

The IOT-Machine Learning Security Algorithm for Detecting the Intruders Gaining an Unauthorised Access to Government Protected Areas

J.K Adedeji¹ and E.A Adenagbe²

¹ Adekunle Ajasin University

Received: 9 December 2017 Accepted: 31 December 2017 Published: 15 January 2018

Abstract

The essentiality in the protection of the government restricted areas using the technology of IOT (Internet of Things) has been observed in this research, with the sole aim of providing certain measures to curbing the activities of the terrorists creating dirty scenario within the environment. The neural network employed four input neurons which are the Sensors used as IP address, while the government authorized areas are the clients who receive messages from the IP neurons, there are two separate hidden layers of orders seven each as the processors preceding the output which is the threshold value that has been determined through the sigmoid activation function. The research adopted the deep learning machine language and internet base IP with python socket command lines to address the problem of detecting unauthorized access in the government restricted areas. The unsupervised neural network algorithm used is of configuration 5-7-7-4, which was coded in python functional programming language and trained with the back propagation algorithm with 300 epoch runs to ensure that errors are maintained at about 5

Index terms— IOT, neural network, algorithm, unsupervised learning.

1 I. Introduction

HE security of our government protected areas within the government offices and environments is the concerns of all the stakeholders. The only way out is full security surveillance which is based on internet of things to watch over the government offices and raise proper alert when there's intruders invading the government areas. The research intends to design an intelligent internet based system, which is capable of detecting the activities of the intruders at the odd hours and make an urgent reports to curb the unauthorized access and monitor the footpaths of the intruders.

In some previous studies, involving the use of internet of things (IOT) and designing of algorithm; Serge Thomas et.al used an unsupervised learning algorithm called K-pattern clustering algorithm of Artificial Neural network and came out with certain evidences that IOT can be used in connection with sensors to provide adequate work place environment [3], [7]. He said that users' daily activities can generate patterns which play an important role in the smart environment. This assisted in receiving prompt alert to detect anomalies in the users' environment [1], [3]. In a similar work by Moeen et.al, IOT was used to monitor the health based on the cloud-based processing. The researchers considered the applications of the remote health monitoring systems for long term recording, management and came up with realizations that this technology can be used as a decision support system by the medical personnel [2], [4].

The IOT technology was used in data analysis which involves the combination of embedded systems, comprising wired, wireless communications, Sensors and actuator devices. The researchers said that IOT requires data to represent better services to users for performance and intelligence [5], [3]. In this manner, the IOT should be

able to access raw data from different sources over the network and analyse these information. This research will try to focus on collecting raw data from different Sensors such as; the actuator sensors as a signal generator to map the footprints of the intruders received from the GPS system, and transforming these for prompt reports, Laser Sensor, ground motion Sensor and sound recognition Sensor.

The system is designed using the coordinates systems of the GPS readings, there's a set boundary for non-inhabitants entering into the government's protected areas of the governor's offices. If an unauthorized access is noticed within these regions, the machine learning system which is also internet connected gives an alert which is viewed through the internet and face recognition cameras within the government's protected regions. The hardware and Engineering requirements is that the system is designed using the pressure or actuator sensor (intruders steps is on the forbidden or authorized regions to actuate the cameras), Laser Sensor, ground motion Sensor, and the sound detection T

2 II. Model Conceptionalisation

Author: Adekunle Ajasin University. e-mail: adedekijunle2@gmail.com Table ?? : Code selection process

3 IV. The Neural Architecture

The neural Algorithm used assumes an unsupervised configuration of order 5-7-7-4 that is, a neural network that has a memory that influences future predictions, as whether it should raise an alert for intruders' case or not. The four input neurons are the sensors, while the fifth neuron is bias; the algorithm has seven processors in the two separate hidden layers preceding the output which represents the messages sent from each neuron to get an alert from the internet connected sensors with different IP address for message dissemination. The algorithm is coded using python computer language for easier real time data processing and timely information on the security state of the government restricted areas. Sensor which gives an indication whether there's an abnormalities in the environment. These sensors are used as the input neurons to carry out information on the states of the regions as per forbidden or an access, in this regards the followings sensors are used; Pressure or Actuator: this will sense the various weights of the different people entering into the government's protected areas and detects whether it is within the forbidden or authorised regions and send a message through IP camera attached to the sensor for a prompt action and response from the government's security agent. The second neuron is the ground motion sensor; this is used to detect any un-allowed or strange motion in the forbidden regions of the protected regions in other to issue a response "intruders" for appropriate action.

The third sensor used as input neuron is the sound detection/ recognition sensor which detects the unwanted sound like whistling, shouting, and any kind of noise in the environment that is unpleasant for proper action to taken by the security agent. The forth neuron as input is the Laser light sensor, which senses any kind of search lights, motor pointer light, touch light for a proper action to be taken. A bias neuron is also attached to all the neurons at all the stages of the processing by the algorithm, the architecture of the system and configuration is an unsupervised neural network of four layers.

4 III. the neuron-computing approach

The neuron access or forbidden equation can be expressed as; for the IP input neuron 1, for the IP neuron 2, for the IP neuron 3, for the IP neuron 4. The deep learning Algorithm will assign the weights according the predetermined values and initial conditions. The values; are the various divisions in IP neurons as; being high, medium and low to classify the neurons into the deep learning algorithm for proper training and error corrections. The various value supplied into the algorithm can be viewed from the table below which have been converted into appropriate digit for the machine to learn. The Neural network model using the XOR data is repeatedly presented to the neural network, which is the function of the weights. The network maintains the deep learning intelligently enough to carry out the roles as an automatic machine that relates appropriate messages to the IP neurons in charge of the duty. At each presentation, the error between the network inputs, the hidden layers and the desired output were calculated, which is the threshold energy value when it has been activated through the sigmoid function. The computed values are then fed back to the neural network for proper adjustments. These sequences of events were done repeated until an acceptable error has been reached, when the network no longer appears to be learning, and the final output computed. The network ensures that the errors from the IP addresses are adequately feedback for automatic responses.

5 Locations and coding sheet for the raw data

6 V. Results and Discussions

The neurons are regarded as the IP addresses while the government restricted areas to be protected is regarded as the clients, the neurons got the signals and immediately transmit the message through the internet protocol address, which is immediately related to the monitoring devices mounted within the closed circuit system. The deep learning algorithm ensures that there's no delay in response to the signals sent by any of the neurons which are the IP addresses. The figure 3 actually showed a particular case which were simulated from different neurons, these are transformed by geodesic software which mapped the forbidden and the authorised regions within the

government areas. Those regions mapped by the intelligent neurons with red pigments are forbidden regions where the intruders can likely take and the neurons through the sensors mapped the footpaths of the intruders for a message of insecurity to be alerted. These areas have been given the tolerance values of noise signals in terms of Decibels strength for the sensors that measures noise/sound signals in those areas, also the Laser light sensor has been restricted to certain allowable values on the amount of light intensity that can be absorbed in the environment, any value above the threshold set by neurons means the deep learning algorithm will quickly initiate, the Laser sensor IP to relay a message of insecurity signal for the appropriate measures to be taken. In general any abnormality sensed in the environment by the IP neurons are quickly and timely related by the deep learning algorithm for proper action to be taken. The regions mapped by the intelligent neurons with pink pigments are the save areas where the inhabitants of the government premises are allowed to tread without any information been related by the neurons as long as no messages are being sent by the neurons. As can be shown in the neural architecture in figure2, it is expected that any of the four neurons can send a message through the IP attached to them, but in actual sense, the deep learning algorithm has been coded using an exclusive OR Boolean, to make the neurons more intelligent, which mean if any the IP is active then we can get an insecurity alert for an action to be taken by the security agents which monitor them on internet cameras based on the coordinates in the GPS.

VI. Conclusion

The research established that the technology of IOT and pattern recognition gave a better idea of getting vital information in real time and as accurate as possible. The IP Sensors also provides another means of getting a firsthand online message that can assist in reducing the level of crimes involving terrorism in our environments, with a little drawback. The research discovered that it is not only useful to the intending stakeholders, but it can be seen by the public all over the world who are using the internet as at the time of any crime and a good information to prevent other locations around the globe of being invaded by intruders.

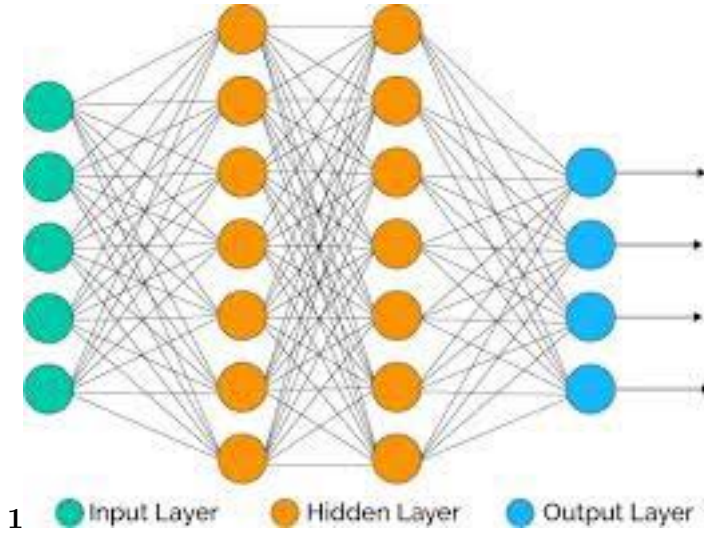


Figure 1: Figure 1 :

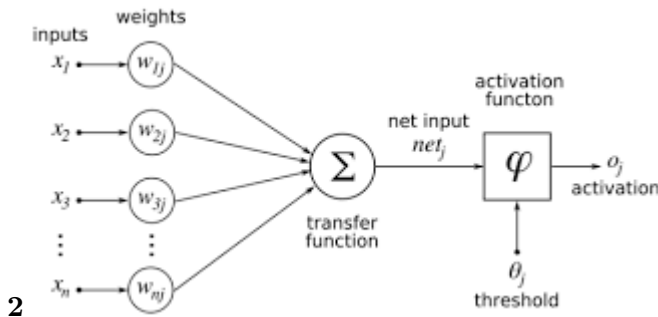


Figure 2: Figure 2 :

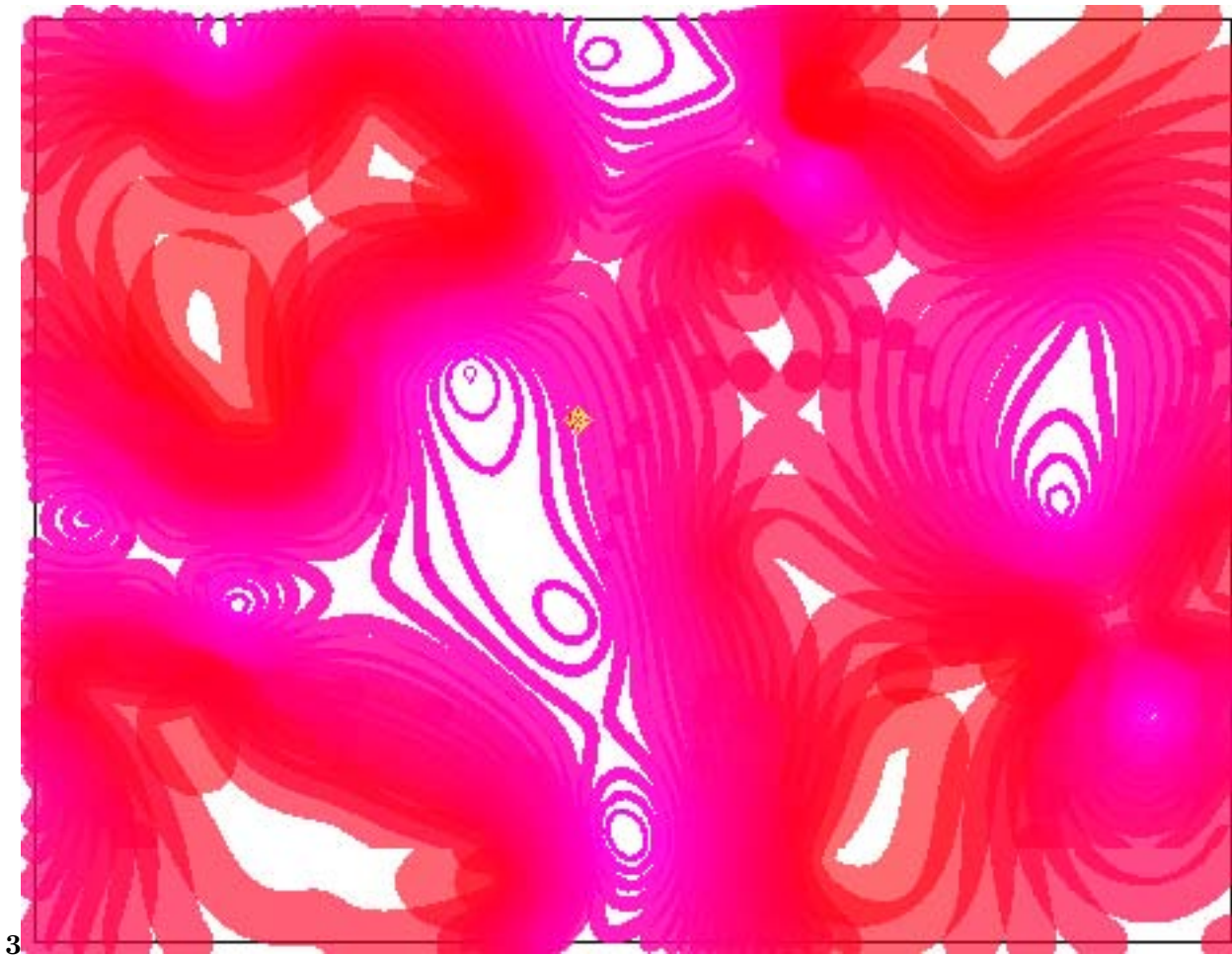


Figure 3: Figure 3 :

Year													
2018													
A		B		C		D		E		F			
21 00001		30	01001 15 00011		35		01001		20	01001		1	
22 00001		31	00011 16 00011		36		00101		7	00001		2	
23 00001		32	00001 17 10001		38		00001		10	01001		4	
24 00001		33	00011 26 01011		39		00001		5	01001		6	
25 01001		34	00011 43 01001		40		00011		9	01001		42	
												00101	
27 00011		3	00001 45 00011		41		00001		8	00001		44	
												01011	
F	28 00001	29	11	00001 47 00001 01001 37 01001		48	19	01001 00001		13	01001	18	
	00001		12							14	11001	00001	
											46		
											01001		
The Neural Algorithm of Back propagation													
Feedback Errors													

¹© 2018 Global Journal

²The IOT-Machine Learning Security Algorithm for Detecting the Intruders Gaining an Unauthorised Access to GovernmentProtected Areas

[Cecchinell et al. ()] ‘An architecture to support the collection of big data in the internet of things’. C Cecchinell , M Jimenez , S Mosser , M . *2014 IEEE World Congress on Services*, 2014. IEEE. p. .

[Hassanalieragh et al. ()] Moeen Hassanalieragh , Alex Page , Tolga Soyat , Gaurav Sharma , Mehmet Aktas , Gonzalo Mateos Burak Kantarci , Silvana Andreescu . *Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-based Processing: Opportunities and Challenges*, 2015. p. 296.

[Bui and Zorzi ()] ‘Health care applications: A solution based on the internet of things’. N Bui , M Zorzi . *Proc. of the 4th Int. Symposium on Applied Sciences in Biomed. and Com. Tech., ser. ISABEL ’11*, (of the 4th Int. Symposium on Applied Sciences in Biomed. and Com. Tech., ser. ISABEL ’11New York, NY, USA) 2011. ACM. 131 p. 5.

[Saeid et al. ()] ‘Machine learning for internet of things data analysis: a Survey’. Mohammad Saeid , Mohammadreza Mahdavinejad , Mohammadamin Rezvan , Barekataan Peyman , Adibi , Payam , Amit P Barnaghi , Sheth . *Digital Communications and Networks* 2013. 2018. 4 p. .

[Zhao et al. (2011)] ‘Medical application on internet of things’. W Zhao , C Wang , Y Nakahira . *IET Int. Conf. on Com. Tech. and Application (ICCTA 2011)*, Oct 2011. p. .

[Hu et al. (2013)] ‘On the application of the internet of things in the field of medical and health care’. F Hu , D Xie , S Shen . *IEEE Int. Conf. o and IEEE Cyber, Physical and Social Computing Green Computing and Communications (GreenCom), (iThings/ CPSCoM)*, Aug 2013. p. .

[Atzori et al. ()] ‘The internet of things: a survey’. L Atzori , A Iera , G Morabito . *Comput. Netw* 2010. 54 (15) p. .