CrypEvote: An advanced Lightweight e-Voting System using Cryptography

Warish Patel
Computer Science & Engineering Department
Parul Institute of Engineering And Technology,
Parul University Vadodara, GJ, India.

Monal Patel
Civil Engineering Department
Parul Institute of Engineering And Technology,
Parul University Vadodara, GJ, India.

Bhupendra Ramani
Information Technology Department
Parul Institute of Engineering And Technology, Parul University
Vadodara, GJ, India.

***Abstract*— These days just hardly any individuals go for casting a ballot because of their tight schedule and also it will useful for pandemic like COVID-19. There are numerous reasons, few might be everybody needs to go to voting center, we need to remain in a long line, many might be drained due to their tight schedule. So we have created web based voting system. But this system has some drawback. Phishing attackers legitimately get the passwords from the client and they go into the important sites with right secrete password. Consider a web based polling system for corporate organizations, polling is occurring once in a year to choose the president or secretary or key managers of the organization. At present system every one of the voters needs to assemble at one spot on polling day and put their vote. In this methodology we are utilizing another plan which is known as Cryptography. In this plan we are utilizing visual data for security. Here we are partitioning unique picture into two offers which are put away in isolated database. At whatever point these two offers are stacked with one another we get the original picture. When we get the original picture it tends to be utilized as secret password. This system is extremely helpful and ok for online remote voting. This system is electronic application so it can be assessed well by any approved individual anyplace on the planet through web.**

Keywords—Salsa20 Key Generator, Secret Password, Secret PartyName, Verification, Vote Online, Cryptography, Ensemble Advance java, Blockchain, COVID-19

I. INTRODUCTION

Elections are held throughout the whole site. But voting stations must be used for voting by voters. The process of the political race is exceptionally complex and requires a lot of voting. A lot of arrangements have to be concluded. It Manual work includes. Elections in government elections are conducted wisely. To throw Vote, voting at the voting website must be available. Vote.

This can decrease support for voters; This undertaking is made simple by based polling. Cryptography includes casting security Vote. Implementing such systems is important. This reduces work, causing casting Easy to use and productive ballot. Encoding picture is a cryptography system. The customer is approached in this system to upload a security image during registration. The customer will receive a security portion via email. The share will be encrypted. The customer can access Edit voting details system whenever. The client must upload security only during voting.

If the share is wrong, voting cannot take place because the safety share is generated by using It cannot be predicted of random pixels, a genuine picture. Moreover, the share cannot be received Any other customer or non-approved party because it is sent safely by email. Casting a vote will be successful only when it is uploaded the correct share of that customer. Fraudsters will send false messages or set up falsified websites. Phishing is an online theft of identity, in which Internet users are tried by fraudsters Unlawful websites for personal information. Typically, phishing tricks are shown as spam or pop-ups, often difficult to identify. If you collect your own data, the fraudsters They can use it for all kinds of identity fraud, with your big credit and your big name. hazard. In the design of their fake sites, Phishers are becoming increasingly modern. As phishing is one of the most disappointing data fraud types, it is important that you become comfortable with different types of phishing tricks just as well as find out how to prepare. The best known and easiest way to securing a system asset is A unique name and password are assigned to it. [13]

Cryptography is an examination of data security. It was actually used as Methods of safe communication between government and people. Cryptography today is a basis for advanced safety technologies to guarantee Open and shut network data and assets. Validation is a way to check a person or thing's personality. [15]

The objective is to check that you have the true deal at the point where you confirm an item. At the point where a person is confirmed, you don't manage an impostor is to check. Requests to implement applications Mechanisms of themselves to determine a user's permissions level. Requests: often do this by maintaining private records containing customer names Access authorized. For example, database applications keep private approval regularly

The fields control tables in a record which may be viewed or changed by a specific client. There are several types of Internet-based applications. The Web-based voting system is one of them. There are some who argue for the benefits of talking, openness, voting from home and the risks of uncoordinated accommodation, infringement of mystery and

obscurity and change of the consequences of a political race, for example. A number of people argue for improved speed and accuracy. This research project focuses on preventing phishing attacks and ensuring Internet voting authentication using Cryptography. Cryptography is a special encryption strategy for hiding data in pictures, so that human vision can decrypt when the right keyframe is used.

A. Problem Statement

The in any case of an election, three main questions were found which are typical for the electorate to cause problems.

First of all, voters often wait for long queues during the elections cycle leading to an exhausted situation before you get the chance to throw your hand voting and also because the queue exists, the aspirants and the campaign teams Use the situation often as both parties are electorally compelled to vote for them Present physically.

Third, an accurate number of votes is necessary to manually vote, so that the results of the winning candidate are known after the vote. Due to several factors in human error and voting error, the results of manual voting were challenged. How can the number of votes in voting centers be accurately measured?

Finally, manual voting takes a lot of time, because voters have to be there It takes very long in person and when voters are in another, it is not possible in town or elsewhere.

The above factors combined to determine a situation in which each vote is deemed unreliable and fair. Thus, a vacuum exists for a program with functions that would reduce the inefficiencies of the existing system.

B. Purpose Of Study

The main purpose of this study is to provide a means of voting for critical and confidential internal decisions of companies.

C. Significant Of The Study

This study would help to increase trust throughout the election and ease various problems, such as the long queues, time loss and lack of credibility, that previously blocked the system. It also ensures that results are readily available and the cost of carrying out elections is reduced overall. This would increase voters' willingness to participate in the elections and eventually lead to a credible election. It allows voters to cast their ballots. The online voting system reduces time spent in the polling stations making long queues in elections. The system should enhance counting speed and accuracy. The system authenticates the user so that only legible voters can vote.

1.5 Aims & Objectives

The main aim of this study is the prevention and authentication of phishing attacks and Internet voting by cryptography that can achieve the following goals:

- Facility for critical and confidential internal business decisions to cast votes.
- Because few people are going to the voting center because of their close schedules or remote work, to increase the number of votes in our country;
- Many people can vote with this system from any location in the word Must go to any center for voting.
- To create a secure online voting system with an algorithm for cryptography technical.
- Reduce the falsified vote and ensure the safety of phishing attackersSystem.

D. Scope Of Study

The scope of the research project is to develop an online voting system using the cryptography password for each voter per election, which will allow voters to vote regardless of their location. Number growing, It is easier and more convenient to vote for voters as individuals, especially those overseas.

E. Limitation of study

The time factor is the greatest barrier to this research project being carried out successfully in the six months, the internet is another barrier for the research project since internet data in Ghana is currently extremely expensive, as the system development is also another factor since every feature needs to be code after each feature as all activity takes place and financial constraints are lastly imposed.

F. Assumptions

The implementation of the new system is expected to rapidly enhance people's economic and social-political lives. Phishing, grumbling and electoral abuse will not be possible.

G. Title Justification

This research project would leverage the foundation of an earlier e-voting system developed and which uses the identification of cryptography during registration. The aim is to increase the ability to universally access the voting request, which means that eligible voters are not constrained by their physical location and the use of the image captcha produced after the voting system has been initiated.

H. Summary

In this chapter, the research project and research field are introduced. It includes the main problems, i.e. the objectives and objectives, to be resolved by the research project. The section as Well contains the scope of the research project to be covered.

II. LITERATURE REVIEW

After this comparative table was created to compare the method and the limitations/future scope, various papers are explained individually.There are different types of voting systems from the early days to the developments in technology. That is explained in this chapter. Develop voting schemes using ICT resources to provide more efficient voting services than conventional paper-based voting methods.[21]

The growth of the world's digital culture, on the other hand, has given rise to concerns about why voting is not possible in the same way as buying products from home or online.

Promise to simplify and improve the democratic process for political parties, Candidates, the electoral government and, above all, the electorate. Various types of Varying degrees of Internet or remote electronic voting systems Achievement. Some systems worked well, but some were even scrapped. Before implementing because of security issues.

2.2 Related Works

A. The system of paper voting

The paper voting system is the standard voting system which is widely used. It will usually be used before the electronic voting system is implemented. Includes paper and seal ballots in the paper voting systems. Each voter uses and does not share one ballot. The inconvenience of this system is: (i) time consuming; (ii) low speeds.[20]

A. The system of electronic votes

An electronic voting system means that the electorate can transmit their secret ballots via internet to election officials using electronic ballots. The system's disadvantages are: (i) poor computer expertise cannot vote properly; (ii) security threats vulnerable; (iii) polling stations consuming power; and (iv) cost.[21]

B. System of vote online

The newest electronic voting system in which ballots are broadcast on the public Internet via a web browser is the online voting system. Voters can vote directly from online Everywhere in the world. Everywhere in the world. Protection is the only disadvantage of this tool.[18]

C. Some other online voting security-based issues are:

Password security is highly protected and does not focus on most applications Attacks on phishing. By phishing, attackers receive the user's passwords They can access the relevant web pages in the correct password. No efficient method is available Protection of phishing for website users.

To fulfill security requirements for privacy, anonymity, qualifying, equity, verifying and receipt freedom of electronic voting, Purusthomata and Alwyn have developed a secure Internet-based e-voting system using an identity-based encryption. Electronic voteSystem tested the use of a unique, public key infrastructure ID number of the vote. [17]

To meet security requirements of the privacy of anonymity, eligibility, fairness, verification, and unique security of secure e-voting, the Sujata and Banshidhar e-vote protocol on basis of blind signatures proposed. The protocol improves over the YES/No E-Voting protocol by using the bit-specific XOR function to generate votes and blind signatures.

A secure e-voting protocol based on identity was developed and was based on two bilinear cryptographic pairing algorithms to meet secure e-voting data protection, eligibility, transparency, precision and unique requirements. The threshold of the protocol is Signature blind encryption scheme

Bilinear primitives of cryptography Blocks of building.

2.3 The Security Issuesof The Online Voting System

International experience has shown that they often face security problems while the voting system is running online. Not only external (e.g. voters, attackers) but Insiders (e.g., program developers and administrators), are responsible for the root of any security problems, even though the legacy of such items in the source code is unacceptable. These mistakes caused a vote system crash. [23]

Similarly, the solutions proposed to prevent these attacks were outlined. In order to prevent hackers from coming into the voting system over network, we can design our system to transmit data without a network. The restriction of vote is another example.Unique data inputs, preventing the execution of command injection.

Table 1: Comparative Table

Sr. No	Paper Name	Publication Year	Conference/ journal	Methodology/tool/ techniques used	Limitations	Future scope
1	A Secure End-to-End Verifiable Internet-Voting System Using Identity-Based Blind Signature	2020	IEEE	Batch verifiability, early voting, elliptic curve cryptography, end-to-end verifiable, functional digital signature, Internet-voting system.	Functional digital signature foranonymously issuing a blank ballot to a voter and used the BLS short signature scheme for protecting the vote from any modification.	The future of voting: End-to-end verifiable internet voting-specification and feasibility study
2	PhishHaven -An Efficient Real-Time AI Phishing URLs Detection System	2020	IEEE	AI-generated phishing URLs, ensemble machine learning, human-crafted phishing URLs, lexical features, multithreading, URL HTML encoding,	Extracts content of webpages, hence computationally inefficient Non-Proactive approach Requires source codes or the entire page content of the website	PhishHaven can be further enhanced by incorporating unsupervised learning,By applying multi-threading technique at an input unit
3	Avoiding Phishing Attack on Online Votig System Using Visual Cryptography	2020	Springer	Visual Cryptography; CAPTCHAImage	Visual Cryptography Technique used to detect phishing site or original site easily.	we will be designingan efficient voting system for Carrom Association that will prevent phishing attack.
4	Secure Electronic Voting Using a Hybrid Cryptosystem and Steganography	2019	Science direct	SDLCmethodfor design and implementation of voters information system. This work employed the iterative waterfall model.	hybrid cryptosystem and steganography was developed, attempt to proffer a more robust scheme in fulfilling the security requirements for electronic voting.	The direction of future works can be tuned towards satisfying the information security requirement for availability. Ensuring availability in information systems also involves preventing denial-of-service attacks.
5	A Novel P2P based System with Blockchain for Secured Voting Scheme	2019	IEEE	Blockchain, P2P network, Ethereum, AES, RSA, security	The existing systems and labels some of the issues of e-voting	This proposed system can be further enhanced by replacing OTP verification by fingerprint or face recognition inreal time implementation.
6	SeVEP: Secure and Verifiable Electronic Polling System	2019	IEEE	Authentication, efficiency, electronic polling, malware, security, verifiability.	Resource allocation polling system have Authentication, process of electronic polling.	develop a working prototype of SeVEP, and evaluate its scalability and usability in real-world deployment.
7	Towards Developing a Secure and Robust Solution for E-Voting using Blockchain	2019	Springer	coercion resistance problem, Blockchain, Online Voting process	Developing a SecureSolution for online Election process information	To slove coercion resistance problem to slove, cryptographic algorithms
8	E2E Verifiable Electronic Voting System for Shareholders	2019	IEEE	Electronic voting, Shareholder voting, Endto-end verifiability, Zero knowledge proofs, Decisional Diffie Hellman assumption, Security proof.	Verifiable election process	More general case that voters to use a smart phone may depart and leave dynamically within computation period.

9	An Electronic Voting Scheme Based on Revised-SVRM and Confirmation Numbers	2019	IEEE	Electronic voting, Revised-SVRM, ElGamal, RSA, Confirmation numbers, Anonymous credential	Revised-SVRM and Confirmation Numbersvirtualization	To consider privacy, robustness, accuracy, integrity, incoercibility and fairness
10	Prevention of Phishing Attack on Online Voting System	2018	ICIEMS	Online Voting, Phishing Attack, Open Redirection, Cyber Security, Website Forgery.	Open Redirection vulnerabilitiesMethod	Verification of voting website this System for website developing a voting process and Attack recognition
11	Secure Online Voting System Using VC	2018	Spring	Visual cryptography, security share, voting system	Secure a voting process for using Cryptography task scenario	Improvement in existing algorithm
12	A Scheme for Threeway Secure and Verifiable E-Voting	2018	IEEE	Electronic Voting, Anonymity, Verifiability.	Paillier Cryptosystem, Homomorphic Encryption	Distributed implementation of Three way Secure and Verifiable Election process
13	Max-MarginMajorityVotingForLearningfromCrowds	2018	IEEE	Max-marginLearning,Crowdsourcing,OnlineLearning,RegularizedBayesianInference.	Simpleanmax-marginmajorityvoting system	willexplorethemax-marginMethodsforcontinuoustypelabels. Itwouldalsobeinterestingtoinvestigatemoreonactivelearning,suchasthem forSelectingsourcing
14	A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption	2018	IEEE	Online voting, privacy preservation, homomorphic encryption, homomorphism tally, endto-end verification.	least one authority is honest, since otherwise the system is not secure	we plan to address this issue and potentially could consider further generalizations.
15	E-voting using blockchain technology	2018	Spring	Security and Protection, Hardware, Online Information Services	1 to n voters consideration of E-voing process	implement voting result using block chain algorithm from every place of election.
16	Anti-Phishing I-Voting System using Visual Cryptography	2017	Spring	Authentication, visual cryptography, image captcha, phishing,	Authentication, communication visual cryptographylink is there	Security for communication

III. RESEARCH METHODOLOGY

3.1 Introduction

Due to the rapid development of technology and the popularity of the internet, a variety of application technologies, such as e-commerce, e-democracy, and e-government, are trending towards digitization.To reduce costs and red tape in government departments, modern states are seeking to provide people with the ability to participate in and benefit from online services by increasing the number of people who have access to the internet. Electronic voting has recently replaced traditional voting in modern states.

For example, (1) electronic voting reduces or eliminates unwanted human errors; (2) in addition to its efficiency, e-voting does not include geographical proximity to electors, which increases the number of voters who participate; and (3) e-voting saves voters time and money while counting voted ballots.Daniel J. Bernstein suggested Salsa20, a software-oriented stream cypher. The algorithm accepts 128-bit and 256-bit passwords. The main, a 64-bit nonce, a 64-bit clock, and four 32-bit constants are used to create the 512-bit initial state during operation. The modified state is used as a 512-bit keystream output after r iterations of the Salsa20/r round feature.

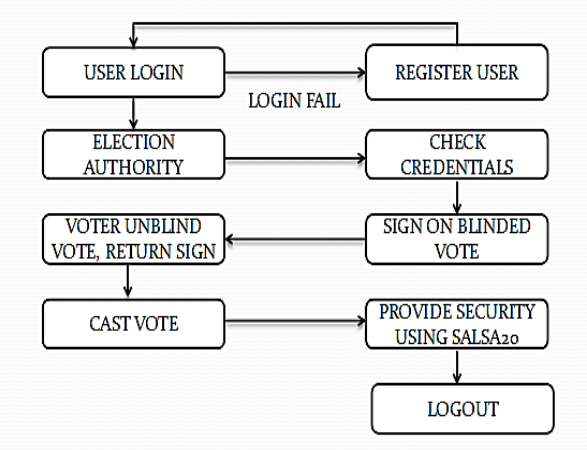

Fig. 1 System Block Diagram [19]

Salsa20/operation r's resembles that of a block cypher in counter mode because each output block is an individual combination of the key, nonce, and counter. Because there is no chaining between blocks, Salsa20/operation r's resembles that of a block cypher in counter mode. As a result, Salsa20/r has the same deployment benefits as Salsa20/r. The ability to produce output blocks in any order and in parallel, in particular. Salsa20/r produces a keystream with a cumulative length of 270 bits.[22]

Salsa20's round transformation is made up of three simple operations: modulo 232 additions, bit rotation, and XOR (what has since become known as an ARX construction). The cipher's software efficiency is enhanced by the effective execution of these operations in software.

Salsa20/8, Salsa20/12, and Salsa20/20 were suggested by eSTREAM as three major variants of Salsa20, based on the number of rounds r. Each offers a different balance of protection and efficiency. The designer suggests Salsa20/20 for "encryption in standardcryptographic applications." Salsa20/12 and Salsa20/8 have 12 and 8 rounds, respectively, and are recommended by the designer for "users who prefer pace over trust." The eSTREAM committee proposed Salsa20/12 as the best compromise between the various models, balancing outstanding performance with a comfortable margin of protection.[11]

1) The eSTREAM testing platform page has more knowledge about the accuracy of eSTREAM cyphers in applications. Refer to D's eBACS stream cypher programme timings page for a more detailed comparison with a variety of other stream cyphers on a variety of architectures. Bernstein is a well-known financial advisor.[24]

2) *Analysis*

Salsa20 has undergone extensive cryptographic research in the years since its release. On either Salsa20/12 or Salsa20/20, there is no attack better than exhaustive key check, despite the fact that some attacks have been discovered on reduced-round variants of the cypher.

Crowley proposed a key-recovery assault on Salsa20/5 at SASC 2006.[5]. The three-round attack uses truncated differentials and has a time complexity of 2165 and a data complexity of 26. Fischer et al. introduced some non-randomness properties after four rounds of Salsa20 at INDOCRYPT 2006, and used this observation to create a key-recovery assault on Salsa20/6 with time complexity 2177 and data complexity 216;Tsunoo et al. [23] used a bias after four rounds of Salsa20 to create a Salsa20/7 attack at SASC 2007. The attack's time and data complexities were 2190 and 211.37, respectively. Aumasson et al. introduced the first key-recovery attack on Salsa20/8 at FSE 2008. [13]. It's a differential attack that uses the probabilistic neutral bits strategy. After identifying a bias in the performance after the fourth round, the authors use it to attack eight rounds in time complexity 2251 and data complexity 231.[16]

STREAM CIPHER WITH SYMMETRIC SECRET KEY

Key length = 32 bytes

Salsa20 is a stream symmetric cypher that is both modern and reliable. Daniel Bernstein, a research professor of computer science at the University of Illinois at Chicago, developed it in 2005.

Make use of

Salsa20 is a cypher that was submitted to the eSTREAM research project, which ran from 2004 to 2008 and was intended to encourage stream cypher development. It is thought to be a well-thought-out and efficient algorithm. There are no known or successful attacks on the Salsa20 cypher family.

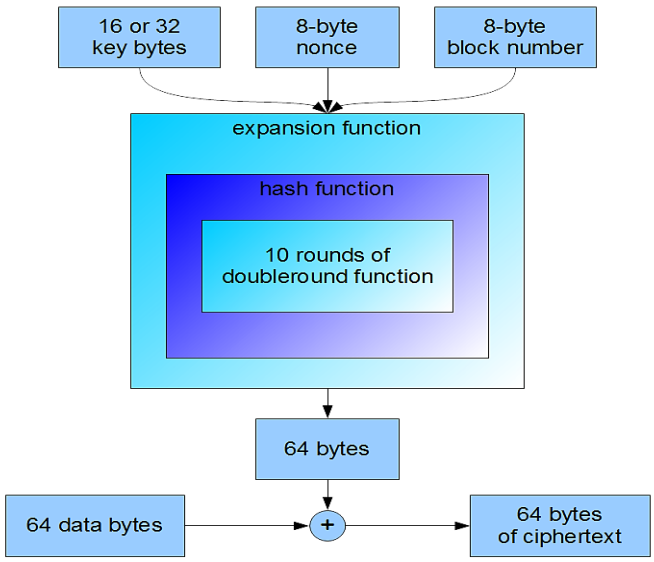

Fig. 2 Block Diagram of Salsa20 Algorithm [12]

a) The Algorithm

Salsa20 is a stream cypher that deals for 64-byte data blocks.

b) Encryption

The algorithm employs the Salsa20 expansion function for each 64-byte data cube. The hidden key (which can be 32 or 16 bytes long) and an 8-byte long nonce concatenated with an additional block number, whose values range from 0 to 264-1 (it is also stored on 8 bytes) are the function's inputs. The block number grows by one with each call to the expansion function.[15]

The hash function that collects the 64-byte long input data from the Salsa20 expansion function, combines it, and finally returns the 64-byte long output is at the heart of the Salsa20 encryption algorithm. The Salsa20 hash function uses the following bytes in the obtained sequence:

- a different hidden key
- another nonce, this time with the block number
- Our constant vectors, whose values are dependent on the size of the hidden key, were obtained from the expansion function.

The hash function works for data that has been separated into words. Each word is made up of four bytes, with values ranging from 0 to 232-1. As a result, the input data is 16characters long, the main is 8 or 4 characters long, and the nonce is 2 characters long.The Salsa20 expansion feature output is XORed with the 64-byte data block. A 64-byte ciphertext block is generated as a consequence.[8]

c) Decryption

During decryption, the same algorithm should be used. The data can be separated into equal-sized parts.

The product of the Salsa20 expansion function should be XORed with the 64-byte ciphertext stack. The outcome is a 64-byte plaintext block.

d) Other Salsa20 ciphers

Other cyphers that are based on the Salsa20 algorithm but vary in specifics are also available.

- Salsa20/8 and Salsa20/12 operate in the same way as the original Salsa20 algorithm, but instead of 10 doublerounds within the hash function, they execute 4 or 6 doublerounds, respectively.
- Bernstein released the ChaCha family in 2008. By using slightly improved hash functions, they have slightly better protection than the original Salsa20 cypher. The input data for the hash function was rearranged to make the algorithm more effective to execute.[23]

3.2 Requirements definition

A systematic and standardised collection of criteria must be defined prior to the design of any voting scheme. The general and system-specific design criteria of the built e-voting system in this work are divided into two categories. Those criteria that extend to any voting scheme are known as common requirements. The system basic criteria, on the other hand, are those that are particular to the system that has been created. The system-specific criteria, on the other hand, are those that are unique to the system that has been created. The system's system-specific specifications allow:

i. Multi-user: Multiple electors will vote at the same time;

ii. Affordability

3.3 Framework design for the system

The framework construction was carried out in order to decide the architectural framework for the applications. The architecture that emerges from this design process is a description of the system that will be used to achieve the given objective. The infrastructure model architecting, in which model(s) is built on the architecture, is an important part of the model design. The models are graphical models that were created with the help of a single modelling language (UML).[14]

3.4 Software development

To validate the architecture, software was developed and implemented. HTML, JSP, Javascripts, PHP, XAMPP api, HTTP SMS, and spring tool gateway were used to build the programme. Windows 10, for example.

3.5 Performance testing and evaluation

After experimental use, users' perceptions of the developed system were gathered to see if the core principles sought in voting systems are present in the developed e-voting system. The following research questions were posed in the questionnaire, all of which concerned whether the developed e-voting scheme met the generic protection criteria desirable in voting systems:

i. Is it possible for cast ballots to stay unaltered? “Integrity” is a requirement.

ii. Is it possible to have a validated vote in the final tally? “Accuracy” is a requirement.

iii. Is it possible to verify the electors are who they say they are? Authenticity is a prerequisite.

iv. Is it possible that the developed e-voting scheme would only allow qualified voters to vote once? Requirement for the term "democracy."

Can the established e-voting system guarantee that no one, even election officials, can attach a ballot to the elector who cast it? “Privacy” is a prerequisite.

3.6 System Design

The framework is divided into three parts: the admin module, the client module, and the server module. Add/manage consumer, add/manage candidate, add/manage groups, and display votes are all included in the admin module. This module allows the administrator to connect, edit, and remove information about users, candidates, and parties. The android programme mounted on the user's smartphone is the client module. The customer must first register with the application, after which he must sign up using the same username andpassword as before registered. The consumer must then choose the candidate on which he wants to vote. When a user clicks the "Vote" button, he is expected to upload the share 1

that was sent to his e-mail address, while the server uploads the share 2 automatically. Authenticated users will be presented with a captcha, which they must correctly enter. The user's vote would be successfully registered if the captcha is correctly entered.

3.7 System Architecture

We propose a new technique to detect the phishing website for phishing identification and prevention. Our system is based on the Anti-phishing Picture Captcha authentication scheme and uses cryptography. It defends passwords and other publicly identifiable information from phishing websites. The suggested method is split into two stages, the first of which is the registration process and the second of which is the login phase..

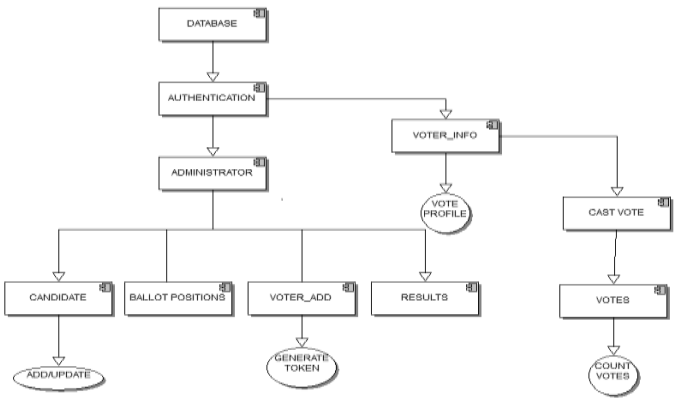

Fig 3 System Architecture [13]

3.7.1 Registration Flowchart

The registry will use the first name and last name as passwords during the registration process. The user's password would be made up of the text of their first and last names. The first and last names are divided into two shares, one of which is held by the recipient and the other by the server. During the login process, the user's share is sent to them for later verification. The first and last names, as well as the password for the telephone number, are stored as sensitive records in the website's database.

3.7.2 LoginFlowchart

The user is first asked for their username during the Login process (user id). The customer is then asked to enter his personal share, which he keeps. This share is sent to the server, where the user's share, as well as the share that is saved in the website's database for each user, are piled together to create the image captcha. The user is presented with a picture captcha. The end user must enter the text shown in the picture captcha, which can be used as a password and through which the user can log in to the website. The user id and password will now be submitted to the authentication scheme for verification.The method of ensuring that the individual is who he wants to be is known as authentication. The user's id is sent to the registry, and the password is retrieved from the database. The user's password and the password retrieved from the database are now compared. Thus, by stacking two shares to create a username and image captcha, one can determine if the website is genuine/secure or a phishing website, as well as if the user is authenticated or not.

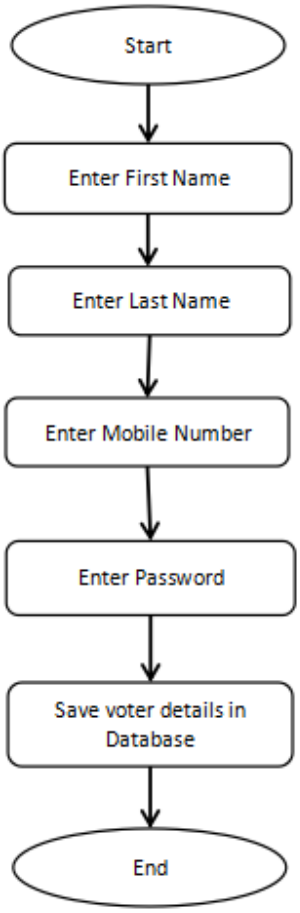

Fig 3.3 Registration Flowchart [03]

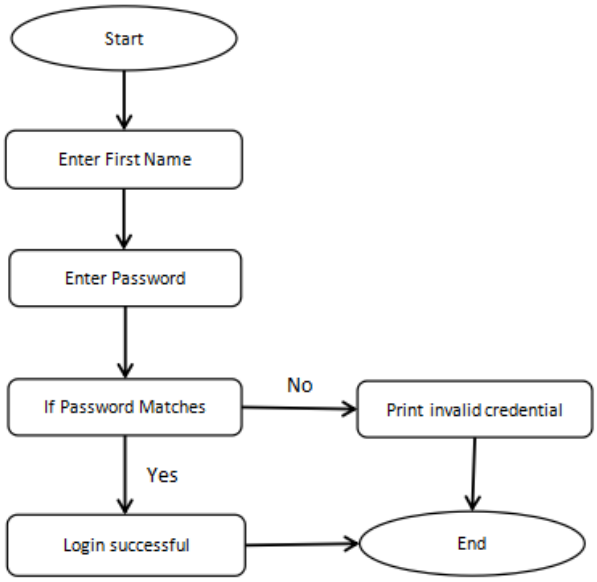

Fig.3.4 Login Flowchart [18]

3.7.3 Sequence Diagram

This is a flowchart that depicts how activities are carried out. They depict the presence between objects in a collaborative environment. The vertical axis of the diagram is used to represent time, and it is used to display the order of the relationship visually by using the vertical axis of the diagram to represent time, and it is used to show what messages are received and when.

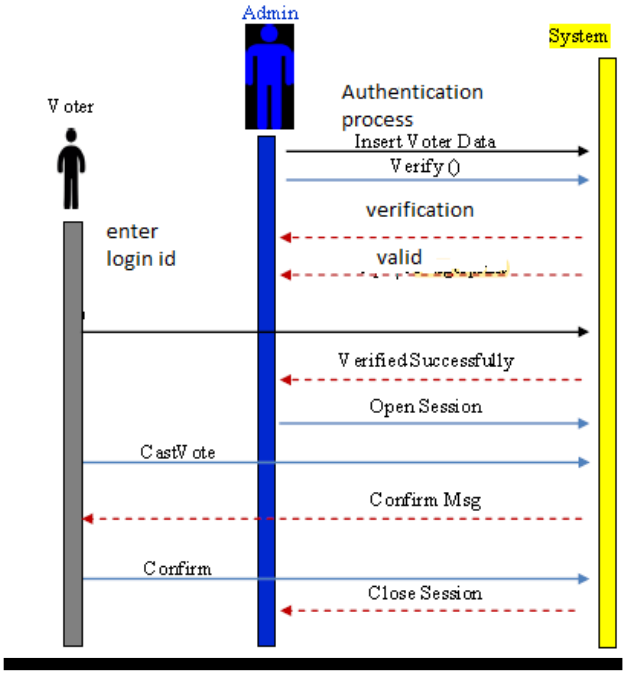

Fig.3.5 Sequence Diagram [26]

3.7.4 Use-Case Diagram

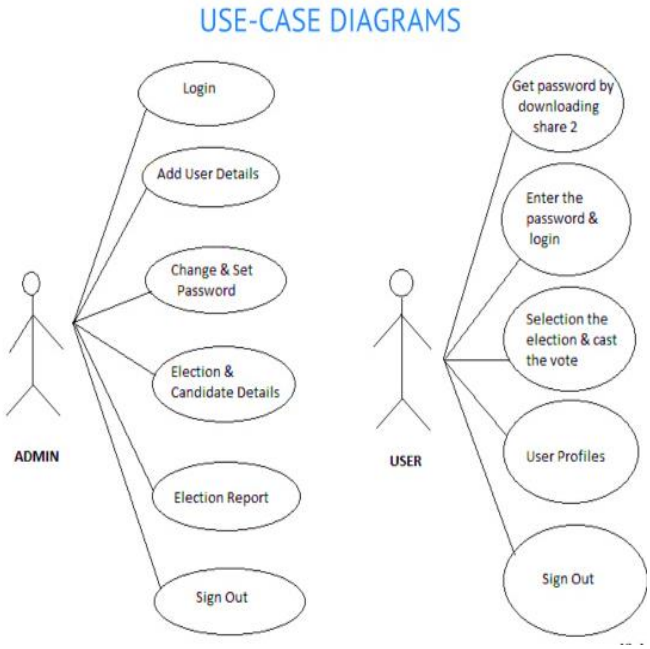

Fig. 3.6 Use-Case Diagram [13]

This is a schematic representation of the major components and processes that make up a system. The main components are referred to as "actors," and the mechanisms are referred to as "usecases." The diagram depicts how the actors deal in each use case, with the Actors, Input, and Output respectively.

3.7 Comparison between Traditional, Existing and proposed system

The machine responds in a fair amount of time. The voter will log in and receive responses to his requests in 2-3 seconds, which is faster than the previous system. Both passwords that are created or adopted are encrypted and stored in a database, as opposed to current systems that store passwords in plaintext and are therefore vulnerable to attacks. Since voting is only performed if the user uploads the correct share and thereby enters the correct strings, the voting mechanism is secure and offers improved security. In election mode, the machine is 99 percent efficient and delivers excellent results. To avoid data loss in the event of a system collapse, votes are polled before they are recovered in the archive, and the system recovers from past failures and resumes the voting procedure with high reliability.

3.7.7 Advantages of Proposed System

Logging in as a user is private and stable. Voters will cast their ballots from anywhere. Voters can access their accounts at any time, but only during voting may they upload a security share that was sent to their registered email address during registration. After entering the text created on the image, if the submitted image is correct, a vote can be cast. The system is safe in this system, and all user information is kept private and secure. Keeping track of voters would be easy. This method would make it simple for electors to cast their ballots, and it is simple to use. It would be simpler for people living in rural areas to vote.

3.9 Database Design

The online voting system makes use of a database called Online Voting, which is made up of two tables, as seen below.
Online Voting from a Database
This research project makes use of many tables, including

- Admin,
- Voter, and
- Candidate.

1. User/voter registry data table - This table stores information about active users/voters, including their favourite user names and passwords. It also includes voter/user contact information, such as phone numbers and email addresses.

Table 2Structure for table registration details

Field	Type	Null	Default
IdNo	int(10)	No	
Fname	varchar(15)	No	
Lname	varchar(15)	No	
Mobile No	int(10)	No	
Password	Varchar(20)	No	
User	varchar(40)	No	voter

username and password for logging in

2. Vote table - This table keeps track of the delegate and the elector who casts a vote in their favour. The id field is its primary key, and it is also needed for vote counting. The index is checked to see how many people voted for a single contestant.

Table 3Structure for table vote

Field	Type	Null	Default
candidate	varchar(25)	No	
Voter	varchar(15)	No	
Id	int(8)	No	

IV. SYSTEM SPECIFICATION AND DESIGN

4.1 Introduction

To approximate the computer cycles consumed by operations using a highly verifiable safe online voting system in which each elector is authenticated using a unique identifier provided by the relevant authority and his biometric details (for example, private and public operations based on RSA, operations on elliptic curve and pairing). The appropriate cryptographic operations' notations and the number of computer cycles they absorb. Our system's success in comparison to other systems. The suggested method and system are based on ECDL and GDH problems and use elliptic curve cryptography. The security of the systems is focused on the discrete logarithm problem (DLP) and integer factorization problems, and they are based on the standard RSA public key cryptosystem (IFP). The ECC-based operations (scalar multiplication and addition) are more efficient than the RSA-based operations, as seen in Table 3.[23]

4.1.1Reqirements for an election system

Researchers also defined a series of specifications for a reliable electronic voting protocol in this framework.

4.1.2 Security Requirements

Since the internet seems to be an unstable place, protection plays an essential role in every voting method, particularly e-voting. In order for the electronic voting framework to function without bugs, it must be applied according to safe design. Despite the system's difficulty of architecture and execution, it seems that certain principles are universally agreed as the minimum security specifications for electronic voting.

Voter authentication: Only registered voters should be able to vote, and only one vote per voter should be counted.

Voter privacy: while only registered electors should be allowed to vote, it should be difficult to link a voter's identity to the substance of his or her vote.

Election Results Accuracy: Since all caste votes cannot be changed, copied, validated votes cannot be excluded from the final result, and null votes can not be included in the final result, the system is accurate. To deter vote tampering, a digital signature is used. Uniqueness can be added to the voting mechanism for accuracy by using a token that is distinctive.

Intermediate result privacy: A scheme is anonymous if no casted ballot can be attributed to its voter (anonymity), and no voter can prove that he or she voted in a specific way (receipt - freeness).

Verifiability of ballots: votes must be checked separately by electors who were inserted in the final tally and counted correctly.

When an adversary orders an elector that may be related to him to vote a certain way, the voter has the ability to trick the adversary. And if the adversary coerced the voter to show his keys or abstain from voting, the adversary would not be able to tell if the voter followed the adversary's instructions or not.

Democracy means that each registered voter has the right to vote and that no one should vote for another.

Robustness: By avoiding any malicious action by voters, officials, or outsiders, the mechanism must be protected and non-infiltrated by adversaries. To engage in the voting protocol, you'll need a token.

There are additional specifications that deal with the system's implementation's public security assets. For example, the framework should be trusted, user-friendly, transparent, and built on open programming architectures and open source applications, among other things. However, some of the above specifications are incompatible. In the case of voting secrecy, the ballot, for example, cannot be attributed to the voter. This is in contrast with the verifiability property, which stipulates that each elector must be able to prove that his or her vote has been counted.

4.1.3System Wide requirements

In this section, the system-wide requirements for implementing voting protocols are discussed. -Voter convenience: Voters should be able to vote without consulting the voting authorities and complete the voting procedures with he bare minimum of skills and equipment.-Voter mobility: Voters should be able to vote from either location without restriction.The scheme is successful if the number of electors and the authorities' involvement in the protocols are equal to the computing and communications resources.

4.2Approach

4.2.1 What approach is taken by the author

Once all the nodes of the network are running, a new user can connect to the server. The user registers a non-anonymous user (using Aadhar Card, phone, password, etc), and performs the login.

The user, locally, generates a RSA key pair (private key & public key). The user blinds his Public-Key with the server Public-Key.

The user's Public-Key blinded, is sent to the server.

The server Blind Signs the Public-Key blinded from the user, and returns it to the user.

The user unblinds the Public-Key signed by the server, and now has the Public-Key Blind Signed by the server.

The user sends the Public-Key blind signed to the p2p network.

The peers verify that the Public-Key Blind Signed is correctly signed by the server, if it is, they add the Public-Key to the Ethereum Blockchain, inside a new block.

4.2.2 Our Approach:

As per recent research RSA method to secure data with blind signature has some flaws and can be cracked using high end computational devices.

So we will be using more secure Salsa20 security algorithm which is found more to be more secure than existing algorithm like RSA and AES.

Also Salsa20 is more FAST and light weight than RSA and AES.

Salsa20 is FAST in terms of encrypting and decrypting.

Means it can encrypt more messages per cycle compare to RSA and AES.

Also it is light weight means it requires less computational resources compared to other.

In spite of such benefits Salsa20 provides better security.

V. SYSTEM REQUIREMENT AND IMPLEMENTATION

5.1 Introduction

The aim of this segment is to focus on the system's deployment climate. This includes the hardware and software environments for the device design and development implementation process. The software was designed using a top-down architecture approach. The framework is made up of modules and sub-modules that are connected together to allow for simple data and control flow.

5.2 System Implementation Technologies

The web-based voting system was created as an online information system to provide users with easy access to the voter registration database. The following are some of the methods that were used during the implementation:

5.2.1 Software

i. MYSQL DBMS - allows data in the voter database to be combined, extracted, modified, and arranged. It is platform agnostic, which means it can be deployed and used on a range of platforms, including Windows, Linux servers, and mainframes. It performs well, is safe, and offers market benefit at a low cost.
ii. Java - This is the new heart of the web world; it is a programming language that is used to create web pages. It's the substance that binds all together. While Java and the Spring tool is used to create the OVS, it is highly compatible with Java and the Spring tool and can be used as a substitute for Java when dealing with details. It is also scalable between various browsers and frameworks with little or no code changes. Macromedia Dream weaver is a preferred method for integrating Java pages, and it was this tool that was used to create the OVS framework.
iii. Java coding-This is for advanced user who find Java codes easy to work with.
iv. Testing - is done via WAMPSERVER.
v. Web browsers - Mozilla Firefox, Google chrome, Opera and Internet Explorer
vi. Reporting Tool - i.e. through Data Report.

5.3 Software Requirementt

Software is a list of programs or instructions written in some programming language that allows the user to do whatever they want with their computer.

Only the following minimum technical specifications are needed to run and build this package:

a. Windows XP, Vista or Window 10 etc.
b. MYSQL DBMS
c. Java coding
d. XAMPSERVER.
e. Web browsers: Mozilla Firefox, Google chrome, Opera and Internet Explorer

5.3.1 System Software

There are pieces of software written by machine programmers who translate instructions in application software (programmes) and then send the basic instructions to the central processor, allowing the different hardware units that make up the computer system to work as intended. DOS is a good example. System software maintains and monitors computer hardware in order for programme software to run tests. Microsoft OS is an example of an operating system.

Application software, on the other hand, is a programme that allows the end-user to perform basic, productive activities like word processing or image editing. System programme runs experiments such as copying data from memory to disc and displaying text on a display screen. Loading applications, operating system interface drivers, programming tool compilers, assemblers, linkers, and utility tools are all examples of system software. Firmware refers to processor information that is stored on nonvolatile memory, such as integrated circuits. The operating system and all utility programmes that handle computing resources at a low level are referred to as this.

5.3.2 Application Software

Application software is end-user software that is programmed to execute a range of functions, such as MS Term. These are typically applications or operating frameworks that are available from a provider and are pre-programmed to execute particular tasks. Application software is a form of computer software that uses a computer's resources explicitly and thoroughly to complete a task that the user desires.

5.4 Hardware Requirement

A decent computer with a hard disc drive of 20GB or more is needed to run the machine. This is required in order to save the software and make it usable at any time. For a successful view of all outputs, it needs a visual display unit (VDU) with a high resolution and graphic capability.

A working CD drive or floppy drive is required in case the programs on the hard disc are ultimately killed by a virus. When PHCH loses control, an uninterrupted power supply (UPS) is needed to maintain power for a short period of time.

5.5 Language Justification

The online architecture of the programme was implemented using Java and the spring tool. Java is an object-oriented programming language built on classes. As a result, it includes a number of libraries that aided in the creation of the user interface, as well as the ability to bind to a MySQL database with ease. It also added to the system's security by using the MD5 feature for data encryption algorithms. The pages were also improved with the use of JavaScript Frameworks/JavaScript CSS (Cascadian stylesheet) to make them more vibrant and appealing. The database engine for the electronic voting system research project was Java.

It's yours for free on the internet. After its inception, Java database software has been heavily preferred against a wide range of database software. 5.2 System Components and Modules The framework was built as a web-based online voting and alteration solution using Spring tool server, Java web server, and Internet Explorer as the primary browser; other web browsers such as Mozilla Firefox, Opera, and Google Chrome can also be used. The system's security and usability are guaranteed.

5.5.1 Shortcomings with the System

The following variables obstruct the system's implementation:a) Financial resources to fully enforce the framework are minimal.b) There is opposition from commissioners who think the tool can do all of their job for them, and residents who do not believe it is a safe way to vote online.c)Power supply in different parts of the world is unreliable, which may discourage voters from using the online voting system to cast their ballots.

d)As in any computer-based information system, garbage in equals garbage out, which means that if incorrect information is inserted into the online voting system, the result will be the same.

e) The election process has lost a considerable amount of personal touch.

5.5.2 Form input and Reports Design

The framework was created as a web-browser-based collaborative process between the user at the interface and the database. This tool helps a user to communicate with a MYSQL database using a web browser to access, edit, view, and retrieve data depending on the privileges given. Java servlets were used to carry out these tasks. HTML forms have the best interface for entering data, modifying the index, and displaying it. For quick public understanding of the tool's use, these forms and report interfaces were kept as short and basic as possible. Some of the forms and report interfaces produced include the following:

5.5.3 The login form

This is where a potential user/voter begins; they must first create a username and password. When this is provided, the machine verifies the user's knowledge to what is stored in the database. The voter/user is then logging in; otherwise, he/she is not logged in.

5.5.4 The voter registration form

For the sake of the machine owner, this type is purely retained. He or she is the only one who has access to and can use this form. Users under the age of 18 are unable to access this page through the connection provided.

5.6 Testing and validation

Testing was performed on the machine at the design period to ensure its reliability and resistance to intentional errors.

This can be accomplished in two stages: -

Unit testing: Unit research examines the output of specific components using test results.

System testing: The components are joined together, and test data is used to determine if the components fit together.

VI. CONCLUSION, RESULT AND RECOMMENDATION

6.1 Conclusion

Using the internet to vote Orthodox voting systems have drawbacks that cryptography overcomes. This method is more stable and takes less time to incorporate. Additionally, there is no possibility of voting intimidation, and the amount of money spending on defence will be greatly lowered. The main goal of this approach is to offer full anonymity to the voter while also ensuring that the voting system is well integrated. The key principle behind this framework is to use a robust authentication mechanism to authenticate electors.

Cryptography encrypts data such that it can be decrypted without the use of mathematical computations. People who have access to the internet at home can vote without having to go to polling places. Since the elector can vote from his place of employment, elections can be held quickly and efficiently in a proper manner using this Internet-based voting system based on cryptography. Internet voting has a number of advantages, including reduced costs and greater voter turnout. This voting method closely respects security and human considerations, ensuring that electors have accurate and intuitive evidence of the legitimacy of the voting procedure. Cryptography is used in the scheme we propose to provide shared security for electors and election servers.

6.2 Result

This system will very useful and safe for online remote voting and specially in pandemic like COVID-19. This system is web based application so that it can be accessed by any authorized person anywhere in the world through internet.

REFERENCES

[1] Ollmann G. The Phishing Guide Understanding & Preventing Phishing Attacks, NGS Software Insight Security Research.

[2] M. Naor and A. Shamir (1994), Visual cryptography, in Proc. Eurocrypt,pp. 1–12.

[3] A. Shamir (1979), .How to Share a Secret,. Communication ACM, vol. 22, pp. 612-613.

[4] G. R. Blakley (1970), .Safeguarding Cryptographic Keys,. Proceedings of AFIPS Conference, vol. 48, pp. 313- 317.

[5] A. Menezes, P. Van Oorschot and S. Vanstone (1997), .Handbook of Applied Cryptography,. CRC Press, Boca Raton, FL, 1997.

[6] Sumit Jagtap, Smitesh Vichare, AlpaVaidya, Mangesh Jogd and, Prof. Shivani Sthapak, "VC Technology in Internet Voting System", published in 4, April 2016.

[7] Rajendra A B and Sheshadri H S ," Visual Cryptography in Internet Voting System".

[8] Pallavi V Chavan, Dr. Mohammad Atique, and Dr. Anjali R Mahajan,"An Intelligent System for Secured Authentication using Hierarchical Visual Cryptography-Review", published in 2011.

[9] Anusha MN and Srinivas B K," Remote Voting System for Corporate Companies using Visual Cryptography", published in 2012.

[10] Sanjay Kumar, Manpreet Singh, "Design A Secure Electonic Voting System Using Fingerprint Technique", published in July 2013.

[11] Olaniyi Olayemi Mikail, Folorunso Taliha Abiodun, Abdullahi Ibrahim Mohammed, Abdulsalam Kayode Abdusalam, "Design and Development of Secure Electronic Voting System Using Radio Frequency Identification and Enhanced Least Significant Bit Audio Steganographic Technique", published in Dec 2014.

[12] Bellis, M. (2007). The History of Voting Machines. Retrieved November 9, 2006 from: http://inventors.about.com/library/weekly/aa111300b.htm

[13] Cranor, L.F., & Cytron, R.K. (1996). Design and Implementation of a Security-Conscious Electronic Polling System. Washington University Computer Science Technical Report (WUCS). Retrieved October 9, 2006 from: http://www.acm.org/crossroads/ords2-4/voting.html

[14] S. Kadam, K. Chavan, I. Kulkarni, and A. Patil, "Survey on Digital E-Voting System by using Blockchain Technology," International Journal of Advance Scientific Research and Engineering Trends, 2019.

[15] F. Yusifov, R. Alguliyev, and R. Aliguliyev, "Multi-criteria Evaluation+ Positional Ranking Approach for Candidate Selection in E-voting," Decision Making: Applications in Management and Engineering, vol. 2, no. 2, pp. 65–80, 2019.

[16] Q. Aini, N. Lutfiani, F. Hanafi, and U. Rahardja, "Application of Blockchain Technology for iLearning Student Assessment," IJCCS (Indonesian Journal of Computing and Cybernetics Systems), vol. 14, no. 2, 2020, doi: 10.22146/ijccs.53109.

[17] . Fauzi, "Perilaku Pemilih Menjelang Pemilu 2019," Journal of Islamic Civilization, vol. 1, no. 1 SE-Articles, pp. 40–48, Apr. 2019, doi: 10.33086/jic.v1i1.918.

[18] H. Wang et al., "Phase-adjusted estimation of the number of coronavirus disease 2019 cases in Wuhan, China," Cell discovery, vol. 6, no. 1, pp. 1–8, 2020.

[19] "WHO Coronavirus Disease (COVID-19) Dashboard." https://covid19.who.int/ (accessed May 23, 2020).

[20] R. Tosepu, J. Gunawan, D. S. Effendy, H. Lestari, H. Bahar, and P. Asfian, "Correlation between weather and Covid-19 pandemic in Jakarta, Indonesia," Science of The Total Environment, p. 138436, 2020.

[21] R. Setiawan, "Scientific Literacy Worksheets for Distance Learning in the Topic of Coronavirus 2019 (COVID-19)," 2020.

[22] Pusat Penelitian Politik - Lembaga Ilmu Pengetahuan Indonesia (P2P-LIPI), "Dampak Pandemi COVID-19 Terhadap Pilkada 2020 - Politik Lipi." http://www.politik.lipi.go.id/kolom/kolom-2/politik-nasional/1398-dampak-pandemi-covid-19-terhadap-pilkada-2020 (accessed May 20, 2020).

[23] S. Engle, J. Stromme, and A. Zhou, "Staying at Home: Mobility Effects of COVID-19," SSRN Electronic Journal, 2020, doi: 10.2139/ssrn.3565703.

[24] U. Rahardja, S. Sudaryono, N. P. L. Santoso, A. Faturahman, and Q. Aini, "Covid-19: Digital Signature Impact on Higher Education Motivation Performance," International Journal of Artificial Intelligence Research, vol. 4, no. 1, May 2020, doi: 10.29099/ijair.v4i1.171.

[25] U. Rahardja, A. N. Hidayanto, T. Hariguna, and Q. Aini, "Design Framework on Tertiary Education System in Indonesia Using Blockchain Technology," 2019 7th International Conference on Cyber and IT Service Management, CITSM 2019, pp. 5–8, 2019, doi: 10.1109/CITSM47753.2019.8965380.

[26] T. Hidayat and R. Mahardiko, "A Systematic Literature Review Method On AES Algorithm for Data Sharing Encryption On Cloud Computing," International Journal of Artificial Intelligence Research, vol. 4, no. 1, 2020.

[27] Kothari, Aansi A., and Warish D. Patel. "A Contemporary Overview on Feature Selection and Classification Techniques in Opinion Mining." International Journal of Computer Applications 110.10 (2015): 10-14.

[28] Patel, Mr Warish D., and Mr Dineshkumar B. Vaghela. "A Novel Approach For Joining Distributed Streaming Data Using Multiple Indexing Methods & Binary Search."

[29] Kothari, Aansi A., and Warish D. Patel. "A novel approach towards context based recommendations using support vector machine methodology." Procedia Computer Science 57 (2015): 1171-1178.

[30] Kothari, Aansi A., and Warish D. Patel. "A novel approach towards context sensitive recommendations based on machine learning methodology." 2015 Fifth International Conference on Communication Systems and Network Technologies. IEEE, 2015.

[31] Patel, Tanvi P., and Warish D. Patel. "A Recent Review on Itemset Tree Mining: MEIT Technique." (2015).

[32] Patel, Warish D. "Tanvi P. Patel." Global Journal of Computer Science and Technology 13 (2013).

[33] Patel, Warish D., et al. "NXTGeUH: LoRaWAN based NEXT Generation Ubiquitous Healthcare System for Vital Signs Monitoring & Falls Detection." 2018 IEEE Punecon. IEEE, 2018.

[34] Patel, Warish, Sharnil Pandya, and Viral Mistry. "i-MsRTRM: Developing an IoT based Intelligent Medicare system for Real-Time Remote Health monitoring." 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN). IEEE, 2016.

[35] Patel, Warish D., Brijesh Vala, and Himal Parekh. "An Advanced Cognitive Approach for Heart Disease Prediction Based on Machine Learning and Internet of Medical Things (IoMT)." Proceedings of the Second International Conference on Information Management and Machine Intelligence. Springer, Singapore, 2021.

[36] Bhaskar, Sourabh, Bhupendra Ramani, and Warish D. Patel. "An Advanced Approach for Link-Based Spam Detection Using Machine Learning." Proceedings of the Second International Conference on

Information Management and Machine Intelligence. Springer, Singapore, 2021.

[37] Konan, Derroh Amany Maxime, and Warish Patel. "i-NXGeVita: IoMT based Ubiquitous Health Monitoring System using Deep Neural Networks." 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). IEEE, 2018.

[38] Mudnur, Shrikant P., et al. "Extraction of Maximum Secret Information Hidden in Approximate Band of Haar Wavelet Transform of an Image." 2018 Conference on Information and Communication Technology (CICT). IEEE, 2018.

[39] Mudnur, Shrikant P., et al. "Hiding the Secret Image Using Two Cover Images for Enhancing the Robustness of the Stego Image Using Haar DWT and LSB Techniques." 2018 Conference on Information and Communication Technology (CICT). IEEE, 2018.

[40] Patel, Tanvi P. and Warish D. Patel. "An Enhanced MEIT Approach for Itemset Mining Using Levelwise Pruning." *World Academy of Science, Engineering and Technology, International Journal of Computer and Information Engineering* 2 (2015): n. pag.

[41] Patel, Mr Warish D., and Mr Dineshkumar B. Vaghela. "A Novel Approach For Joining Distributed Streaming Data Using Multiple Indexing Methods & Binary Search."

[42] Patel, Mr Warish D., et al. "An Adaptive Join Algorithm for Result Rate Maximization over Distributed Streaming Inputs Using Hybrid Searching and Multiway Join Methods."

[43] Patel, W., Chirag Patel, and Carlos Valderrama. "IoMT based efficient vital signs monitoring system for elderly healthcare using neural network." International Journal of Research 8.I (2019): 239-245.

[44] "Smart Health: Natural Language Processing based Question and Answering Retrieval System in Healthcare", International Journal of Emerging Technologies and Innovative Research (www.jetir.org | UGC and issn Approved), ISSN:2349-5162, Vol.6, Issue 5, page no. pp127-137, May - 2019, Available at : http://www.jetir.org/papers/JETIRCQ06022.pdf

[45] Patel, Warish D., and Dineshkumar B. Vaghela. "An efficient improved join algorithm using map reduce in Hadoop." 2014 International Conference on Signal Propagation and Computer Technology (ICSPCT 2014). 2014.

[46] Patel, Warish, and Dinesh Vaghela. "A Review on Adaptive Join Algorithms for Efficient Query Processing On Heterogeneous Data Sets." International Journal 2.1 (2014).

[47] Warish D. Patel*, Chirag Patel and Monal Patel, "VitaFALL: Advanced Multi-threshold Based Reliable Fall Detection System", Recent Advances in Computer Science and Communications (2020) 13: 1. https://doi.org/10.2174/2666255813999200904132939