Project Development Phase

Debugging & Traceability

TEAM ID	NM2023TMID04400
PROJECT NAME	BIOMETRIC SECURITY SYSTEM FOR VOTING PLATFORM

THE GIST:

- Antique voting gear disappears from polls by the 2008 election. The workhorse voter system of tomorrow is part high tech, part low: It looks like an ATM that spits out a correctly marked, machine-readable piece of paper that can also be counted and definitively checked by human eyes.

FALSE ALARM:

- Political machines can't be trusted: All-electronic systems and Internet crypto fall far short of ensuring "one person, one vote."

- Good point, and that's why total automation isn't the goal - experts warn that error and fraud are best minimized by human oversight at each step of the process.

EXHIBIT A:

- The Caltech-MIT Voting Technology Project, an interdisciplinary campaign launched early this year, seeks to identify the pitfalls in current polling procedures and outline ways to make voting machines foolproof.

- The project's February report warned that all forms of poll automation used in the November election were, on average, less reliable than the old manually marked paper forms, hence the desire for a hybrid solution.

WORDS TO LIVE BY:

- "All current and recently proposed systems are inadequate."

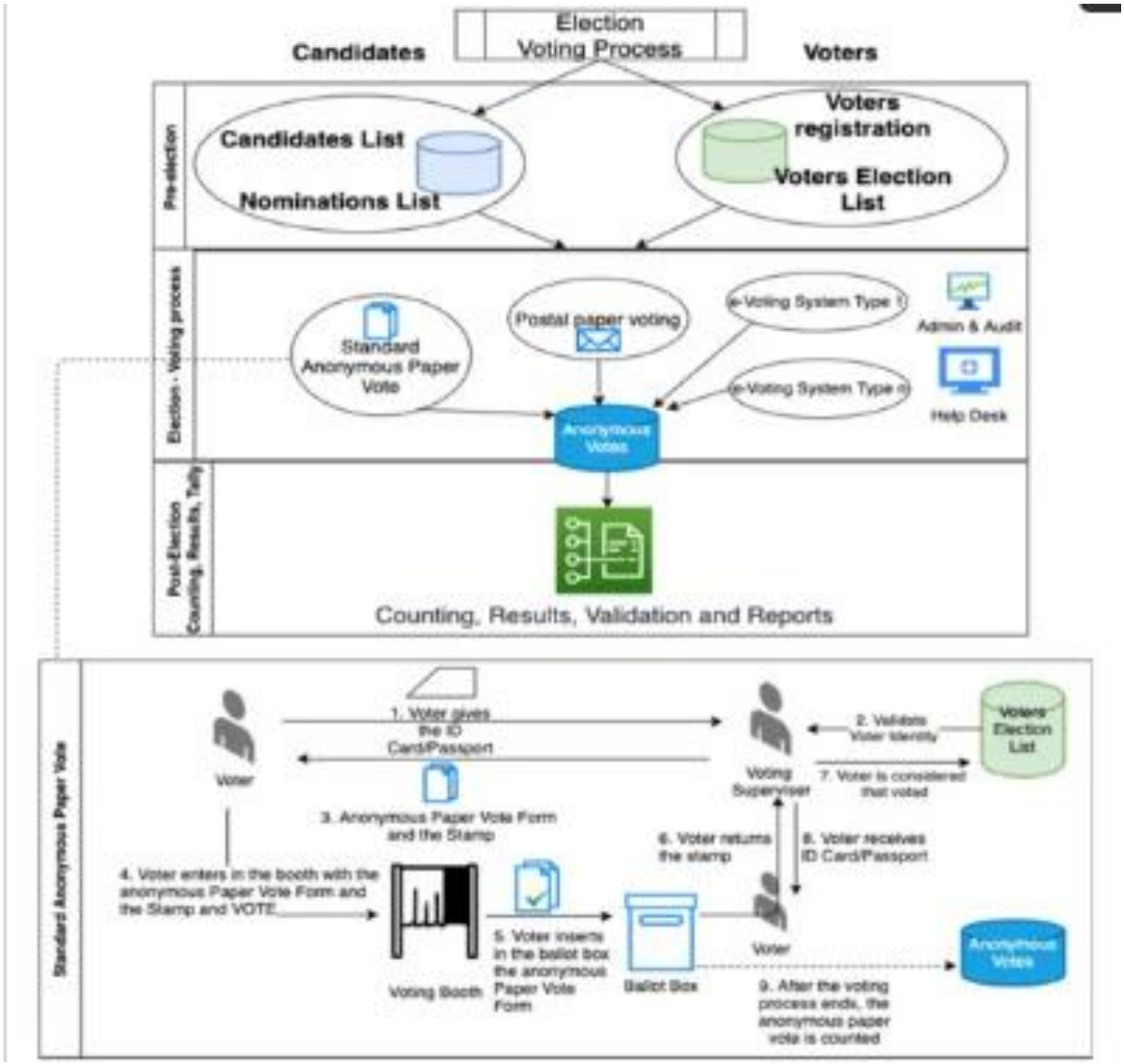
ON THE RISE:

- Senators Charles Schumer (D-New York) and Sam Brownback (R-Kansas) want $2.5 billion in federal matching funds to assist states in upgrading voting systems, while California legislators are pushing for $300 million of state money.

- With that kind of cash on the table, companies like Sequoia Voting Systems will face healthy competition: Unisys, Dell, and Microsoft are already working jointly on an electronic system.

FUTURE REFERENCE:

- Election Center (www.electioncenter.org); Caltech-MIT Voting Technology Project (www.vote.caltech.edu); Federal Election Commission (www.fec.gov/pages/faqsvss.htm); Mercuri's site (www.notablesoftware.com/evote.html)



The Concept of Traceability and Traceability Tokens :

- To establish these correlations between votes in different elections, we propose the introduction of traceable tokens, or pseudonyms, as identifiers of voter origin that should be separated and impossible to associate with the voter's true identity, but remain constant for each voter throughout elections.
- It is a very simple notion, but we have found no literature on the subject. It is likely that work on traceability exists under different naming.

Traceability (token) Requirements

Consistency:

- A voter should not be able to submit votes with different pseudonyms in different elections.

Collision-free:

- Pseudonyms from different voters should not collide.

Secrecy:

- Pseudonyms must not be stored or accessible alongside data that may reveal voter identity. This means it must never be available to administrators.

Coercion:

- To prevent proof of vote, pseudonyms must be unknown to voters. If a voter is able to prove his vote, he may be coerced to vote in a predefined way. For this reason, the pseudonym should be handled in a secure and transient way by voter software.

Levels of traceability

- We can think of three different levels of traceability:

1. Weak:

- users can include pseudonym in their votes in different elections, but there is no way to verify they keep using the same token, so voters are given the liberty to choose whether their votes are to be associated.
- There is also no way to verify that no two users share the same token, so votes from different voters may be incorrectly associated. Under the requirement definitions above, weak traceability systems provide no consistency.
- This level of traceability can be trivially added whenever there is flexibility to provide a free-form field in the ballot: the user simply uses a

predefined form to fill in, if he opts to, a pseudonym of his choice, without any verification.

2. Strong:

- users are forced to use their token consistently throughout elections, and that token is guaranteed to be unique.