Avinashilingam Institute for Home Science and Higher Education for Women
(Deemed to be University Estd. u/s 3 of UGC Act 1956, Category A by MHRD)
Re-accredited with 'A++' Grade by NAAC.CGPA 3.65/4, Category I by UGC
Coimbatore – 641 043, Tamil Nadu, India

PLAGIARISM CHECK REPORT (THESIS)

1.	Name of the Research Scholar	Swathy Akshaya M
2.	Roll No. and Year of Registration	17PHCSF003, 2017
3.	Department	Computer Science
4.	Name of the Research Guide	Dr. G. Padmavathi
5.	Title of the Thesis / Dissertation	PERFORMANCE · EFFICIENT METHODS TO HANDLE ZERO-DAY ATTACKS IN CLOUD ENVIRONMENT
6.	Similarity Content (%) Identified	**6%**
7.	Software Used	Turnitin
8.	Date of Verification	10-01-2026

Note : The report is excluding 14 Consecutive words, Review of Literature and Quoted Materials.

Checked by :

10/1/26
Information Scientist

Research Scholar

K. Mahalakshmi 10/1/26
Assistant Librarian

10/1/2026
Research Guide

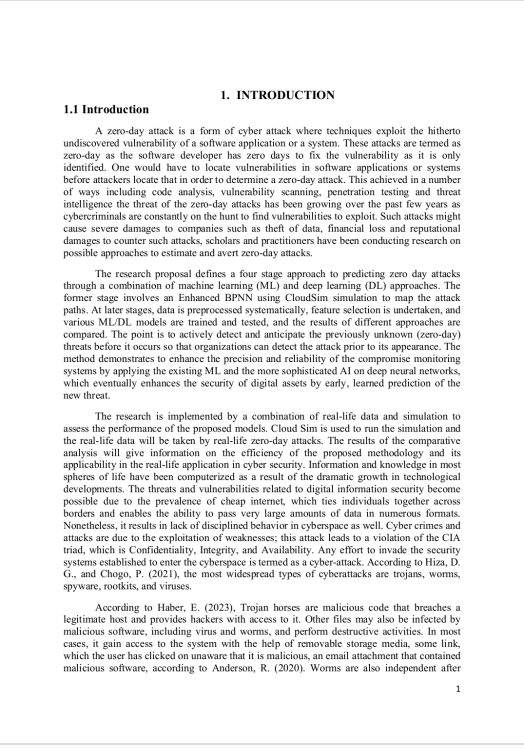
Date: 10-01-2026

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Central Library
Assignment title:	New Assignment 2025
Submission title:	PERFORMANCE EFFICIENT METHODS TO HANDLE ZERO-DAY A...
File name:	Swathi_Thesis_Plag_2.docx
File size:	3.74M
Page count:	137
Word count:	54,265
Character count:	300,925
Submission date:	10-Jan-2026 04:45PM (UTC+0530)
Submission ID:	2854712481



1. INTRODUCTION

1.1 Introduction

A zero-day attack is a form of cyber attack where techniques exploit the hitherto undiscovered vulnerability of a software application or a system. These attacks are termed as zero-day as the software developer has zero days to fix the vulnerability as it is only identified. One would have to locate vulnerabilities in software applications or systems before attackers locate that in order to determine a zero-day attack. This achieved in a number of ways including code analysis, vulnerability scanning, penetration testing and threat intelligence the threat of the zero-day attacks has been growing over the past few years as cybercriminals are constantly on the hunt to find vulnerabilities to exploit. Such attacks might cause severe damages to companies such as theft of data, financial loss and reputational damages to counter such attacks, scholars and practitioners have been conducting research on possible approaches to estimate and avert zero-day attacks.

The research proposal defines a four stage approach to predicting zero day attacks through a combination of machine learning (ML) and deep learning (DL) approaches. The former stage involves an Enhanced BPNN using CloudSim simulation to map the attack paths. At later stages, data is preprocessed systematically, feature selection is undertaken, and various ML/DL models are trained and tested, and the results of different approaches are compared. The point is to actively detect and anticipate the previously unknown (zero-day) threats before it occurs so that organizations can detect the attack prior to its appearance. The method demonstrates to enhance the precision and reliability of the compromise monitoring systems by applying the existing ML and the more sophisticated AI on deep neural networks, which eventually enhances the security of digital assets by early, learned prediction of the new threat.

The research is implemented by a combination of real-life data and simulation to assess the performance of the proposed models. Cloud Sim is used to run the simulation and the real-life data will be taken by real-life zero-day attacks. The results of the comparative analysis will give information on the efficiency of the proposed methodology and its applicability in the real-life application in cyber security. Information and knowledge in most spheres of life have been computerized as a result of the dramatic growth in technological developments. The threats and vulnerabilities related to digital information security become possible due to the prevalence of cheap internet, which ties individuals together across borders and enables the ability to pass very large amounts of data in numerous formats. Nonetheless, it results in lack of disciplined behavior in cyberspace as well. Cyber crimes and attacks are due to the exploitation of weaknesses; this attack leads to a violation of the CIA triad, which is Confidentiality, Integrity, and Availability. Any effort to invade the security systems established to enter the cyberspace is termed as a cyber-attack. According to Hiza, D. G., and Chogo, P. (2021), the most widespread types of cyberattacks are trojans, worms, spyware, rootkits, and viruses.

According to Haber, E. (2023), Trojan horses are malicious code that breaches a legitimate host and provides hackers with access to it. Other files may also be infected by malicious software, including virus and worms, and perform destructive activities. In most cases, it gain access to the system with the help of removable storage media, some link, which the user has clicked on unaware that it is malicious, an email attachment that contained malicious software, according to Anderson, R. (2020). Worms are also independent after

1

PERFORMANCE EFFICIENT METHODS TO HANDLE ZERO-DAY ATTACKS IN CLOUD ENVIRONMENT

by Central Library

Submission date: 10-Jan-2026 04:45PM (UTC+0530)
Submission ID: 2854712481
File name: Swathi_Thesis_Plag_2.docx (3.74M)
Word count: 54265
Character count: 300925

PERFORMANCE EFFICIENT METHODS TO HANDLE ZERO-DAY ATTACKS IN CLOUD ENVIRONMENT

ORIGINALITY REPORT

6%	2%	5%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	aircconline.com Internet Source	<1%
2	Hamid Gavari Bami, Elaheh Moharamkhani, Behrouz Zadmehr, Vahid Najafpoor, Mohammad Shokouhifar. "Detection of zero-day attacks in computer networks using combined classification", Concurrency and Computation: Practice and Experience, 2022 Publication	<1%
3	"Theory and Models for Cyber Situation Awareness", Springer Science and Business Media LLC, 2017 Publication	<1%
4	Nerella Sameera, M. Shashi. "Deep transductive transfer learning framework for zero-day attack detection", ICT Express, 2020 Publication	<1%
5	Dominic John Kavoi, Charles Jumaa Katila, Richard Otieno Omollo. "An Ensemble Machine Learning Based Algorithm to	<1%