|  |  |  |  |
| --- | --- | --- | --- |
| **Student Name :** | Lucky Pathan S. | | |
| **Enrollment No** | 210303105790 | **Branch :** | CSE |
| **Title of Journal Paper** | Design And Implementation Of Network Security | | |
| **Authors** | Nwauba Nnaemeka Kennedy | | |
| **Journal / Conference :** | Department Of Computer Science And Information Technology, Caritas University | | |
| **Volume / Issue** | 1 | **Pages :** | 48 |

**Section – 01**

**Abstract / Introduction**

**Abstract:-**

**(1) What is the objective of the Paper?**

Purpose of the research paper is to improve the security that flexible communication infrastructures which provide a diverse set of operations. Understanding the network data flow to manage data packages.

**(2) What are the main results mentioned in the abstract?**

Access control is the ability to permit or deny the use of a particular resource by a particular entity. Access control mechanisms can be used in managing physical resources, logical resources, or digital resources.

**(3)** **What rational is given by the authors, attributing importance to the research problem?**

* in this document authors mention bank low level network security and plans to improve it by adding encryption and access control for user verification .
* Bank has no security from attacks like eavesdropping, loops, and traffic amplification.
* To overcome from this problem we uses challenge-responses and erasure-coding, for minimum security of the bank network.

**Section – 02**

**Methodology**

**(1) Describe the methodology is used by author(s) to address the research problem?**

In this project , Administration is an aspect of running the organization by devising systems

which will run smoothly. The goal of authentication is to first verify that the user, either a person or system, which is attempting to interact with your system is allowed to do so. Gathering basic host information, such as its location and security aspects of its connection, is critical. After all process done, inputs are stripped off with headers and all output is the information which is inside the headers and outputs are in human readable form. Several strategies are implemented like User id and Password , Physical security device, Biometric Identification and more.

**(2) In what way the methodology used by the authors is relevant to the methodology you proposed to adopt?**

Based on research we use the network creation and network monitoring data to get multiple hosts with there ID’s and User Profiles.

**Section – 03**

**Results and Conclusions**

**(1) List the results obtained by the authors.**

1. To eliminate all forms of mistakes associated with security control
2. Detecting security violations
3. Re-creating security incidents
4. To disallow unauthorized users
5. To safeguard the organizational data/information
6. To computerized the organizational security
7. To enhance the organizational security

**(2) What are the conclusions drawn by the authors from the study.**

In computer security, access control includes authentication, authorization and audit. It also includes measures such as physical devices, including biometric scans and metal locks, hidden paths, digital signatures, encryption, social barriers, and monitoring by humans and automated systems.

* Identification and authentication determine who can log on to a system, and the association of users with the software subjects that they are able to control as a result of logging in
* Authorization determines what a subject can do
* Accountability identifies what a subject (or all subjects associated with a user) did.

**Critical Analysis**

Based on this research paper , authors described Network Security is essential part of organization.

It is concerned with people trying to access remote services that they are not authorized to use. Most security problems are intentionally caused by malicious people trying to gain some benefit, get attention, or to harm someone. The main purpose of this project is to design a NETWORK SECURITY that will assist bank in the area of ensuring effective security measures

A security context is the collection of roles that a user is associated with. The security context is often defined as part of the authentication process. Depending on the technology used a security context is maintained by the system. Credential is presented to a reader, the reader sends the credential’s information, usually a number, to a control panel, a highly reliable processor .Credentials can be passed around, thus subverting the access control list