iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.82866

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

Analytical Study of Cybersecurity Awareness and Data Protection in Digital Systems

Sneha Nitin Chavan
Department of Computer Engineering, JSPM Narhe Technical Campus Pune, India

Abstract: ***In the digital age, cybersecurity is a pressing issue due to the increase in internet-connected systems and services. This research paper explores cybersecurity awareness and some of the data protection methods for digital information security. This research paper presents potential threats such as phishing attacks, viruses, and data breaches and explores measures to mitigate these risks. It also examines user education, encryption and authentication techniques. It concludes that technical and human factors play a crucial role in enhancing the security of data. This article seeks to offer basics for beginners in understanding cybersecurity practices, and strongly advocates for security systems to be constantly upgraded.***
Keywords: Cybersecurity, Data Protection, Encryption, Malware, Phishing, Authentication

I. INTRODUCTION

Thanks to the technological revolution, cybersecurity has become a critical component of computer systems. Internet-based services are being used to communicate, transact, educate and conduct business. But this has also led to an increased vulnerability to cyber threats, including hacking, phishing and malware attacks.

Cybersecurity is the protection of systems, networks and data from cyber attacks [1],[7]. In previous research, hacking has been found to be due to lack of awareness and security measures [3],[4]. Encryption, firewalls and authentication technologies are some of the methods proposed for security [1].

This research is about the understanding of cybersecurity awareness and the assessment of simple methods of data protection. The aim of this study is to showcase easy yet useful strategies that users can adopt to secure their data and minimise cyber-related threats.

A. Study Purpose

1) To identify cybersecurity challenges
2) To understand the fundamental techniques of data security
3) To understand the role of user awareness
4) To give basic security tips to start

B. Organization

This paper is structured as follows: Section 1 has a brief discussion on cybersecurity, Section 2 talks about related work, Section 3 has the theoretical concepts used, Section 4 has the methodology used, Section 5 has the results and discussion, Section 6 discusses the conclusion of the study and future works.

II. RELATED WORK

There has been extensive research in cyber security and data protection in recent years. Many studies have described various techniques for encryption of data communication [5]. The role of firewalls in securing network systems has also been discussed [1]. There have been some studies on techniques of malware detection and prevention [4]. Other research has also reported on the latest techniques for data protection in electronic systems [1].

In recent research, the focus is on educating users to prevent attacks. It is found that users are a main cause of data breach [4],[6]. Both technical and human factors can be used to improve data safety [3],[6]. There have also been studies that have focused on phishing attacks and prevention [2]. These studies show that technical and human factors should be taken into account to secure data.

III. THEORY OR CALCULATION

Cybersecurity is based on three main principles known as the CIA triad [1]:

1) Confidentiality: Ensures that data is accessed only by authorized users.

2) Integrity: Ensures that data remains accurate and unaltered.
3) Availability: Ensures that data is accessible when required.

Encryption is a key technique used to secure data by converting it into an unreadable format [5]. Authentication methods such as passwords, One-Time Passwords (OTP), and biometric systems are used to verify user identity and prevent unauthorized access [3].

IV. EXPERIMENTAL METHOD / PROCEDURE

A. *Proposed Methodology*

This study follows a simple and structured approach:

1) Identification of common cyber threats such as phishing and malware
2) Analysis of existing security techniques like encryption and firewalls
3) Comparison of different methods based on effectiveness
4) Suggestion of improvements for better data protection

B. *Process Flow*

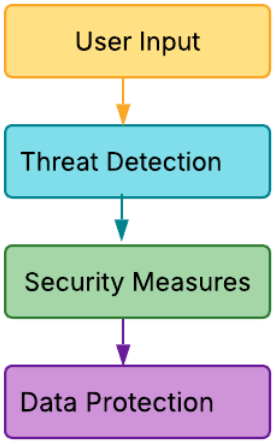


Figure 1: Flowchart of Threat Detection and Data Protection System

V. RESULTS AND DISCUSSION

A. *Results*

The findings of the study are as follows:

1) Weak passwords increase the risk of cyber attacks [4]
2) User awareness reduces the success rate of phishing attacks [2]
3) Encryption significantly improves data security [5]

TABLE I
SECURITY TECHNIQUES COMPARISON

Technique	Advantage	Limitation
Encryption	High data security	Complex to use
Firewall	Network protection	Limited coverage
Antivirus	Detects malware	Requires updates

B. *Discussion*

The results indicate that no single security technique is sufficient to provide complete protection. A combination of different methods is necessary to ensure effective cybersecurity. User awareness plays a crucial role in preventing cyber attacks. Simple practices such as using strong passwords and avoiding suspicious links can greatly reduce risks.

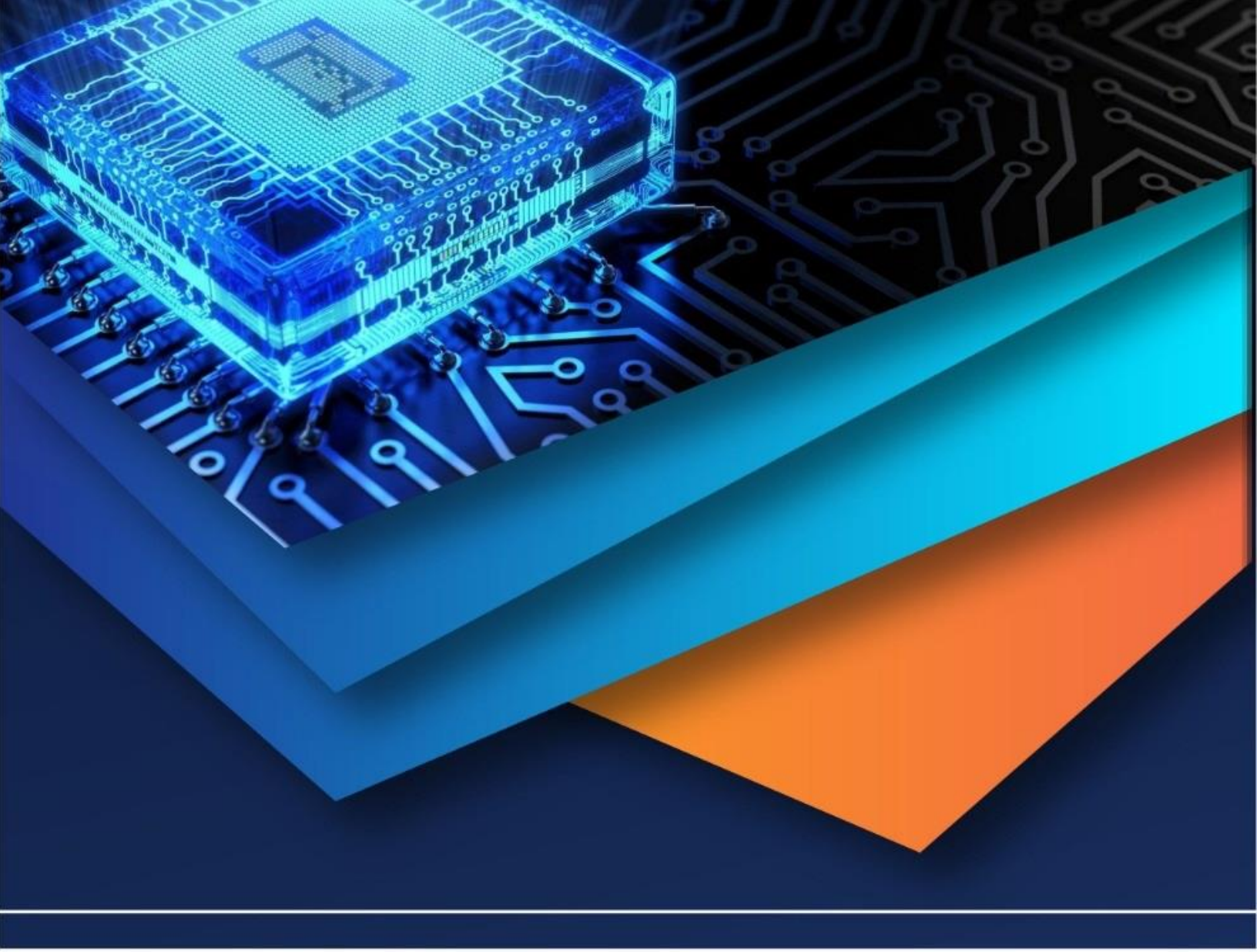
VI. CONCLUSION AND FUTURE SCOPE

Cybersecurity has become an essential part of modern digital systems. This study highlights the importance of cybersecurity awareness and basic data protection techniques in reducing cyber threats. The results show that combining encryption, firewalls, and user education can significantly improve data security. However, challenges such as evolving cyber attacks and lack of awareness still exist.

Future work can include proposing criteria and guidelines for implementation and monitoring of security systems [6].

REFERENCES

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed. Pearson, 2022.
[2] A. Alsharnouby, F. Alaca, and S. Chiasson, “Why phishing still works: User strategies for combating phishing attacks,” International Journal of Human-Computer Studies, vol. 82, pp. 69–82, 2015.
[3] S. Furnell and N. Clarke, “Power to the people? The evolving recognition of human aspects of security,” Computers & Security, vol. 55, pp. 39–51, 2015.
[4] Verizon, “2023 Data Breach Investigations Report (DBIR),” 2023.
[5] D. Boneh and V. Shoup, A Graduate Course in Applied Cryptography, 2020.
[6] National Institute of Standards and Technology (NIST), “Framework for Improving Critical Infrastructure Cybersecurity,” 2023.
[7] B. Schneier, Secrets and Lies: Digital Security in a Networked World. Wiley, 2015.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY