Security Framework Connection Assistance for IoT Device Secure Data communication

Sarangam Kodati[1*], *Kumbala* Pradeep Reddy[2], *Thotakura* Veerananna[3], *S* Govinda Rao[4], *G* Anil Kumar[5]

[1]Associate Professor, Department of CSE, Teegala Krishna Reddy Engineering College, Hyderabad, Telangana.
[2]Associate Professor, Department of CSE, CMR Institute of Technology, Hyderabad, Telangana.
[3]Assistant Professor, Department of CSE, Sai Spurthi Institute of Technology,Sathupally, Telangana, India
[4]Professor CSE Department, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad.
[5]Assistant Professor CSE Department, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad.

Abstract: Today, Internet of Things (IoT) services has been increasing extensively because of their optimum device sizes and their developed network infrastructure that includes devices based on internet embedded with various sensors, actuators, communication, and storage components providing connection and data exchange. Presently number of industries use vast number of IoT devices, there are some challenges like reducing the risks and threats that exposure, accommodating the huge number of IoT devices in network and providing secure vulnerabilities have risen. Supervised learning has recently been gaining popularity to provide device classification. But this supervised learning became unrealistic as producing millions of new IoT devices each year, and insufficient training data. In this paper, security framework connection assistance for IoT device secured data communication is proposed. A multi-level security support architecture which combines clustering technique with deep neural networks for designing the resource oriented IoT devices with high security and these are enabling both the seen and unseen device classification. The datasets dimensions are reduced by considering the technique as auto encoder. Therefore in between accuracy and overhead classification good balancing is established. The comparative results are describes that proposed security system is better than remaining existing systems.

1. Introduction:

The Internet of Things (IoT) technology is widely spread around us because of its high level of security and provides best privacy to the system [1]. As much as the best, facilities of the IoT devices are used. If there is increment in connected devices in a network through internet then estimation is created by IoT as billions of users are crossed till 2020 [2]. Therefore security issues are raised by increasing the number of devices in IoT wireless and security devices. Number of devices is connected with internet through the Internet of Things (IoT). So there is chance of threats from unauthorized user on a large scale which can manipulate the data[3]. Therefore data confidentiality, privacy, authorization and authentication are IoT main security issues [16]. In the following mentioned layers attackers can enter into the communication as cloud layer, network layer and hardware layer[6]. The attacker was entered into the communication at hardware layer of IoT device and security parameters are retrieved or hacked which are stored in the IoT device [4]. By using these stolen security parameters virtual IoT device or duplicate one is recreated by the attacker. False data is uploaded to the server by this duplicate IoT device and users secure information is retrieved from network to which IoT device is connected [5].

Once the attacker starts to retrieve security parameters of the IoT device, there are some extra security issues are raised without being physical connection with device. ECC (*Elliptic Curve Cryptography)* and RSA (Rivest–Shamir–Adleman) based encryption keys are stolen by the side channel attacks based on electromagnetic which is exhibited by the researchers. From IoT devices AES encryption keys are stolen by using side channel attacks because all these IoT devices are connected to the internet so weak strength is acquired by IoT devices which causes to interferences in the form of attacks [17]. One example of such attacks is MIRAI malware in which most of the IoT devices outside of the network are attacked. Other internet services and websites are attacked by using network zombies which are from outside of the

Corresponding author: k.sarangam@gmail.com