International Journal of Research in Engineering, Science and Management
Volume-2, Issue-1, January-2019
www.ijresm.com | ISSN (Online): 2581-5792

E-Polling System using Cloud Computing and Biometrics

R. Prasanthi[1], H. Meharban[2]
[1]*Lecturer, Department of Computer Engineering, ADJD Polytechnic College, Nagapattinam, India*
[2]*Lecturer, Department of ECE, ADJD Polytechnic College, Nagapattinam, India*

***Abstract*: Cloud computing is a computing paradigm in which tasks are assigned to a combination of connections, software and services that can be accessed over internet. This paper proposes the usage of cloud computing in E-polling. The main aim of this project is to avoid fake votes in polling by having a cloud database about the voters. Thumb impression of candidates is used for authentication. A candidate can vote at any place irrespective of his polling booth, and can vote through mobile phones. The min-min average algorithm used in this paper increase the communication workflow in cloud. The cloud computing relies on the internet. When the internet connection fails it does not work with mobile phone. The paper introduced the smart client technology to overcome this difficulty in mobile phones.**

***Keywords*: Cloud Computing, Smart Client, E-polling, Biometrics.**

1. Introduction

Polling is a choice that is made by counting the number of people in favour of each alternative. Current polling system is not very secure. The main aim of this paper is to provide high security internet polling. This system is implemented using cloud computing and biometrics. Cloud computing is a paradigm in which virtualized resource are provided as a service over the internet to the cloud user. Users need not have knowledge of, expertise in or over technologies infrastructure in the "cloud" that supports them. Biometric identification refers to identifying an individual, based on his/her distinguishing physiological and or behavioral characteristics. This system uses thumb print as distinguishable factor. Instead of buying software, installing and upgrading it periodically and storing all data on hard drive, cloud computing enables software applications online, as a service with a computing device and an Internet connection on demand. The cloud computing thus can be used in polling system

2. Existing system

The security level in existing voting system is not up to the mark. In the case of EVM (Electronic Voting Machine) data reliability is not assured as it is based on microcontroller on which the program and the memory can be protected from external read, but that is very low level security and chip centric. In case of chip failure data loss occurs and it cannot be recovered. In many voting system the candidate are restricted to vote at their respective places. Internet voting system SERVE (Security Electronic Registration and Voting Experiment) is found to be vulnerable to denial of service attack and website spooling .This can compromise the results. Moreover there are a number of technical issues, including authentication and validation of the end-point, protecting the voting system against the inevitable attempts by hostile parties to disrupt the election, and ensuring that the network is capable of handling traffic storms if potentially millions of citizens cast their E-ballots in a short period of time.

3. Proposed system

In the proposed system the database creation is done with the details of the candidate along with thumb impression which serve as the key for authentication (Biometric Database).

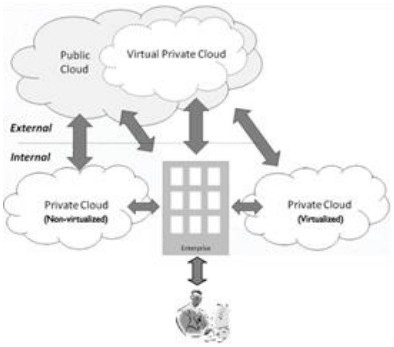

Fig. 1. Cloud Structure

While casting vote, the thumb impression of candidate is being matched with the existing database. If the match is found, candidates are allowed to caste their vote, otherwise they are denied. This system provides safe and secure polling. Cloud provides a service for voting to all authenticated user.

4. Min-min average algorithm for cloud workflow

The polling processing application may need to process millions of transactions per day and store the biometric information of the people. The main purpose of using this algorithm is to improve the communication overhead between the local cloud servers to the main server. Due to a huge number

of concurrent workflow instances, the algorithms should focus on minimising the mean execution time of all process in order to maximise the overall throughput rather than minimising the execution time of individual process. Mean execution time is the time spent from the beginning of the first task to the end of the last task for a workflow instance. Hence they can be modelled as instance-intensive cloud workflows with considerable communication overheads. The main characteristic of such workflows is a huge number of relatively simple concurrent instances of which may involve considerable communication overheads among relevant tasks. Thus it is necessary to consider multiple instances of multiple workflows with communication overheads when designing scheduling algorithms for such workflows. Workflows on service-based cloud computing environment construct the simulation environment focusing for the MMA algorithm, testing nodes located in different places connected via the Internet has been used and thus the communication overheads vary.

A. Scheduling infrastructure

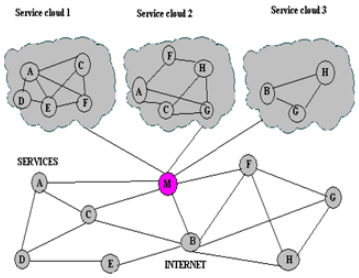

Fig. 2. Scheduling infrastructure

As Fig 2 shows, the workflow execution environment is divided into several service clouds according to different services available. For each new computing node, it joins the service clouds according to individual polling booth it provides, and all the polling booth grouped in the cloud. If the service cloud already exists, the node simply joins it; otherwise, it creates a new service cloud and joins it as a creator. There are two kinds of nodes, namely, ordinary and monitor. Ordinary node maintains the entire nearest nodes. The monitor node keeps track of all the connected node. It should be noted that all service clouds are registered and maintained by the monitor nodes.

MMA (Min-Min-Average) Scheduling Algorithm

- Procedure Schedule (Instance Array Instances [])
- // Step 1: select ready tasks from the multiple instances of multiple workflows.
- for each instance I in Instances [] do
- for each task t in polling do
- if polling is ready then
- add t to Ready Tasks [];
- end if
- end for
- // divide ready tasks to task groups against required resources;
- for each task polling in ready tasks do
- If polling requires resource r then
- add the task group that requires resource r;
- end if
- end for
- //Step 2: for each task group, select a list of capable nodes with requested resources.
- for each task group poll booth do
- if the host has the resource to execute the tasks in poll then
- select a list of capable nodes with required resources from hash table;
- else if nodes can be found in the cached hash table
- // for all selected neighbours, send request messages and wait for responses.
- if response is found store in hash.
- end for

B. Biometric authentication

Biometric data should be collected from the voters as part of the election pre-registration process. Database regarding the candidates are managed with thumb impression as primary key. While casting vote the thumb impression of the candidate is matched with the existing database. If the match is found the casted vote is considered otherwise discarded. No candidate is recognized twice. In prior to polling, biometric authentication can also be used to check whether the candidate is eligible for casting vote or not. Many notebook computers include fingerprint readers. In the near future, the mobile handset industry will begin to embed some type of biometric identification system into their devices.

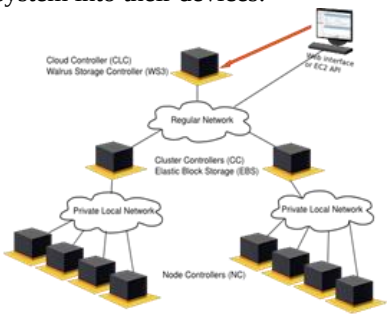

Fig. 3. Voting using cloud

C. Cloud storage

In the cloud computing technology we can store the details of the people along with their thumb impression. The database creation is done with the details of the candidate along with thumb impression which serve as the key for authentication (Biometric Database).While casting vote the thumb impression of candidate is being matched with the existing database. If the match is found candidate is allowed to caste their vote, otherwise they are denied. This system provides safe and secure

polling. Cloud provides a service for voting to all authenticated user. The cloud computing mainly works based only on the internet facility. All your data is stored online, so you don't have to worry about the capacity.

D. Problem with cloud computing

The main problem with the cloud computing is it requires an internet connection. If the candidate want to vote at the time where the internet connection is not available it is impossible. So a smart client technology is introduced to overcome this problem.

5. Smart client approach

The term Smart Client was coined to highlight the differences between the typical "Rich Client" applications of yesteryear and the next generation of client applications. The advantages of smart client technology:

A. Utilizes local resources

A smart client application always has the ability on the client that enables local resources (hardware, software) to be utilized. A smart client may take advantage of the local CPU, local memory or disk, or any local devices connected to the client.

B. Offline capable

As they are running on the local machine, one of the key benefits that smart client applications offer is that they can be made to work even when the user is not connected. For applications running in occasional or intermittent connectivity situations, such as those used by travelling workers or even those running on laptops, tablets, PDA's, and so on, where connectivity cannot be guaranteed at all times, being able to work while disconnected is essential. Even when the client is connected, the smart client application can improve performance and usability by caching data and managing the connection in an intelligent way.

C. Intelligent install and update

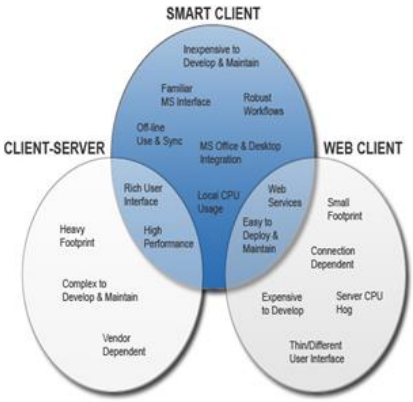

Fig. 4. Smart client technology

Smart client applications manage their deployment and update in a much more intelligent way than traditional rich client applications. There are many frame work that provides the smart client technology. It enables application artifacts to be deployed using a variety of techniques, including simple file copy or download over HTTP. Applications can be updated while running and can be deployed on demand by clicking on a URL.

D. Client device flexibility

This technology provides a common platform upon which smart client applications can be built. Often, there will be multiple versions of the smart client application, each targeting a specific device type and taking advantage of the devices unique features and providing functionality appropriate to its usage.

E. Storing candidate biometric information

The biometric information of the candidate stored in the local database is the thumb impression. The main purpose of using the local database in the server is to store the data of the candidate and update them in the cloud instantly with the main server. There are many local servers available across various polling booths. All of them have been combined to form the cloud structure so that they can share the resources. The main advantage of using the cloud computing storage is listed below

1) Simple Scalability

Cloud storage requires a high degree of automation with self-management, self-configuration and self-healing, all orchestrated through high-level policies specified by the storage administrator. Next generation storage provides administrators flexibility and control. As the cloud grows, additional nodes are able to service the data requests in parallel. If administrators require more performance, they can add a processing node. If they need more capacity, they can add disks. Each can be added independently or scaled simultaneously.

6. Ensuring data storage in cloud computing

Cloud computing security sometimes referred to simply as "cloud security" is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. There is a number of security issues associated with cloud computing but these issues fall into two broad categories: Security issues for the polling system and security of the candidate biometric authentication.

A. Data Protection

To be considered protected, data from one candidate must be properly protected, it must be stored securely when “at rest” and it must be able to move securely from one location to another.

Cloud providers have systems in place to prevent data leaks or access by third parties. Proper separation of duties should ensure that auditing and/or monitoring cannot be defeated, even by privileged users at the cloud provider. Providers ensure that

physical machines are adequately secure and that access to these machines as well as all relevant customer data is not only restricted but that access is documented. All the attacks has to be prevented in the cloud computing. Finally, providers ensure that all critical data (thumb impression) are masked digital identities and credentials must be protected, as should any data that the provider collects or produces about customer activity in the cloud.

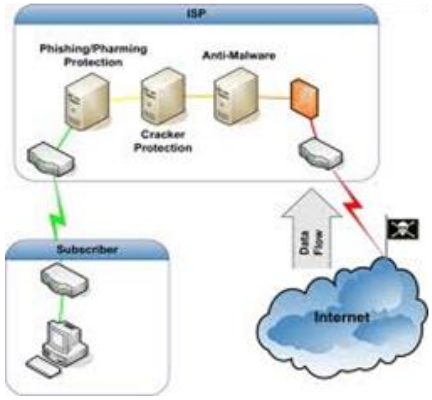

Fig. 1. Security Aspect in cloud

7. Voting through mobile phones

In the cloud computing technology, many derives can be grouped in the cloud including PC, Mac or Smartphone. The local database is used to store the information of the thumb impression when the internet connection is failed. When the internet connection is available, it can send the data to the main server. If the internet connection is available directly it can send the candidate information directly to the server. Thus voting can take place in the polling booth at any place and also through other devices.

A. Cloud-computing to address voting storms

Instead of building a dedicated data center to process these one-time transactions, the infrastructure should be built through the cloud-computing model to allow for real-time on-demand availability of the necessary additional resources through the cloud. Election authorities in one state might use the secure computing facilities in another to handle the bursts of traffic they experience at a particular hour of the day. The ability of global application delivery through the cloud would be critical to ensure efficiency and performance in the event of "voting storms" on the network.

8. Conclusion

Some countries and states will probably move ahead with these voting systems quickly. The advancement of biometric databases, point-to-point security for both the end-user and the network, and on-demand application delivery solutions via the cloud and regulatory controls would play a pivotal role in this next-generation technology definitely. Thus cloud computing technology has been implemented for the purpose of voting.

Thus the candidate can vote irrespective of polling booth as all the polling booth are combined to form the cloud structure with the support of smart client technology.

References

[1] Anil K. Jain, "An Identity-Authentication System Using Fingerprints", Proceedings of the IEEE, Vol. 85, No. 9, pp. 1365 – 1387, September 1997.
[2] Michael Miller, "Cloud Computing- A Web Based Applications That Change the Way You Work and Collaborate Online", August 2008.
[3] Mr. Aviv, "All IP- national carrier network based on wireless access technologies", Converge, November 04, 2008.
[4] B. Miller, "Everything you need to know about automated Biometric identification" Security Technol. Design, Apr.1997.
[5] Wenmoth, D. (2008) Education in the age of cloud computing.
[6] Advanced Networks, Virtualisation, cloud computing, emerging technologies, networks and learning.
[7] M. Bacca, K. Rabuzin: "Biometrics in Network Security", the Proceedings of the XXVIII International Convention MIPRO 2005, and Rijeka, Croatia.