# An Improved Dynavote E-Voting Protocol Implementation

*Abdulwasiu Kailani AbdulRahim, University of Agriculture, Nigeria*

*Olusegun Folorunso, University of Agriculture, Nigeria*

*Sushil K. Sharma, Ball State University, USA*

## ABSTRACT

*Electronic voting—the use of computers or computerized voting equipment to cast and tabulate and tally ballots in an election in a trustable manner—is a pillar of e-Government. The DynaVote voting protocol system proposed by Cetinkaya and Koc (2007) is assumed secure and practicable on a network. However, the DynaVote e-Voting protocol does not completely protect the voting counter against impersonated votes, especially when the pseudo-Vote identities are known by the wrong voter or compromised by authorities. To address this problem, a prototype called improved DynaVote e-Vote protocol was designed to protect the counter from anomalies associated with counting impersonated votes (multiple votes) in the same election. This was achieved by introducing biometric fingerprint and pseudo voter identities (PVID) encryption for each voter during voter registration via online or data mining of population data containing fingerprint biometrics. Furthermore, fingerprint reader and RSA public key cryptography is used in PVID to eliminate counting impersonated votes. The performance results showed that improved DynaVote e-Vote protocol is more reliable, eligible, and accurate, and protects voter privacy against other e-Vote protocols.*

*Keywords:* *Biometrics, DynaVote, E-Voting, E-Voting Requirements, Protocol, Pseudo Voter Identities (PVID), RSA Public Key Cryptography*

## INTRODUCTION

Traditionally, elections have served as the official mechanisms for people to express their views to their governments or organisations, while surveys have augmented elections as unofficial but nonetheless valuable measures of public opinion. In both elections and surveys, privacy and security are usually desired, but not always simultaneously achievable at a reasonable cost. Mechanisms that ensure the security and privacy of an election can be time consuming and expensive for election administrators, and inconvenient for voters. Conducting secure and private elections can become even more difficult when voters are geographically distributed. Due to the rapid growth of computer networks and advances in cryptographic techniques, electronic polling is now a viable alternative for many non-governmental elections and surveys, and it is likely to become viable for governmental elections as well. Electronic polling over the Internet can be convenient for voters with easy access to networked computers,

DOI: 10.4018/jea.2011070104

even if the voters are geographically distributed. In addition, electronic elections and surveys can be inexpensive to administer. However, if not carefully designed, electronic voting/polling systems can be easily compromised, thus corrupting results or violating voters' privacy.

Electronic government (e-Government) in democratic generation is essential in this era of Information and Communication Technology (ICT) drive. Electronic voting (e-Voting) is one of pillars of the e-Government, which means the use of computers or computerized voting equipment to cast and tabulate, tally ballots in an election in a trustable manner. As a result of the nature of electronic systems, the security and reliability of the system should be handled properly in order to make the e-Voting system an acceptable alternative to the paper base voting system for the elections in Nigeria or elsewhere.

The DynaVote voting protocol system claims that it is secure and practicable on a network fulfilling main voting requirement (privacy, eligibility, accuracy, reliability, etc.) (Cetinkaya & Doganaksoy, 2007a). DynaVote does not use complex algorithms such as homomorphic encryption and does not require anonymous communication channel such as mix-nets. Beside it has no physical assumption such as untapped channel. It only need an unlink-able Pseudo-Voter Identity technique or mechanism so it employs Pseudo-Voter Identity (PVID) scheme (Cetinkaya & Doganaksoy, 2007a) which relies on blind signature (PVID) scheme provides PVIDS that are unlink-able to the voter real identity for security, transparency and mobility.

It is popularly known that the development of complete protocol as a software implementation is not easy job. Developing a software requires considerable time and cost. Therefore in order to make use all resources, implementation of prototypes gains more importance. This paper project presents a prototype design and implementation of Improved DynaVote e-Vote protocol system on internet that uses Fingerprint biometrics data for validation of vote. The prototype includes implementation of a PVID scheme component as well as Fingerprint biometrics Identity (BIOFIGID) during registration. In its current level the prototype mainly serves practical purpose to actualize the An Improved DynaVote e-Vote Protocol system scheme which is more secure. During the development some implementation issues has arisen. This paper shows that the implementation issue will be resolvable and Improved DynaVote e-Vote protocol on internet is reality and applicable for large scale elections, as well as implementing the PVID and BIOFIGID scheme that will provides unlink-ability for sustainable e-Government in Nigeria.

Traditionally, Electoral fraud has been prevented through the use of physical security measures, audit trails and observers representative of all parties involved. But the prevention of electoral fraud is made more difficult by the frequent requirement that votes remain private. Observer may not observe a ballot until after is has been placed in a ballot box, and audit trails must not provide the ability to link a ballot back to the voter who cast it, even so, these security measures generally work well enough that the possibility of widespread fraud is small. It important to note that designing an electronic polling system, it is essential to consider ways in which the tasks involved can be performed electronically without sacrificing voter privacy or introducing opportunities for fraud. In addition, it is useful to consider all desirable voting or polling system properties, including those not always achievable in traditional systems Lorrie and Ron (1997).

The protocols described in the work are to monitor fraudster whose behavior is typically exploited by authorities and voters.

We start by addressing the problem by considering active internet-based routine fraud, authorities and voters monitoring. The key part of the approach is that it can contribute significantly to computer base voting (e-Voting), if it is employed as a new layer of defined to e-voting protocol.