ARGUS - An Adaptive Smart Home Security Solution

R.M. Ruwin R. Ratnayake[1], G.D.N.D.K. Abeysiriwardhena[1], G.A.J. Perera[1], R. Ponnamperuma[1], Amila Senarathne[1], and B.A. Ganegoda[1]

[1]Department of Computer Systems Engineering, Sri Lanka Institute of Information Technology, Sri Lanka.

ruwinrathnayake@gmail.com, it19180694@my.sliit.lk, it19235066@my.sliit.lk, it19156002@my.sliit.lk, amila.n@sliit.lk, binura.g@sliit.lk

Abstract

Smart Security Solutions are in high demand with the ever-increasing vulnerabilities within the IT domain. Adjusting to a Work-From-Home (WFH) culture has become mandatory by maintaining required core security principles. Therefore, implementing and maintaining a secure Smart Home System has become even more challenging. ARGUS provides an overall network security coverage for both incoming and outgoing traffic, a firewall and an adaptive bandwidth management system and a sophisticated CCTV surveillance capability. ARGUS is such a system that is implemented into an existing router incorporating cloud and Machine Learning (ML) technology to ensure seamless connectivity across multiple devices, including IoT devices at a low migration cost for the customer. The aggregation of the above features makes ARGUS an ideal solution for existing Smart Home System service providers and users where hardware and infrastructure is also allocated. ARGUS was tested on a small-scale smart home environment with a Raspberry Pi 4 Model B controller. Its intrusion detection system identified an intrusion with 96% accuracy while the physical surveillance system predicts the user with 81% accuracy.

Keywords

Smart Home System, Intrusion Detection, Activity Monitoring, Surveillance, Firewall, Bandwidth Management, IOT, Cyber Security