A Study of Soft Computing Based IoT Device Security System

Santhosh, K. Thinakaran

Abstract: ***The ubiquitous computing environment has increased interest in IoT technology. As IoT has open characteristics in the fields of industry, increased accessibility has raised the possibility of threats. As the IoT network was small on scale, there was risk of security. IoT development brought the network environment by combining networks, therefore risk of security attack compared to small network. The response time while operating IoT devices to detect intrusion through hacking, the artificial neural network responses using mobile devices. This process help to deal with hacking. By detecting virus in real time, this process help to prevent intrusion. As IoT security risks, we suggested an intrusion detection system using artificial neural network model in this study. The system which is developed in this can be adjusted to fit situations of IoT by facilitating modification of critical values. The research which detects anomaly through the response to be used for information security system which utilize IoT .***

Keywords: Anomaly, Intrusion Detection, Artificial Neural Network, Information System, IoT, Security System

I. INTRODUCTION

The ubiquitous computing environment has increased interest in IoT technology. IoT is the devices form network and exchange information. By making the network between objects and people possible, IoT introduced the environment that each object can freely exchange information with each other [1], and it increased flexibility and openness in various fields. The external accessibility has the possibility of external threats. Together with the weakness of the source technology itself, new vulnerability may arise.By examining the response and implementation time while operating IoT devices, the artificial neural network may learn different responses using many other mobile devices to detect intrusion through virus or hacking.

II. INTERNET OF THINGS

Internet of Things is a global infrastructure which interconnects intelligent objects and helps communication between objects and people combined with context-awareness based knowledge [2].

As shown on Figure 1, IoT concepts are adopted on existing network such as M2M and Wireless Sensor Network that devices form the network and exchange information.

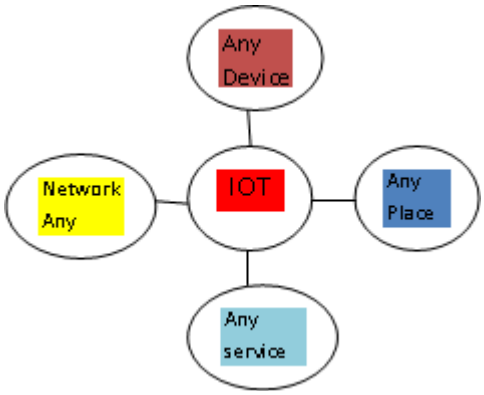

Figure 1: IoT Description

IoT can connect physical and virtual things and communication between objects to exchange , the IoT platform has now more flexible and open characteristics. As the recognition that flexibility of IoT service quality throughout the industry, focusing on connectivity and data sharing, studies are now in progress combining IoT with fields of service such as home appliances , buildings, transportation and health care.

2.2 Artificial Neural Network

Artificial neural consists of processing units, and it has resilience and learnability [3, 4]. The processing units consisting artificial neural network are constructed by connection weights between each other [5]. Figure 2 shows the structure of an artificial neural network.

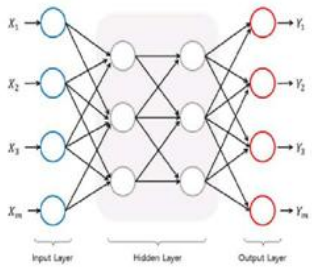

Figure 2: Structure of Artificial Neural Network

Compared to existing models or inductive learning method models, artificial neural network models have relatively high predictability Applying probit analysis, ID3 and artificial neural network on each experiment, artificial neural network have the predictability. Probit analysis did not show difference in predictability[7]. Artificial neural network is the one of the accurate models which predict social, economic, engineering, foreign exchange and stock issues.[8]. Artificial neural network models have possibility to solve issues which are hard to deal with computers, many related studies are on rapid progress[9].

Revised Manuscript Received on September 05, 2020.

Santhosh, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Tamil Nadu, India.

K. Thinakaran, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Tamil Nadu, India.

Back-propogation neural network is known as the generalized delta rule[10,11]. It is one of the widely used to train the neural network[12]. Back-propogation neural network consists of process units which are known as neurons, also known as neurodes. Neurons of each layer are completely linked to each other by connection stability called weights which save network information[13]. Back-propogation neural network is linked by process units . The process units have a learning function which learns input data and a transfer function [14]. Multi-layer Perceptron has been used in application based on the mathematical proof that a have number of middle layer nodes can approximate a function. Especially, MLP is also often used in pattern issues [15]. MLP makes learning of a training set possible and it can be used as a tool to solve complicated classification issues of pattern recognition [16]. The learning process of the artificial neural network is as shown as below

1) According to the target, determine the cost function $(R(\theta))$.
2) After randomly entering the initial weight, calculate the fitted value $(\hat{R}(X))$.
3) Partially differentiate the cost function on each weight $(\beta_{new}, \alpha_{ml})$.
4) By adding or subtracting r^{th} weight (learning rate (η) xpartial differentiation value), calculate $r+1^{th}$ weight.
5) Repeat from step 2 to step 4 until the error rate is within the margin of the error [17].

In the artificial network theory, backpropogation is adjusting the network to reflect the data connected by processing units of input,hidden and output layers. backpropogation, aritificial neurons learn the data entered in processing units and transfer the activation data interconnected to each other transfer function. We used sigmoid mathmetical function having a characteristic of "S"-shaped curve which is generally used in the artificial neural network. Theconnection weights are decided by backpropogation. Backpropogation is used in application of artificial neural network [18]. Figure 3 shows the curve function in this study.

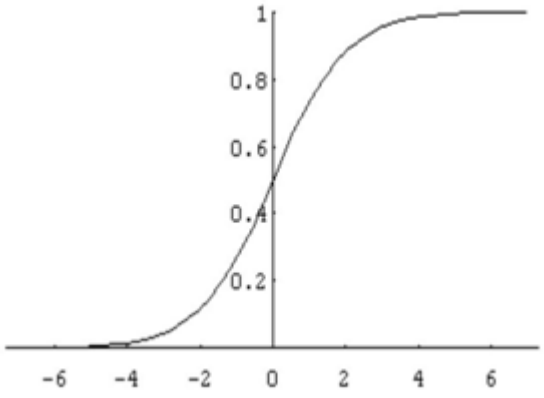

Figure 3: Sigmoid Function

2.3 Information Security System

Detecting network intrusion accurately in real is always a difficult goal for dministrators and information security researchers [19]. Security attack technology has been developed than information technology. However, as shown in the graph in Figure 4, it is difficult to solve the problem . Due to the development of Internet, the need to establish protection system to deal with Internet security and threats is increasing . However, this issue is not easy to solve. [20].It is not surprising that the enterprises are investing money in information security [21].

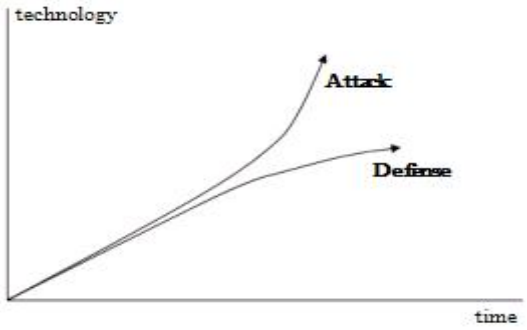

Figure 4: The difference between various attack

Based on security attack patterns, the method to detect network intrusion is to monitor security attacks . An intrusion detection system can be classified into host-based intrusion detection system which monitors the system and detects traffic and network intrusion detection system (NIDS) which monitors the whole network activity [22].However, the weak point of IDS is that it cannot detect unknown intrusion. New pattern of attack is found, the system to be updated. As the complexity of the network is increasing, the type of intrusion is also surging. It is to be harder to update the system . An intrusion detection system identifies system intrusion by monitoring network anomaly[23]. An intrusion detection system is considerably noted for a mechanism that protects the network system by keeping confidentiality, integrity and availability of the network system. many researchers made considerable efforts, there are still weaknesses with an intrusion detection system such as false positive and false negative[24]. Intrusion detection system wrongly interprets traffic against attack, it is called FP [22]. When an intrusion detection attacking the system as normal traffic, it is called FN [25]. These critical weaknesses of the intrusion detection system, it is to lower FP and FN to increase the accuracy of detection.

2.4 IoT Security System

IoT can be interpreted as a forms and integrated technologies such as network, user centered applied service and web service. The range of IoT security technology can be regarded as extensive and complicated [26].

As the existing IoT network was small in scale, there was less risk of security attack. Continuous IoT development brought a network environment integrating various network and it also raised security risk compared[27]. The security issue is more important. Wifi and ZigBee are most widely used as IoT network technology. However, each technology has its own weakness: It is difficult to apply high-level encryption technology on ZigBee. Wifi has weakness in security against the attack of information leakage and modification. Recently, development of application level protocols such as CoAP and MQTT effectively deals with various linking functions between publish/subscribe sensing devices and services. In the future, it is expected to be widely used as IoT protocol [28].

III. SYSTEM IMPLEMANTATION

Security is being used in IT industy and will be used extensively in number of fields. As ultra-light are essential in commercial IoT environment, extensive prevention system does not match with IoT enviroment, which makes it difficult to measure . Use the factor 'time', which is impossible to fabricate and tried to find ways for detection and prevention against virus . The performed learning of the response and implementation data using Neural Networkl of MATLAB. Based on learning and results, we suggest IoT information security based on artificial neural network. Figure 5 shows the flow chart for this.

Figure 5: Flow Chart for research

We used Arduino Uno as IoT device for implementation and installed Wifi Shield to connect to the Internet. As shown on Figure 5, using Arduino Connection , the installed 7-segment on breadboard and connected with Arduino Uno for device work.

Table 1: List of IoT Devices

List of product	Quantity
Arduino Uno R3 Board	1
Arduino Wifi Shield R3	1
Breadboard Standard Half+	1
Register 470Ohm	2
7-segment 1-digit FND	1
Breadboard Jumper Wire	12
Tact Switch 12x12 mm	1
USB Cable B-Type	1

The wifi shield to connect Arduino Uno to the Internet . Arduino circuit we set 7-segment on breadboard and equipment on Table 1 and connected it to Arduino Uno on Figure 6.

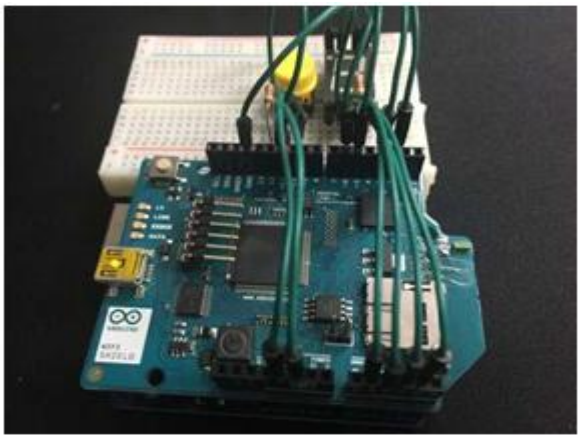

Figure 6: Device of Arduino

By obtaining device information from wireless router connected to Arduino Uno The increased the access and control to IoT devices from 1 device to 9 devices. Using control of 9 devices and 7-segment, tried number counting from 0 to 8.To control Arduino Uno which was used for this study, we used ARDUINO program through the Arduino. website. This program enables connection with Arduino Uno and programming design. ARDUINO 1.8.1 version was used for this study. As shown on the t diagram on Figure 1, we set 2, 5, 6, A1, A3, A4 as output pin of 7-segment and set wifi server as 81. Sset serial as 9.6K, set password of wireless router and web server by connecting to wifi. Generating JavaScript by client, we set the 7-segment to count using a herf. Furthermore, through the generator of JavaScript, we measured the time to Milliseconds using Date Object. Through this process, by accessing to Arduino web server, we created a method for number counting of 7-segment and extraction of response and implementation time. Figure 7 shows the connection to Arduino web server.
As Arduino Uno has concurrency control, it processes according to the input and control. As the number of devices controlling Arduino Uno increases, the response time also increases in turn.
We have 9 types of data using 1 device to 9 devices, measured 199 times each type and extracted 1,999 response time in total. Here used the method to measure and detect to find out implementation time and reduced 2,000 data in total response time. we extracted 3,000 data and 1,000 response time data and 1,000 implementation time data. Figure 8 depict the process of response time.

IV. EXPERIMENTAL CLASSIFICATION

In this study, we built the artificial neural network using Toolbox of MATLAB R2017a. The structure of neural network in this study used ten factors; input of ten nodes from device to ten devices. For extracting data of the artificial neural network, Here used ten nodes as factors and generated data 200 time with response and implementation time 2000 data each time and 4000 data .In the learning data, Here sorted 200 data in one pair and produced 10 pairs of data according to response time and 10 pairs of data according to implementation time.
Table 2 and Table 3 describe extracted data for response time.

Table 2: Table for Response Time

1	2	3	4	5	6	7	8	9	10
0.936	6.312	12.64	19.146	26.224	31.74	37.987	44.325	46.256	57.293
1.276	7.109	12.826	19.17	25.422	31.739	37.954	44.818	50.557	57.115
1.455	6.278	12.831	18.85	25.402	31.644	38.072	44.34	47.076	52.637
0.875	6.292	12.623	19.06	25.429	31.728	37.994	44.463	46.216	57.042
1.416	6.291	12.722	18.996	25.423	31.643	39.646	44.329	51.164	57.036
1.414	6.529	12.829	19.63	25.541	31.609	37.624	44.456	46.102	56.625
1.527	6.178	12.722	19.159	25.227	31.928	38.084	44.489	46.193	57.253
0.94	6.418	12.718	18.751	25.794	31.642	37.99	44.535	46.235	56.433
1.358	6.412	12.724	19.107	25.437	31.738	37.989	43.639	50.59	57.433
1.39	6.42	12.724	19.021	25.906	37.873	37.997	44.528	46.146	57.44

Table 3: Part of Time Data Table

1	2	3	4	5	6	7	8	9	10
0.00284	0.0058	0.0088	0.0116	0.01468	0.01732	0.02036	0.02344	0.02628	0.029
0.00296	0.0058	0.00868	0.0114	0.01444	0.0174	0.02024	0.02364	0.02612	0.02932

0.00 296	0.00 592	0.00 872	0.01 164	0.01 456	0.01 708	0.02 008	0.02 324	0.02 616	0.02 916
0.00 284	0.00 592	0.00 864	0.01 152	0.01 492	0.01 744	0.02 024	0.02 352	0.02 628	0.02 88
0.00 284	0.00 592	0.00 848	0.01 16	0.01 456	0.01 756	0.02 004	0.02 308	0.02 612	0.02 872
0.00 288	0.00 592	0.00 864	0.01 16	0.01 472	0.01 756	0.02 052	0.02 308	0.02 58	0.02 928
0.00	0.00	0.00	0.01	0.01	0.01	0.02	0.02	0.02	0.02

Table 4: Learning

Training		Testing		Validation	
MSE	**Time**	**MSE**	**Time**	**MSE**	**Time**
0.112	15	**0.99**	**31**	0.96	14
0.12	31	0.5	109	0.168	18
0.12	47	0.44	111	0.133	24
0.12	62	0.35	114	0.106	30
0.11	78	0.31	116	0.087	34
0.02	82	0.27	119	0.081	39
0.03	94	0.19	122	0.078	44
		0.1	125		

Figure 12 details the process to find the artificial neural network through the program using Tool of MATLAB and it shows convergence of output errors. the experiment of learning and test data according to response time are as follows; 1Device 0.8265, 2Devices 1.1487, 3Devices 1.16684, 4Devices 2.4455, 5Devices 3.5776, 6Devices 4.7788, 7Devices .0764, 8Devices 7.2208, 9Devices7.7096, 10Devices 8.434. The experiment of learning and test data according to implementation time are as follows; 1Device 0.33986, 2Devices 0.87542, 3Devices 2.0052, 4Dvices 3.2757, 5Devices 4.0609, 6Devices 4.7048, 7Devices 6.1006, 8Devices 7.4577, 9Devices 8.2584, 10Devices 8.6097. Figure 12 shows learning results based on output layers set from 0 (the best) to 9 (the poorest), not on response and implementation time. By setting values of response and implementation time rate, the anomaly of IoT can be detected. Several limitations of IoT such as low specification power, this study suggested learning response and implementation time of IoT devices and tests based on the learning results. Based on the learning results, we used test data in order to verify and utilize results. This study implemented the standard of critical values from 0 to 9. Based on the values, it is expected that setting values based on devices, situations and fields will help to flexibly detect various anomaly when IoT is in use.

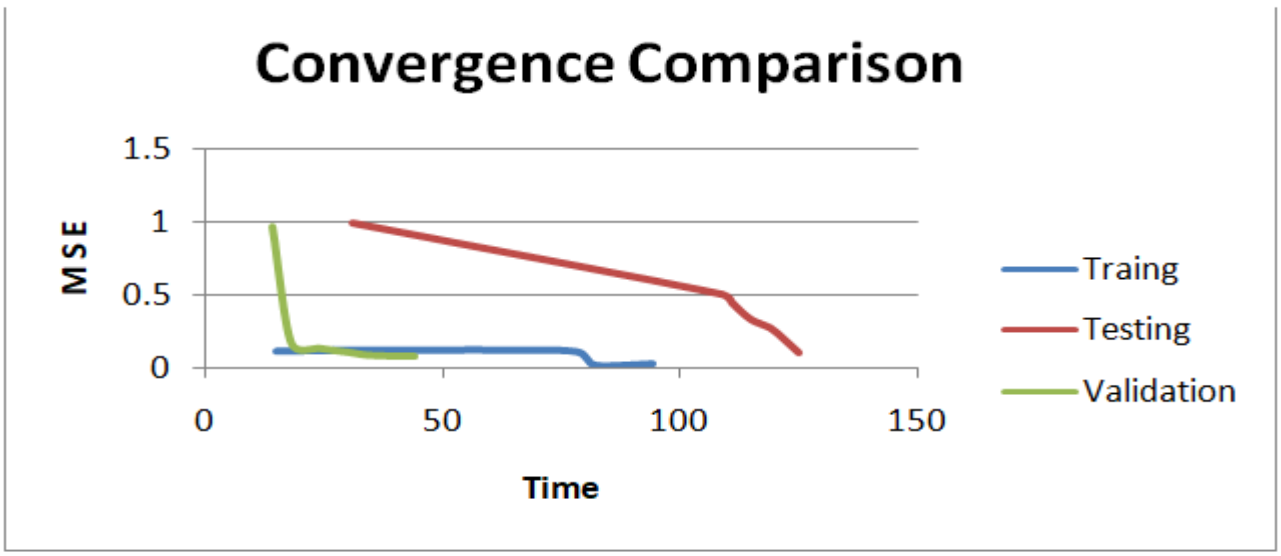

Figure: 8 Convergence Comparisons

V. CONCLUSION

Here suggested to detect anomaly of IoT system by artificial neural network. IT industry uses IoT in the products. IoT is widely used in service sectors. Malicious users access IoT system using deceptive ways to steal private information, which may cause problems on IoT system. IoT system communicates with devices, there be malfunction and non function compared to a single device. the combination of security technology and models with IoT security is insufficient. In this study, research based on data using artificial neural network . If we use inputs, we could have fixed learning . If we use unexpected inputs , we need to study unexpected situation and. The security of IoT components in physical environment also needs to be considered. Secure authentication of physical access is required to prevent potential physical damages. It is necessary to identify threats and find solutions in terms of security.

REFRENCES

1. Bong-Im Jang, Chang-su Kim, “A Study on the Security Technology for the Internet of Things”, Journal of Security Engineering, Vol. 11, No. 5, October 2014, pp. 429-438.
2. Chul-Sik Pyo, Ho-Yong Kang, Nae-Su Kim, Hyo-Chan Bang, “IoT (M2M) technology trends and development prospects”, The Journal of The Korean Institute of Communication Sciences, Vol. 30, No. 8, July 2013, pp. 3-10.
3. M Zeidenberg, “Neural Models in Artificial Intelligence”, llis Horwood, 1990.
4. Richard P. Lippmann, “An introduction to computing with neural nets”, IEEE ASSP Magazine, Vol. 4, Issue 2, April 1987, pp. 4-22.
5. Russell, I.F., “Neural Networks”, The UMAP Journal Vol. 14, No. 75, 1993, pp. 75-88.
6. Kun Chang Lee, "A Comparative Study on the Bankruptcy Prediction Power of Statistical Model and AI Models: MDA, Inductive Learning, Neural Network", Journal of the Korean Operations Research and Management Science Society, Vol. 18, Issue 2, 1993, pp 57-81.
7. Liang. T.P, J.S. Chandler, H. Ingoo, J.Roan, "An Empirical Investigation of Some Data Effects on the Classification Accuacy of Probit, ID3 and Neural Networks," Contemporary Accounting Research, Vol. 9, No. 1, Fall 1992, pp. 306-328.
8. Mehdi Khashei, Mehdi Bijari, 2010, "An artificial neural network (p, d, q) model for timeseries forecasting," Expert Systems with Applications, Vol. 37, Issue 1, January 2010, pp. 479-489.
9. K. Y. Lee, Y. T. Cha, J. H. Park, 1992,
10. "SHORT-TERM LOAD FORECASTING USING AN ARTIFICIAL NEURAL NETWORK," Transactions on Power System, Vol. 7, No. 1, February 1992, pp 124-132.
11. D. E. Rumelhart, G.E. Hinton, J. L. McClelland, “Parallel Distributed Processing”, The PDP Perspective, Vol. 2, 1987, pp. 45-76.
12. 11] J. L. McClelland G.E. Hinton, D. E. Rumelhart, “Parallel Distributed Processing”, The PDP Perspective, Vol. 1, 1987, pp. 3-44.
13. Philip D. Heermann, Nahid Khazenie, “Classification of Multispectral Remote Sensing Data Using a Back-Propagation Neural Network”, IEEE TRANSACTIONS ON GEOSCIENCE AND REMOTE SENSING, Vol. 30, No. 1, January 1992, pp. 81-88.
14. Iebeling Kaastra, Milton Boyd, 1996, “Designing a neural network for forecasting financial and economic time series”, Neurocomputing, Vol. 10, No. 3, April 1996, pp. 215-236.
15. Dae-Gyun Choi, 2016, “Anomaly detection algorithm of IoT system using an artificial
16. neural netwrok theory,” Hanyang University Thesis for the Master Science, August 2016, pp.1-34.
17. Y. Ito, “Approximation of continuous functions on by Rd linear combinations of shifted
18. rotations of a sigmoid function with and without scaling”, Neural Networks, Vol. 5, No. 1, 1992,pp. 105-115.
19. G.E. Hinton, J.L. Mcclelland, DE Rumelhart, “Parallel Distributed Processing, Explorations in the Microstructure of Cognition: Foundations”, MIT Press, vol. 5, 1992, pp.45-76.
20. Trevor Hastie, Robert Tibshirani, Jerome Friedman, The Elements of Statistical Learning, Springer publisher, 2017
21. Kun Chang Lee, “Synergism of Knowledge-Based Decision Support Systems and Neural Networks to Design an Intelligent Strategic Planning System,” The Journal of MIS Research, Vol. 2, No. 1, June, 1992, pp 35-56.
22. Mukherjee, B., Heberlein, L.T., Levitt, K.N., “Network Intrusion Detection”, IEEE Network, Vol. 8, Issue 3, May-June 1994, pp. 26-41
23. Lim Chae-Ho, “Effective information protection awareness improvement plan”, Journal of the Korea Institute of Information Security and Cryptology, Vol. 16, April 2006, pp. 30-36.
24. Lawrence A. Gordon, Martin P. Loeb, “The Economics of Information Security Investment”, ACM Transactions on Information and System Security, Vol. 5, Issue 4, November 2002, pp. 438-457.
25. Jimmy Shum, Heidar A. Malki, “Network Intrusion Detection System Using Neural Networks”, Fourth International Conference on Natural Computation, October18-20 2008. PP. 242-246.
26. Huiqiang Wang, Xiaowu Liu, Jibao Lai, Ying Liang, 2007, “Network Security Situation Awareness Based on Heterogeneous Multi-Sensor Data Fusion and Neural Network”, Second International Multisymposium on Computer and Computational Sciences, August 13-15 2007, pp 352-359.
27. John Goodall, Wayne Lutters, Anita Komlodi, “The work of intrusion detection: rethinking the role of security analysts,” Proceeding of the Tenth Americas Conf. on Information System, December 2004, pp 1421-1427.
28. Seongrae Jo, Haengnam Sung, Byung-Hyuk Ahn, 2016, "A Comparative Study on the Performance of SVM and an Artificial Neural Network in Intrusion Detection," Journal of the Korea Academia-Industrial, Vol. 17, No. 2, February 29 2016, pp 703-711.
29. Wha-Jung Seo, Dong-Gun Lee, Jong-Suk Lee, and Ho-Won Kim, IoT Security Technology Trends, The Proceedings of the Korea Electromagnetic Engineering Society, Vol. 24, No. 3, July 2013, pp. 27-35.
30. Zhao, K., Ge, L., “A Survey on the Internet of Things Security”, International Conference on Computational Intelligence and Security, December 14-15 2013, pp. 663-667.

AUTHOR PROFILE

K. Thinakaran, received Ph.D degree in computer science from Anna University, Tamilnadu in 2017. He is currently working an Associate Professor in Computer Science Engineering,Saveetha School of Engineetring, Chennai India. His current research interests include Neural Network and DataMining.

Mr. Santhosh is doing his B.E degree in computer science in Saveetha School of Engineering, SIMATS, Chennai. He is currently working on the project based on IOT.