A

Project Report

On

MULTI CONTROL BANKING TECHNIQUE

Submitted to

Department of
Computer Science and Engineering

By

SEELAM NANDHINI	(206Y1A6720)
YARA SAI SRI	(206Y1A6723)
BIJJA PRIYA CHANDRIKA	(206Y1A6705)
KYATHAM JYOSHNA	(216Y5A6702)

Under the guidance

Of

Mr.E.HARIKRISHNA
Asst.Professor

Department of Computer Science & Engineering

SUMATHI REDDY INSTITUTE OF TECHNOLOGY for WOMEN

(Approved by AICTE, New Delhi; Affiliated to JNTU, Hyderabad)

Ananthasagar(Vill), Hasanparthy(M), Warangal – 506 371 (A.P.), Website : www.sritw.org

2022-2023

S.R.I.T. FOR WOMEN * WARANGAL *

PRINCIPAL
Sumathi Reddy Institute of Technology for Women
Ananthasagar (V), Hasanparthy (M)
WARANGAL - 506 371 (T.S.)

SUMATHI REDDY INSTITUTE OF TECHNOLOGY for WOMEN

(Approved by AICTE, New Delhi; Affiliated to JNTU, Hyderabad)

Ananthasagar(Vill), Hasanparthy(M), Warangal – 506 371 (A.P.), Website : www.sritw.org

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the project entitled **"MULTI CONTROL BANKING TECHNIQUE"** is submitted by SEELAM NANDHINI(206Y1A6720), YARA SAI SRI(206Y1A6723), BIJJA PRIYA CHANDRIKA(206Y1A6705) and KYATHAM JYOSHNA(216Y5A6702) to the department of Computer Science and Engineering during academic year 2022-23.

Mr.E.HARIKRISHNA
Project Guide

Dr.E.SUDARSHAN
Head of the Department

S.R.I.T. FOR WOMEN * WARANGAL *

PRINCIPAL
Sumathi Reddy Institute of Technology for Women
Ananthasagar (V), Hasanparthy (M)
WARANGAL - 506 371 (T.S.)

ABSTRACT

Pattern classification systems are commonly used in adversarial applications, like biometric authentication, network intrusion detection, and spam filtering, in which data can be purposely manipulated by humans to undermine their operation. As this adversarial scenario is not taken into account by classical design methods, pattern classification systems may exhibit vulnerabilities, whose exploitation may severely affect their performance, and consequently limit their practical utility. Extending pattern classification theory and design methods to adversarial settings is thus a novel and very relevant research direction, which has not yet been pursued in a systematic way. In this paper, we address one of the main open issues: evaluating at design phase the security of pattern classifiers, namely, the performance degradation under potential attacks they may incur during operation. We propose a framework for empirical evaluation of classifier security that formalizes and generalizes the main ideas proposed in the literature, and give examples of its use in three real applications. Reported results show that security evaluation can provide a more complete understanding of the classifier's behavior in adversarial environments, and lead to better design choices.