Received: 15 December 2021 | Revised: 20 April 2022 | Accepted: 12 May 2022

DOI: 10.1002/ett.4578

RESEARCH ARTICLE

WILEY

Block chain fostered cycle-consistent generative adversarial network framework espoused intrusion detection for protecting IoT network

G. Sugitha[1] | **A. Solairaj**[2] | **J. Suresh**[3]

[1]Department of Computer Science and Engineering, Muthayammal Engineering college (Autonomous), Namakal, India

[2]Department of Computer Science and Engineering, Nadar Saraswathi College of Engineering and Technology, Theni, India

[3]Department of Computer Science and Engineering, CARE College of Engineering, Trichy, India

Correspondence
G. Sugitha, Department of Computer Science and Engineering, Muthayammal Engineering college (Autonomous), Rasipuram, Namakal, India.
Email: sugitha1091@gmail.com

Abstract

In smart city infrastructure, IoT networks contain intelligent devices for collecting and processing data using open channel internet. Some challenges have occurred in the existing methods while transferring the data, like centralism, safety, secrecy (data destroying, inference attacks), transparency, scalability, verification, and controlling the rapid adaptation of smart cities. To overcome these challenges, a machine learning based block chain method is proposed in this manuscript. The machine learning strategies can process massive datasets. Furthermore, they contain adequate generalization to identify various attack vectors. Here, the block chain fostered cycle-consistent generative adversarial network (CCGAN) framework espoused intrusion detection is proposed for protecting the IoT network. Also, a 3 level privacy model is introduced for protecting the IoT devices. The first level is block chain based privacy detection and the second level is CCGAN and the third level is classification. In first level, ToN-IoT, BoT-IoT datasets are taken to detect the IoT intrusion, these data's are given to the block chain to authenticate and to collect the data in the IoT devices in the smart cities and stored in the blocks present in the block chain. In second level, the feature mapping and feature selection are done. The normal and attacked instances are classified in level 3. The performance of the proposed method shows higher accuracy 25.37%, 29.57%, and 18.67%, higher recall 23.75%, 17.58%, and 14.68% better than the existing methods, like block chain and machine learning method based privacy protection in IoT using optimized gradient tree boosting system (IOT-BC-XGBoost), and block chain and machine learning method based privacy protection in IoT using deep gated recurrent neural network (IOT-BC-DGRNN), respectively.

1 | INTRODUCTION

In general, the term "smart city" indicates the application of technological-based methods, like IoT, big data analysis, cyber-physical systems, real-time control[1] IoT differs as a type of technology that facilitates the integration of entire distributed sensors as well as smart appliances to gather as well as process data in the smart city structure utilizing