International Journal of Information Security and Privacy
Volume 17 • Issue 1

Optimized Deep Neuro Fuzzy Network for Cyber Forensic Investigation in Big Data-Based IoT Infrastructures

Suman Thapaliya, Department of IT, Lincoln University College, Malaysia*

Pawan Kumar Sharma, Department of Faculty of Science Health and Technology, Nepal Open University, Nepal

ABSTRACT

Forensic skills analysts play an imperative support to practice streaming data generated from the IoT networks. However, these sources pose size limitations that create traffic and increase big data assessment. The obtainable solutions have utilized cybercrime detection techniques based on regular pattern deviation. Here, a generalized model is devised considering the MapReduce as a backbone for detecting the cybercrime. The objective of this model is to present an automatic model, which using the misbehavior in IoT device can be manifested, and as a result the attacks exploiting the susceptibility can be exposed by newly devised automatic model. The simulation of IoT is done such that energy constraints are considered as basic part. The routing is done with fractional gravitational search algorithm to transmit the information amongst the nodes. Apart from this, the MapReduce is adapted for cybercrime detection and is done at base station (BS) considering deep neuro fuzzy network (DNFN) for identifying the malwares.

KEYWORDS

big data, Cyber forensic investigation, Deep neuro fuzzy network, Internet of Things, MapReduce framework

1. INTRODUCTION

The IoT devices link the static or mobile devices and objects using the sensors and actuator and offers smooth communication through network. IoT provides the widespread utilization of several modern technologies and models using the transmission control protocol (TCP) /internet protocol, which emerges in the model of interconnecting devices considering the physical platform. The main aspect adapted in routing considering IoT is efficiency of energy, safe communication, and scalability. The routing and data transmission using sophisticated services provides a key problem in IoT. The online business and Mobile commerce are emerging IoT application. The security considering IoT includes in-depth assessment as a basic need to preserve the network and is essential task. The genuine susceptibility in the IoT platform is insecure web interface, mobile interface and deficiency of security

DOI: 10.4018/IJISP.315819 *Corresponding Author

configurability. The aspects to avert cyber-attacks are devised by specified authors (Chhabra et al., 2020). A major IoT model accumulates large quantity of data known as big data and it transmits to layer that performs processing. The big data are devised with three features, such as volume, variety and velocity (Srinivasan et al., 2012). The big data is growing each year and thus the rebellion in the technology and scientific face influenced the size of data to maximize the lucrative tasks (Triguero et al., 2016 ; Venugopal et al., 2021). The database of big data is complex to accumulate, split, sort, envisage and examine the contemporary techniques (Terzi et al., 2015 ; Suthaharan, 2014 ; Venugopal et al., 2021).

Classically, the majority of data contained in big data represents streaming data, because of the connections, capacity, and events of the data modeling, which progress through the internet. The data are produced considering the time instance (Zhang et al., 2012 ; Venugopal et al., 2021). Cybercrime represents a crime through computer in which the computers are utilized for prohibited tasks, such as child pornography, theft, fraudulent behavior, intellectual possessions. The Cybercrime is progressively growing in internet technologies because of the computer operations, like commerce, entertainment and government. The server can conceal its data by foraging sender address, which are transmitted through unidentified server or channel. The detection of cybercrime is a basic domain in the retrieval of information, processing language and machine learning (Venugopal et al., 2021). Cybercrime is digital crime caused by considering network as weapon. The multiple cybercrime domains are extended from uncomplicated credential risks to geopolitical crime in recent days (Guarino, 2013). The report of crime survey reveals that 49% of global CEOs pose issues over the emerging network and figures out way to avert its institutions from risks (Meidan et al., 2017). The cybercrime requires coherent and logically effective technique for managing the crime space (Fahdi et al., 2013). Here, the cyber-attacks on IoT devices tend to be emerging. Some of the IoT attacks pose a hit in IoT platform in several years due to attacks, like Mirai botnet and Brickerbot (Chhabra et al., 2020).

The major problem in forensic relies in three classes, named legal, technical and resource issues. Amongst them, the technical issues provide a huge class of real-time live examination of anti-forensics data. The resource issues involve processing time and volume to attain and evaluate probable evidence item. The legal factors or issues include deficiency of legislation principles, simulation, reconstruction and other admissible problems (Fahdi et al., 2013). Generally, one requires meeting critical problems ranges to search for proving the evidence (Chhabra et al., 2020). The deep model is utilized for designing cyber security solutions and it has gained huge focus from both industry and academia. The DL method has huge ability to generate improved outcomes from big data of industrial models (Aljawarneha et al., 2018). However, the development of feasible and effectual attack detection methods for IoT is a major issue (Huma et al., 2021). Several machine learning models are utilized for performing analysis of big data and it includes several classifier, like Naive Bayes (NB), support vector machine (SVM), and k-nearest neighbors (KNN). The images and text are utilized in analyzing the big data whereas the cyber assessment contains elastic learning and flexible techniques (Wang and Jones 2021; Liu et al., 2013 ; Venugopal et al., 2021).

The purpose is to devise novel deep technique using MapReduce for cyber attack discovery. The inclusion of deep model helps to offer more accuracy and fast processing. It aimed at devising a new malware detection model based on DNFN for enabling the detection of attacks in IoT. The model performed routing amidst IoT devices to transmit data. The routing is done using FGSA for sending the accumulated data towards BS. The DNFN is trained with MSSO for detecting the malware wherein the MSSO is obtained by combining Mayfly Algorithm (MA) and Shuffled Shepherd Optimization Algorithm (SSOA). The proposed model was capable to discover and classify the cyber-attacks of IoT networks.

The major contributions involves

- **MSSO-based DNFN for discovering cybercrime in IoT with big data**. The proposed MSSO-based DNFN is adapted for detecting cybercrime in IoT platform using big data. Here, the DNFN