creation of E-VS Interface

INPUT: Getting voters details.
OUTPUT: Votes are casted.

PROCESS: Every people who are the citizen of India need to give the respective details to the Election Authority. The Election Authority after collecting all the details from the user sends to the admin who manages those details. The admin once received all the details from the election authority creates an account for every user one week before the election date being announced. During the election time every user can login with their respective account. After they login with their id's they need to keep their fingerprint in order to ensure whether the particular person is casting his/her vote. Once the fingerprint is recognized the particular the user is allowed to cast their vote for the parties available. In our system once the user cast their vote they cannot vote for the second time since that option will be disabled in order to remove the duplication of votes. The Fig. 4 depicts the creation of E-VS user interface for proposed system.

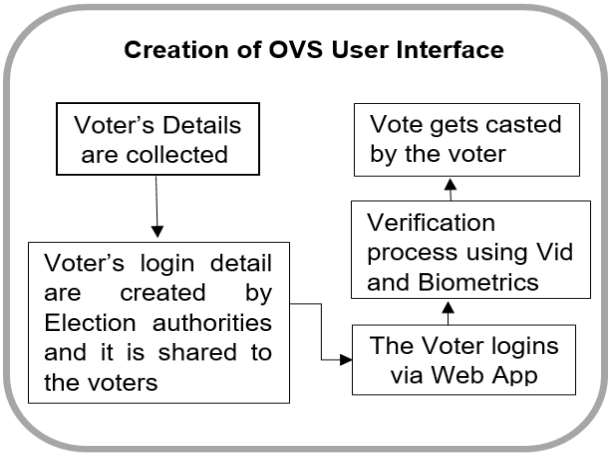

Fig. 4.Creation of E-VS User Interface

B. Creation of Private Cloud Database

INPUT: The casted votes are fetched from the user interface.
OUTPUT: The votes are stored in an encrypted manner in private cloud.

PROCESS: The Voter once cast their vote there must be a separate Database for storing the votes. In our proposed system we have implemented using cloud as a platform for storing the votes as well as the user details in the Database. The main concept cloud database implies that it is nothing but the database which normally runs or access on the platform of cloud computing, also that the general access for database is always provided in the form of a service which is (the Database as a Service). By using the private cloud database the storing, accessing and retrieving of data becomes more simple as it can be accessed anywhere. The user details are encrypted and stored in cloud database using md5 and it is decrypted while retrieving. The services of the database makes all underlying software stack typically clear to all users. The Fig. 5 depicts the creation of private cloud database for proposed system.

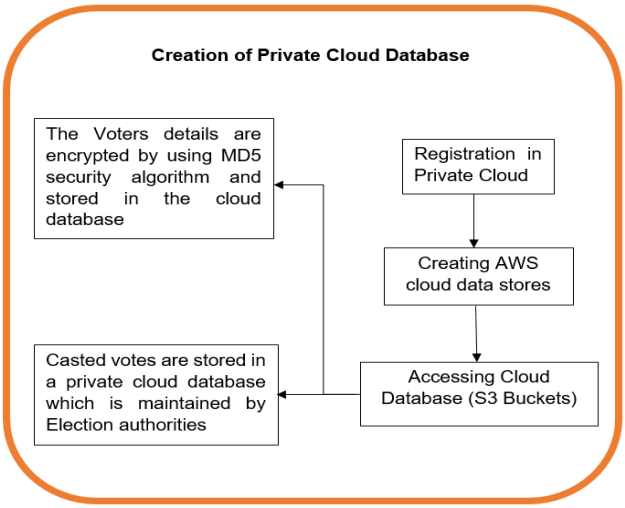

Fig. 5.Creation of Private Cloud Database

C. Pre-processing and Storing User Votes in Cloud Database

INPUT: The votes are stored in an encrypted manner in private cloud.
OUTPUT: It verifies and rejects the votes id that has already casted its vote.

PROCESS: Once the votes are collected from the private cloud, the preprocessing operation is done. The voter's unique id gets expired within some time and this makes no unauthorized person to caste the vote. It eliminates the duplicates in the form of repeated and redundant vote data. The preprocessed votes are stored in private cloud database. It is designed to give 99.99% of availability of objects and 99.99% durability. The Fig. 6 depicts Pre-processing and Storing user votes in Cloud Database.

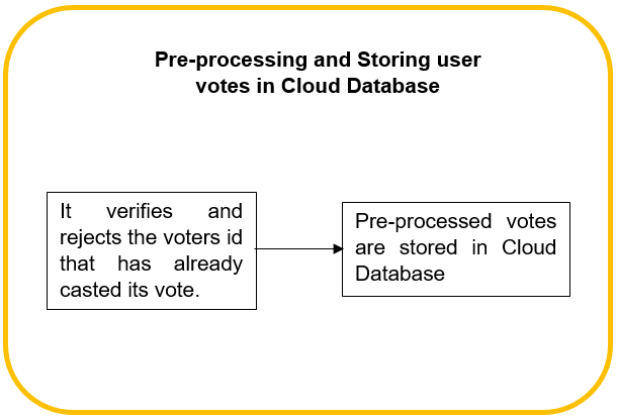

Fig. 6.Pre-processing and Storing User Votes in Cloud Database

D. Cloud Database Protection using Consensus BlockChain Algorithm

INPUT: The votes are stored in a block.
OUTPUT: The votes are stored in an encrypted manner using consensus algorithm.

PROCESS: The Consensus algorithm is a mechanism in which at a Decentralized network all nodes comes to an agreement and makes decision. In a centralized system every nodes simply accepts the agreement whatever the central host says. In Decentralized network there is no such central host and each node does not trust any other node. Generally in this algorithm, for a node, to create a block and broadcast it to other nodes, it needs to do some computation work and once it completes, it will broadcast it to other nodes. By this way all the other nodes will receive the block and verify whether it the proof-of-work requirements. If the block is right and if meets the proof-of-work requirements then this gets broadcasts it to the peers. If it does not meet the proof-of-work requirements, then the immediate peers rejects the block. By doing this process the block will be added to the local copy of Blockchain. This prevents the denial of service attack. The Proof-of-work which is generally also known as same as the Consensus Algorithm in the Blockchain technology. The concept of proof of work is that it makes things difficult for the fraudulent nodes to catch up with the honest nodes. The concept proof of work is also used beyond the context of Blockchain, which is in various web based framework and various secured mail servers to prevent fraud or spam. The Fig. 7 depicts Cloud database protection using proposed consensus Blockchain algorithm.

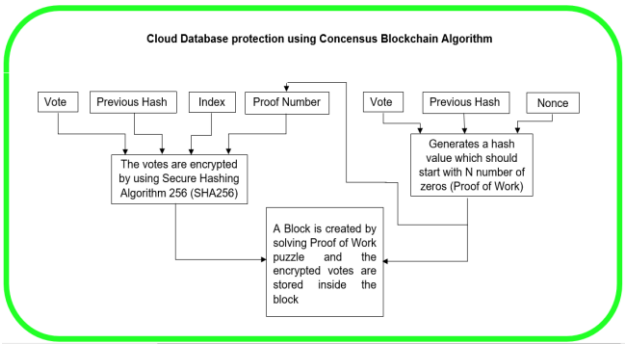

Fig. 7.Cloud database protection using Consensus Blockchain algorithm

a. Proof of work in Blockchain

- It is to find or generate a value which is very difficult to generate in terms of CPU power.
- It should be very easily verifiable.

Example -Proof of Work in Blockchain

The Figure 8 shows the significance of Proof-of-work using Consensus Blockchain algorithm. Initially, it contains leading zeros. If we look in the block structure we will have: Block No, Vote Data, and other fields, which field can be used to generate such N leading zeros in block hash. One such field is the NONCE field: We will generate or we will find a value of Nonce (may be by brute force) starting from zero to some value such that the combination of nonce and block data which has been generated including the hash value of previous block comes out with the required leading zeros. You can set the value of N as per the difficulty of Proof of work you want: more the value of N, more it will be difficult for the computer to find such value with that many leading zeros. The computational required is exponential to the no. of leading zeros required in proof of work algorithm. Once the CPU power has be expended to satisfy the criteria of proof of work, the proof of work cannot be changed. Hence if the data is changed, the block is changed, the proof of work has to be redone again.

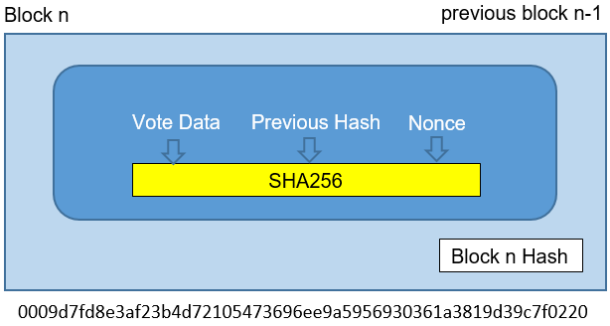

Fig. 8.Significance of Proof-of-work

b. Proof of work in Blockchain

Algorithm 1 – Valid Proof and Proof of Work
INPUT: Vote data, previous block hash and nonce value
OUTPUT: Highly secured vote data is stored in a block.
Step 1: dbrowx, Last hash and proof are passed as arguments.
Step 2: Converting all arguments to string type and encoding.
Step 3: 256 bit conversion of guess, and then return to main function with the expression
Guess_hash[0:2] == '00'
Step 4: Initializing lastblock as [–1] of Blockchain, then converting lastblock to hash.
Step 5: Giving proof's value as 0
Step 6: While proof is not valid, increment proof and return the same.

Algorithm 2 – Blockchain Generation
Step 1: Declaring error result and error type as global variables.
Step 2: If the variable role Object has value None, then return the URL for Error.

Step 3: Checking to see if can Role is false, if so return result as "Permission denied" and return URL for error.
Step 4: Initialize, establish connection with SQL server, and execute specific SQL command.
Step 5: In a while loop, blocks created are initialized with dbrow[] array.
Step 6: Blocks created are printed.
Step 7: If the blocks created are not = 0, establish connection through the command connx = pypyodbc.connect('Driver={SQLServer};Server=HEM\SQL EXPRESS1;Integrated_Security=true;Database=E-Voting', autocommit=True)
Step 8: Executing a SQL command and giving value of cursor.fetchone() to dbrowx.
Step 9: After checking of drowx, repeating Step7, Step8 for dbrowy.
Step 10: Closing both database connections.
Step 11: Executing SQL command sqlcmd = "SELECT * FROM VoteData WHERE isBlockChainGenerated = 0 or isBlockChainGenerated is null ORDER BY voteID". After establishing connection with database.
Step 12: Repeating Step11,then assigning values for block_serialized and block_hash with block_serialized = json.dumps(str(dbrow[1])+" "+str(dbrow[2]), sort_keys=True).encode('utf-8') and hashlib.sha256(block_serialized).hexdigest() respectively.
Step 13: Establishing new connection, executing SQL command with block hash and previous hash and then closing the connection.
Step 14: Returning blockchaingeneration webpage html link.
Step 15: Routing to blockchain report.
Step 16: Step2 and Step3 are repeated, except for process
Step 17: Establishing connections with EVoting, cursor commandexecution, assigning empty array for records[].
Step 18: While checking for dbrow, establishing new connections and setting political party as None.
Step 19: Executing a new SQL command for username and userid and then assigning user as None.
Step 20: Checking for user in row2, then initializing row as row = VoteDataModel(dbrow[0],dbrow[1],.. PoliticalParty=PoliticalParty, User=User).
Step 21: Appending row in records.
Step 22: Closing all connections.
Step 23: Returning render template "BlockchainReport" html document.
Step 24: Importing ElectionResultModel from ElectionResultModel.
Step 25: Routing to Election Result.

The Fig. 9 depicts the creation of a Block in a Blockchain. In each block there will be a miner which maintains the block in Blockchain network. The miner encodes the vote data and last block hash into string format and then the miner hashes the encoded data by using Secure Hashing Algorithm (SHA-256) which will result in 64bit character. The miner has to guess a hash value which should start with N number of zeros (Nonce) which is a cryptographic puzzle (Proof-of-work) need to be solved by the miners. If the miner solves the puzzle which satisfies the nonce value, the miner gets rewarded and a new block will be created by the miner and gets chained with other blocks in chronological order and so the data will be stored with high security which is provided by Blockchain network.

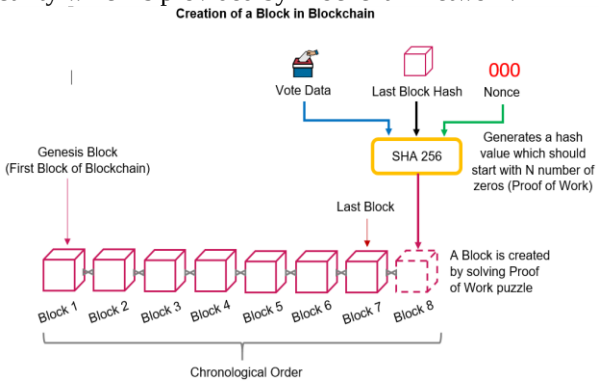

Fig. 9.Creation of a Block in a Blockchain

VI. PERFORMANCE ANALYSIS

The performance of all the proposed modules are improved and accordingly analyzed which promotes results that are effective that are compared to that of the existing and the proposed in a secured cloud setup.

A. Performance Metrics

The performance metrics generally measures and gradually analysis the process which is involved in the creating and providing of trusted works to the users who asks for services for various kinds of processes.
The given below are the following performance metrics used to analyze the proposed system with already existing ways.
Data Integrity - The integrity of data which stored in the cloud storage.
Data Confidentiality - The user authentication and authorization to access the data without affecting the user and data privileges.
Storage Space – The space required to process the data in cloud storage. Storage space analysis is used to identify the trustable storage services.
Computation Time - The time required to process the data to and from the cloud storage.

VII. RESULT ANALYSIS

A. Data Integrity V Number of Votes

Fig. 10 depicts the percentage of data integrity for both existing E-VS and proposed system for E-Voting System Application with Blockchain technology (E-VS_BC). Once every user castes their votes to their respective parties then these votes are to be stored in a cloud database. Then the votes are kept safe and secure in the cloud database till the election results will be announced. The hackers may try to steal or manipulate the casted votes using active and passive modes of attacks. In order to avoid such kind of attacks, the proposed system E-VS_BC uses the Consensus Blockchain approach to secure those votes from hackers which is to be hacked. Those votes are stored in the cloud database safely and therefore the chances of the hackers attempting to attack the vote data is quite difficult or not possible when compared to the existing system.

The existing system applies security techniques only in the form of traditional encryption and decryption cryptographic techniques. If the number of votes are increased from 100 – 500 based on the clock time period, in proposed system E-VS_BC,

the originality of the casted votes are maintained and monitored around 75-80% when compared to existing system. Table-I represents the numerical points of Fig. 10.

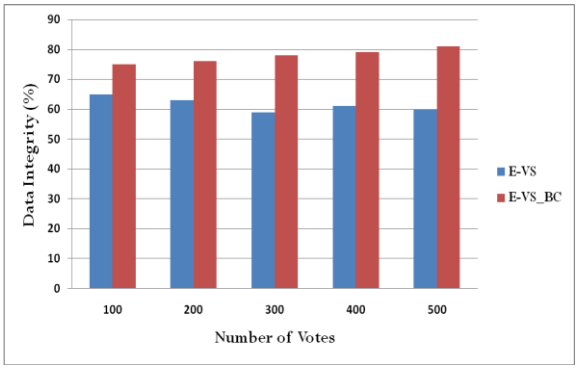

Fig. 10. Data Integrity Vs Number of Votes

Table-I: Percentage of Data Integrity Vs Number of Votes

Number of Votes	Data Integrity (%)	
	E-VS	E-VS_BC
100	65	75
200	63	76
300	59	78
400	61	79
500	60	81

B. Data Confidentiality Vs Number of Votes

The Fig. 11 depicts the percentage of data confidentiality for the existing E-VS and proposed system E-VS_BC when number of user accessing the voting system during election dates. Since it is an online voting web application where the security plays a major role for this type of critical access. As a cloud database administrator, the cloud users can vote only once with their corresponding login id and secret password. Once the votes are placed at the first time, the vote option will be disabled if the users try to attempt for second time. In this way, the user authentication and authorization is achieved in our proposed system to access the data without affecting the user and data privileges. The existing system was failed to implement the data confidentiality approach and hence there is a more chance of data fraudulent to occur. The existing electronic voting system implemented with only authorized user and password cryptographic technique. So our proposed system has comparatively improved data confidentiality around 73-80% when the number of users vary from 10-50 than the existing system approach. Table-II shows the corresponding values of Fig. 11.

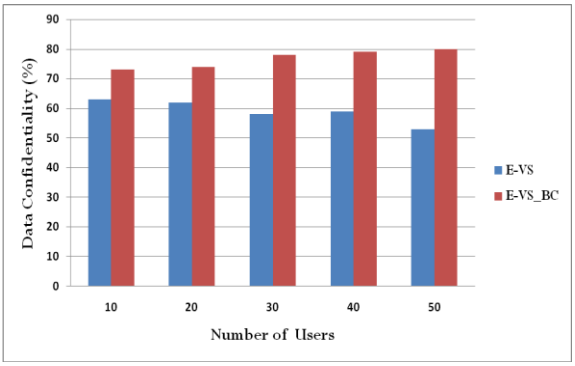

Fig. 11. Data Confidentiality Vs Number of Users

Table-II: Percentage of Data Confidentiality Vs Number of Users

Number of Users	Data Confidentiality (%)	
	E-VS	E-VS_BC
10	63	73
20	62	74
30	58	78
40	59	79
50	53	80

C. Storage Space Vs Clock Time

The Fig. 12 depicts the storage space utilization for both the existing E-VS and proposed system of E-VS_BC. The storage space is required to process the data in cloud database. In our proposed system, once the every user cast their votes, the votes are stored in secure cloud database. When any hacker attempts to access and manipulate the vote data in the cloud database the storage space may increase. The proposed system does not allow the hacker to access the cloud data by applying data confidentiality and data integrity measures. But in the existing system, the cloud storage will be hacked easily by applying intelligent cryptanalysis techniques, in this way the storage space is increased in terms of increasing the storage overhead. If the clock time increases from 900sec-1020sec, our proposed system eliminates the storage overhead around 5-10% and thus inturn analysis the storage space which is used to identify the trustable storage services. Table-III shows the corresponding numeric values of Fig. 12.

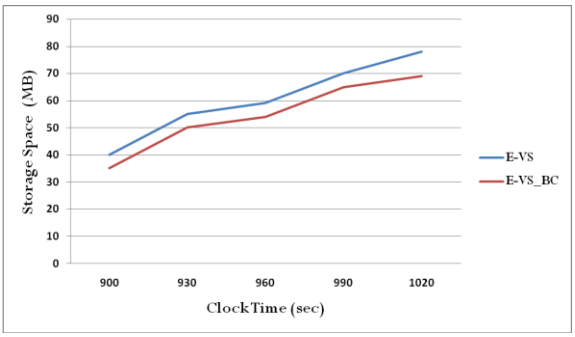

Fig. 12. Stroage Space Vs Clock Time

Table-III: Storage Space Vs Clock Time

Clock Time (sec)	Storage Space (MB)	
	E-VS	E-VS_BC
900	40	35
930	55	50
960	59	54
990	70	65
1020	78	69

D. Computation Time Vs Clock Time

The Fig. 13 depicts the computation time for both the existing E-VS and proposed system of E-VS_BC. In existing system, the hacker can easily access the cloud data that inturn increases the storage overhead and storage space. So, the system will take more computation time to process the vote data to and from cloud storage. But in proposed system, the chances of hacking by the hackers is very less as it is implemented using the concept of Blockchain, it takes very less time to complete the overall process. In proposed system, the computation time is reduced around 10-15% when compared to existing system. Table-IV shows the corresponding numeric values of Fig. 13.

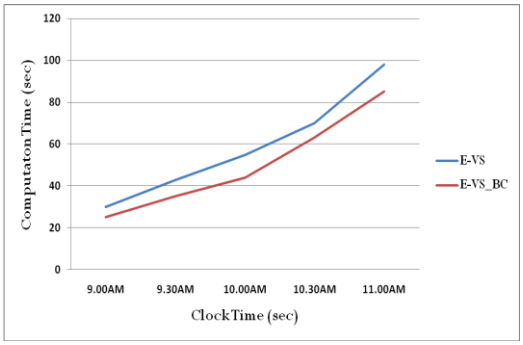

Fig. 13. Computation Time Vs Clock Time

Table-IV: Computation Time Vs Clock Time

Clock Time (sec)	Computation Time (sec)	
	E-VS	E-VS_BC
9.00AM	30	25
9.30AM	43	35
10.00AM	55	44
10.30AM	70	63
11.00AM	98	85

VIII. CONCULSION AND FUTURE WORK

A. Conclusion

The cloud database security is one of the major challenges in today's research trends. Many of the applications are developed without the concern of the security threats. The private cloud databases are created for data computation and data storage. The outcome of the proposed electronic voting system is to provide higher amount of security so that there is no way of any threats or fraud activities to be done throughout. The proposed system is implemented using Blockchain technology for giving high reliability and security using the algorithm called Consensus/Proof-of-Work. The system uses MD5 algorithm for user encryption and decryption and SHA-256 algorithm for vote encryption and decryption. The main idea of the proposed system is to highly secure the cloud database which contains the results of the election process from any kind of attacks or fraudulent activities which will disrupt the entire process. Finally, the proposed system is solely to help the people to find it easy and convenient to in electronic voting system.

B. Future Work

The future work tends to focus on the following directions:

- Extend and implement the proposed system in public cloud secure database.
- Implement data mining algorithms for pre-processing and data selection in cloud database for voting application.

REFERENCES

1. Paul U. Umoren, Idongesit E Eteng, and Ugochi D Ahunanya, "An Online Voting System for Colleges and Universities: A Case Study of National Association of Science Students (NASS)" , vol. 22, no. 2, 2018.
2. Zibin Zheng, Xiangping Chen, and Huaimin Wang, Hongning Dai and Shaoan Xie, " An Overview of Blockchain Technology – Architecture, Consensus, Furture Trends.", *6th International conference on Big Data (IEEE)*, 2017.
3. Priyanshu Srivastava and Rizwan Khan," A Review Paper on Cloud Computing", *International Journals of Advanced Research in Computer Science and Software Engineering*, vol. 8, no. 6, June2018.
4. Priyanka Madhiraju , M.Praveen Kumar," A research on simple way to a Private Cloud and its uses", *International Research Journal of Engineering and Technology (IRJET)*, vol.. 4, no. 1, Jan 2017.
5. A. Venkatesh, Marrynal. S and Eastaff," A Study of Data Storage Security Issues in Cloud Computing", *International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT)*, vol. 3, no. 1, 2018.
6. Giang- Truong Nguyen and Kyungbaek Kim," A Survey about Consensus Algorithms used in Blockchain", *Journal of Information Processing System*, vol. 14, no.1, February 2018.
7. Bhuvanapriya.R, Rozil banu.S, Sivapriya.P and Kalaiselvi.V.K.G, "Smart Voting System", *Second International Conference Paper on Computing and Communication Technologies(ICCCT'17)*
8. Deepika J, Kaliselvi S, Mahalakshmi S, and Agnes Shifani. S, "Smart Electronic Voting System Based on Biometric Identification-Survey", *Third International Conference Papers on Science Technology Engineering and Management (ICONSTEM)*, 2017.
9. Usmani Z A, Kaif Patanwala, Mukesh Panigrahi and Ajay Nair, "Multi-Purpose Platform Independent Online Voting System", *International Conference on Innovations in Information, Embedded and Communication system (ICIIECS)*, 2017.
10. Annadate M N, Nivita Ravi Kaniampal, Pushkar Satish Naral, "Online Voting System Using Biometric Verification", *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)*, 2017.
11. Tabish Ansari , Brijesh Chaurasia, Niraj Kumar, Nilesh Yadav, Sonalii Suryawanshi, "Online Voting System linked with AADHAAR Card", *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)*, 2017.
12. Aishatu Shuaibu1, Abubakar Mohammed2, Arthur Ume " The Adoption of Electronic Voting System", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 7, no. 3, March 2017.
13. Mr. M. Sanjai1, Dr. R. Umamaheswari2, Mr. S. Muthuraj "Advanced Technology in Secured Online Voting System", *International Research Journal of Engineering and Technology (IRJET)*, vol. 5, no. 4, April 4 2018.
14. Lauretha Rura1, Biju Issac and Manas Kumar Haldar ,"Online Voting System Based on Image Steganography and Visual Cryptography" *International Journal of Computing and Information Technology*, vol. 25, no. 1, March 2017.

15. Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, Gísli Hjálmtýsson, "Blockchain-Based E-Voting System", *IEEE 11th International Conference on Cloud Computing*, 2018.
16. Zibin Zheng, Hong-Ning Dai," Blockchain Challenges and Opportunities: A Survey", *International Journal of Web and Grid Services* , 2018.

AUTHORS PROFILE

Dr.L.Shakkeera is working as an Assistant Professor (Selection Grade) at B.S.Abdur Rahman Crescent Institute of Science & Technology, Chennai, Tamil Nadu, India since 2006. She has received B.Tech. in Information Technology from Crescent Engineering College affiliated to Anna University, Tamilnadu, India in 2005, M.E in Computer Science and Engineering from B.S.Abdur Rahman Crescent Engineering College affiliated to Anna University, Tamilnadu, India in 2010. She completed her Ph.D degree from B.S.Abdur Rahman Crescent Institute of Science & Technology, Chennai in 2018. She has a teaching experience of 14 years. She has published more than 20 research publications in refereed International/National Journals and 15 publications in International/National Conferences. Her areas of specializations are Cloud Computing, Mobile Cloud Computing, Network Security, IoT, Data Mining, Mobile Ad-Hoc Networks and Web Services. She has ACM & ISTE membership.

Hem Prasanth.K.C is a student at B.S. Abdur Rahman Crescent Institute of Science & Technology, Chennai, Tamil Nadu, India. He is currently pursuing his B.Tech in Information Technology degree in B.S.Abdur Rahman Crescent Institute of Science & Technology, Vandalur, Chennai. His areas of interest are Blockchain, IoT and Web Technology.

Sabareesh.M is a student at B.S. Abdur Rahman Crescent Institute of Science & Technology, Chennai, Tamil Nadu, India. He is currently pursuing his B.Tech in Information Technology degree in B.S.Abdur Rahman Crescent Institute of Science & Technology, Vandalur, Chennai. His areas of interest are Web Technology and Big Data.

Sumaiya Begum.I is a student at B.S. Abdur Rahman Crescent Institute of Science & Technology, Chennai, Tamil Nadu, India. She is currently pursuing her B.Tech in Information Technology degree in B.S.Abdur Rahman Crescent Institute of Science & Technology, Vandalur, Chennai. Her areas of interest are Database Management, Operating Systems and IoT.

Sharmasth Vali Y is working as Assistant Professor at Dhanalakshmi College of Engineering, Chennai, Tamilnadu, India since 2013. He has received his B.Tech. in Computer Science and Engineering from Shadan College of Engineering and Technology, JNTU Hyderabad in 2007, M.E. in Computer Science and Engineering from B.S.Abdur Rahman Crescent Engineering College, Anna University in 2009. He is presently doing Ph.D in Information Technology from B. S. Abdur Rahman Crescent Institute of Science & Technology, Chennai, Tamil Nadu, India. He has a teaching experience of 9 years. He has published more than 10 research publications in refereed International/National Journals and International/National Conferences. His areas of specializations are Network Security, Intrusion Detection and Prevention Systems, cloud computing and Mobile Ad-Hoc Networks.