

## **An Application of Artificial Neural Networks to Continuous Authentication**

Karishma Asthana

*Continuous Authentication* (CA) is an important security mechanism which has far-reaching implications. It surpasses traditional authentication in that it works against “lunchtime attacks” and “masquerade attacks”. However, beyond this, continuous authentication is applicable to more large-scale situations such as implementation in flight decks (in response to the 9/11 attacks) or large vehicles (in response to recent terrorist attacks using trucks). Although CA systems are a powerful security measure, they pose many challenges in terms of trading off between security and usability. In order to address this, we can look to Artificial Neural Networks (ANNs) for biometric authentication. Biometric traits allow for non-intrusive and passive authentication. ANNs are not “statically” programmed, so they can adjust well to different environments and work well with noisy data. The main goal of my project is to develop a proof-of-concept, powered by neural networks, which will continuously authenticate faces. The main scope of my prototype is for the workplace setting. It takes in as input an RFID card scan, which then triggers the authentication to begin. My neural network then looks to match the face found to the ID card scanned, such that the software does not have to compare the face against all faces in a database to determine if it is a valid person. It can instead have a very quick, binary decision of if it matches the scanned card. The neural network utilizes the Adam Optimization algorithm, an algorithm which works well with noisy data. With this algorithm, the neural network achieves 99% accuracy.