SOLUTION ARCHITECTURE

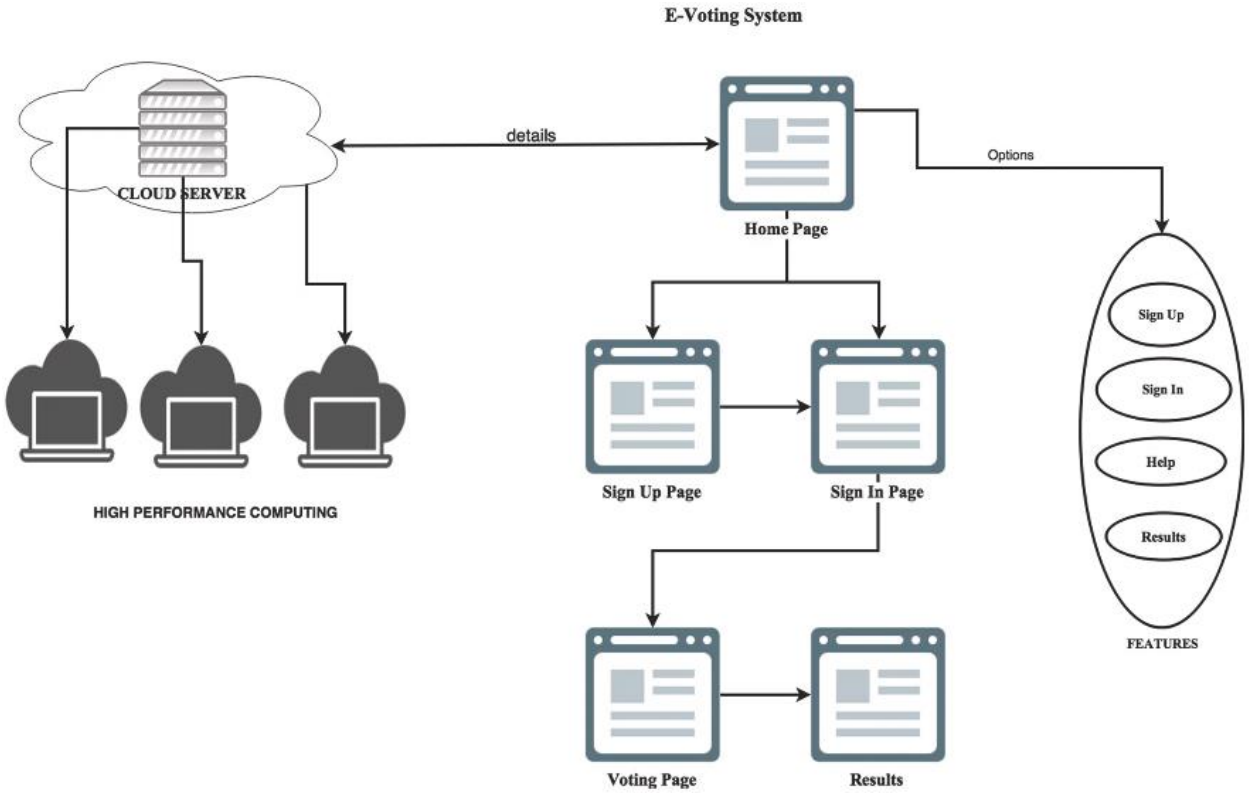
TEAM ID	**NM2023TMID04404**
PROJECT NAME	**ELECTRONIC VOTING SYSTEM**

- **The voter would then select one of the possible choices before casting their ballot into a box at a polling station. An example ballot taken from the political election of Thailand.**

- **After the voting period is over, the voting authorities would usually carry the boxes that are filled with the voters ballots and bring them to a public place that was reserved for voting tallying. The boxes would be open, and each of the ballots would be checked for correctness, and the votes would be classified publicly.**
- **To help authenticate the tallying process, stakeholders in the voting would usually be presented to witness the vote tallying process.**
- **Traditional ballot-based voting systems suffer from many disadvantages. For the voting process, the ballots must be prepared beforehand to account for all potential voters for every polling station.**
- **These ballots are notNreusable. Preparing the ballots, in turn, becomes an expensive undertaking that is also time-consuming to print out all the ballots. Another major issue found is during the voting tally.**

The voting tally is a manually intensive process. Due to the nature of the tally process, it is time-consuming to examine each of the ballots, classify the ballots, and tally the votes.

Due to the shortcomings of existing approaches, the proposal of an alternative approach is recommended. The new approaches should be able to address the following challenges:



• Securing Network Infrastructure: A highly securedelectronic voting system must ensure that all network infrastructure related devices must be able to withstand all kind of cyber-attacking;

• Securing Voting Data: A highly secured electronicvoting system must keep all the voting data in such a way that the result can always be available for tallying while ensuring that all the data cannot be tampered either through cyber-attacking nor cheating by internal officers;

• Trust Management: A highly secured electronic voting system must be able to prove to every voter that all the vote records and results are 100% reliable and trustable to all related parties.

Another area is to expand the test voting scenario, and a larger voting scenario could be explored and examined in further details.

Another area would be exploring the security of the system, by attempting systematic attacks on the system to examine the resilience of the system.

Another future work that would be useful is to propagate the usefulness of blockchain technology in elections to a wider audience so that the voting authorities and governmental organizations would examine the technology and may adopt it for future voting.