A Zero Trust Approach to Network Security

ABSTRACT

In the last years, we have seen an increase in the use of wireless networks due to new forms of communication. The online security has become a hotly debated topic in the community. People want to have access to all of your applications and resources anywhere, anytime. With the increase in the use of Cloud computing and IoT, the number of connected devices increases that consequently also increase the targets of cybercrime. A simple change of mentality can help protect data and the entire network. This paper describes what a Zero Trust Network is and show some concepts behind this architecture/philosophy. Zero Trust is an architecture that has a principle that everything inside or outside the network is not reliable until verified.

**EXISTING SYSTEM**

In the last years, we have seen an increase in the use of wireless networks due to new forms of communication. The online security has become a hotly debated topic in the community. People want to have access to all of your applications and resources anywhere, anytime. With the increase in the use of Cloud computing and IoT, the number of connected devices increases that consequently also increase the targets of cybercrime. A simple change of mentality can help protect data and the entire network. traditional security models are becoming increasingly impractical due to the increase in the sophistication of the attacks and the elimination of the perimeters of computer networks.

**Disadvantages of Existing System**

1.data not secure.

**PROPOSED SYSTEM**

This paper describes what a Zero Trust Network is and show some concepts behind this architecture/philosophy. Zero Trust is an architecture that has a principle that everything inside or outside the network is not reliable until verified. Zero trust arises from the need to simplify data security. In the absence of a simple implementation formula, this philosophy is based on "never trust, always verify". This is the beginning of the change of the mentality eliminating the trust of our network. Zero Trust segmentation platform is the basis of any Zero Trust initiative that allows us to break the network into micro-segmentation, giving us the ability to adapt our needs without restructuring our entire network

**Advantages of Proposed System**

1. data protection.

**SYSTEM REQUIREMENTS**

# System Architecture



Fig.4 Zero Trust Architecture

# Hardware Requirements

# Processor - Pentium –IV

* Speed - 1.1 GHz
* Ram - 256 MB
* Hard Disk - 20 GB
* Key Board - Standard Windows Keyboard
* Mouse - Two or Three Button Mouse
* Monitor - SVGA

**Software Requirements**

* Operating System - Windows XP
* Coding Language - Java