Chapter 8
E–Vote:
A Cloud–Based Electronic Voting System for Large–Scale Election

Ionut-Mihai Posea
University Politehnica of Bucharest, Romania

Marius Ion
University Politehnica of Bucharest, Romania

Florin Pop
University Politehnica of Bucharest, Romania

Decebal Popescu
University Politehnica of Bucharest, Romania

Nirvana Popescu
University Politehnica of Bucharest, Romania

ABSTRACT

The electoral system is an essential element for the survival of the democracy. Efforts are being made to develop voting systems that are convenient, reliable, transparent and secure. However, considering the security problems that can occur using the underlying technologies, it is difficult to construct an impenetrable system. This chapter presents e-Vote, a distributed electronic voting system architecture that is designed to ensure the accuracy, privacy, verifiability, convenience, and the openness of the democracy of a large-scale electoral process. We describe the necessary requirements for the e-voting protocol, and propose a cryptographic voting scheme that achieves them. The e-voting protocol makes use of several well-established cryptographic primitives e.g. symmetric and asymmetric encryption, digital signatures, blind signatures and secret sharing. Using the suggested framework, we also demonstrate an approach using the current computing and network technologies to effectively describe an architecture that can support a computationally secure and reliable voting process.

INTRODUCTION

The electoral system is an essential element of the democracy, and moving it into an electronic service is one of the more important issues for e-Democracy. Electronic voting (also known as e-voting) is a term that defines several different types of voting, including both electronic methods of casting a vote and electronic methods of counting votes. The electronic voting is considered to be an important topic.
for the progress of democracy in the world. If a secure and convenient electronic voting system can be developed, it can be used more frequently to collect people’s opinion on a variety of decisions using electronically methods. An efficient analysis over the types of possible attacks, their scope, target or probability can help in the process of developing an electronic voting architecture that must be computationally secure, reliable and trusted. A paper by Beroggi (2004) concludes that an electronic voting system, even when exposed over the Internet, should exploit the new technologies for the design, realization and maintenance of the voting systems. It is noted that trust is a major issue of concern, but starting to use the electronic voting systems is equivalent to postal or ballot voting. With time, use, experience and continued improvements, the trust will be built and the system accepted by the citizens.

Electronic voting systems may offer advantages over the other voting methods. An electronic voting system can be involved in any one of a number of steps in the setup, distributing, voting, collecting, and counting of ballots, and thus may or may not introduce advantages into any of these steps. Simultaneously achieving security and privacy in electronic polls is a problem that must be solved if electronic systems are to be used for serious large-scale governmental elections. As new technologies emerge which address these concerns, electronic voting is likely to become increasingly appealing as an alternative to the traditional paper ballots method. Electronic elections have the potential of being cheaper and less time consuming to administer than conventional elections. Eventually electronic voting may be a viable solution to increasing voter participation and maximizing security by decreasing the number of frauds in governmental elections.

The Cloud Computing paradigm offers support for e-Services development in an easy to use meaner, with continuous access, direct communication, and with timely and consistent information. The e-Services are exposed to all kind of threads from the Internet, so when it comes about their security or other challenges, it should receive a special attention. In a digital world, when it comes to e-Services, there are some main characteristics that are common to all of them. One of them is scalability, which indicates the ability to handle growing amounts of work in a graceful manner or its ability to be enlarged, so the distributed environments are required. Cloud systems offer the best support for hosting e-Services by offering solution to the issues addressed by e-Services.

The main focus of this chapter is to present a Cloud-based e-voting system (e-Vote) in order to ensure the security, interoperability and availability of our proposed systems. This is not a new system; it rather extends several existing systems and we highlight the methodology to design such a system. We propose a modular system with a distributed architecture that is be deployed using different services available in the Cloud; so it is easy to extend and improve functionality, re-use software modules that are proved to be reliable and the required audit or supervising process can be conducted in an efficient manner. Furthermore, the implementation of the proposed and its usage as a national electronic voting system can lead to cost reductions, an important aspect as state budget funds are tightening.

The e-Vote system is considered computationally secure and even if the data transmission can be intercepted, highly improbable as the network is not open to public access, using actual computing power the information cannot be disclosed in a reasonable amount of time. Also, because the electoral process is the foundation of democracy, voting systems must be designed with great care. Such systems are very important, and can be very well compared to other types of critical systems such as those used in the military, in the financial and banking sectors, or in medicine. All these critical systems can only be implemented if we know beyond any doubt that they not fail unless faced with exceptional circumstances. Electronic voting systems, in general, and the e-Vote protocol in particular, share this trait. It