Trust Negotiation among IoT-based Objects in Critical Healthcare Environment

Raghu Ram Nallani Chakravartula, V. Naga Lakshmi

Abstract: ***In pervasive environment, the opportunity of unidentified objects involving in malevolent interactions increases due to the lack of centralized services. Traditional authentication and access control rules cannot be applied due to limitations of foot print of the objects used in Internet of Things. The proposed model presents authentication and authorization for an IoT-based ad-hoc objects using human notion of trust. The paper presents testing the proposed model with relevant use-cases in patient monitoring healthcare devices and presents the analysis results used in the critical care areas.***

Keywords: Authentication and Authorization, Internet of Things, Fuzzy logic, Objects.

I. INTRODUCTION

To achieve the best possible outcomes in the patient's health condition, monitoring of critical parameters is essential [1]. Monitoring may occur on an intermittent basis, such as having the blood pressure checked during an annual physical examination or in a continuous manner such as monitoring breathing when anesthetized during an operation [2]. Internet of Things plays pivotal role in patient diagnosis, monitoring and their treatment [3].

The goal of medical facility is to enhance the patient's state of being or at minimum ease their suffering. Internet of things helps by providing solutions, which generate detailed patient information and make it readily available over the Internet to right stakeholders, necessary to make rapid and accurate decisions by the panel of doctors to achieve the best patient outcomes [4].

Security and privacy aspects are considered as a crucial differentiator to embrace the Internet of Things in the healthcare domain [5][6]. The traditional computing environment is based on a client-server computing model; whereas most IoT-based devices are in ad-hoc. Thereby, availability of source and destination nodes and connectivity between the source server and destination client is a challenge.

Traditional systems would need human interaction to perform authentication and authorization like entering a password or by placing the finger as biometric information. IoT devices would expect minimal to no human intervention & most decisions would happen spontaneously [7][8]. The IoT-based services collect user sensitive data to offer anytime anywhere services. Privacy of user's data poses a significant risk compared to traditional computing model [9].

II. METHODOLOGY

The proposed framework performs trust negotiation among objects to make trust decisions which is dependent on the trust level with six identified factors hence the model is called "Hexagon Framework" [10,11,12]. The following are the six factors that affect and influence the trust negotiation process are Privacy, Peer recommendation, Reputation, Operational Risk, Role and Identity management, Operational Cost.

The input sub-system values of Operational Cost (OC), Reputation Value (RP), Peer Recommendations (PR), Operational Risk (OR), Role and Identity (RI), Privacy (TTV) are calculated by each individual sub-system by interacting with the knowledge base. OC, RP, PR, OR, RI, and TTV are the fuzzy sets for the corresponding Peer Recommendation, Role and Identity, Operational cost, Reputational value, Privacy, Operational Risk values as depicted in figure 1.

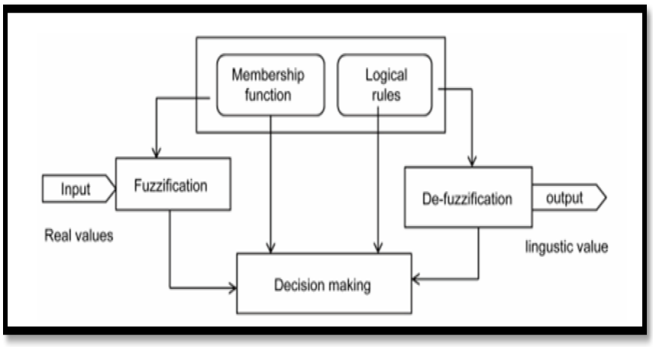

Figure 1 Trust Negotiation using Inference Engine

Normalized values are inferred with linguistic values derived from membership function as depicted in figure 2. Combination of overlapped trapezoidal and triangular membership functions are used. Linguistic values are mapped to real values by their respective ranges mentioned as defined in the membership function. The linguistic values are of OC, RP, PR, OR, RI, and TTV are provided as low, high, very high, very low, moderate, medium [13].

In the next step, evaluating each policy strength in combination of fuzzified values with respect to fuzzy rules. T-Norm represents the fuzzy combination operators, and they are defined as "and" and "or." Based on the policy strength determines the minimum and maximum values from the fuzzified sets. The "And" and "or" policy brings "Minimum" and "maximum" value [14].

Revised Manuscript Received on January 10, 2020.

Raghu Ram Nallani Chakravartula, Head of Information Security and Compliance in Mirra Healthcare, USA.

Prof. V. Naga Lakshmi, HOD, Department of computer science in GITAM (Deemed to be university), India.

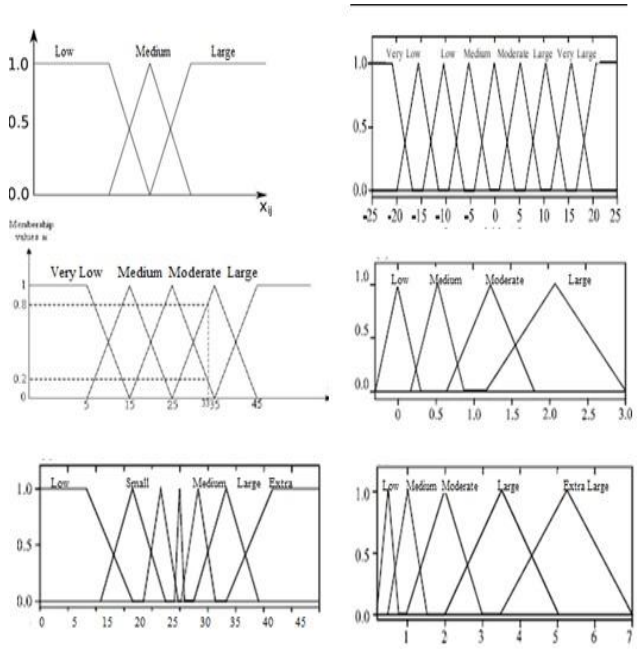

Figure 2. Membership functions for OR, PR, OC, RI, RP TTV

The trust negotiation of each corresponding sub-system is represented as follows

µOR(x)= T-norm [min x [µOR(i)]] for i=trust values 1,2,..5

Using equations (1-6); The final step in the process is defuzzification. Defuzzification provides linguistic output for each policy which in turn result in an accurate decision. Defuzzification is calculated by the mean of maxima. The output for action is singleton set expressed from the constructed policy.

PR = max (min (no of peers/ total peers, 1), 0)	(1)
OR = max (min (operations performed / total cost, 1), 0)	(2)
OC = max (min (cost involved/ total cost, 1), 0)	(3)
RI = max (min (parameters captured in context information / total context, 1), 0)	(4)
RP = max (min (value of reputation received/ total reputation, 1), 0)	(5)
TTV= max (min (level of privacy / total privacy value, 1), 0)	(6)

The largest output value is taken, and an average value of the output is obtained. The final output will be in between 0 and 1. value closer to 1 indicates the highest priority to perform the action. If OR is A, AND OC is B or TTV is C AND PR is D AND RP is E OR RI is F THEN TV where k is the result of the fuzzy policy inferred from the membership function. The fuzzy output defines the trust decision to be taken for that operation.

The fuzzy system uses six sub-systems to determine the decision making. Each sub-system provides a value between 0 and 1 as input parameters into the inference engine

III. TESTING OF THE HEXAGON FRAMEWORK

Hexagon framework allows the sensors of patient monitoring to take trust-based decisions without human intervention as depicted. forty-four unique use cases and scenarios have been identified to verify and validate the framework. Based on the nature of the use case, the scenarios are broadly classified into 2 groups – Clinical and Malicious. Clinical use cases are designed and developed to improve the diagnosis, assessment, and treatment of ailments in critical care areas in hospitals. All the use cases under this section are clinically validated by the qualified medical practitioner, and each scenario is represented as SC-#. Malicious use-cases and scenarios are designed to test the resilience of the system against cybersecurity attacks and all use-cases in this section are referred to as MA-#.

Scenario 1 (SC-1): Diabetes mellitus type 2
Sensors: Glucose sensor
Description: Trust negotiation among glucose sugar and time of the day service helps to determine blood glucose levels at a period of fasting, postprandial, random blood sugar to identify the potential diabetic mellitus in patients.
Scenario 2 (SC-2): thyrotoxicosis or Hypothyroid
Sensors: Sphygmomanometer, blood pressure, ECG, pulse oximeter
Description: Trust negotiation among sphygmomanometer, blood pressure, ECG and pulse oximeter and time of the service (night time) to identify thyroid levels of patients to determine Hypothyroid in myxedema.
Scenario 3 (SC-3): Evolving myocardial infarction
Sensors: ECG, blood pressure and pulse oximeter
Description: Trust negotiation among ECG, Blood pressure and pulse oximeter to detect and diagnose evolving
myocardial infarction.
Scenario 4 (SC-4): Hypertension
Sensors: blood pressure and pulse oximeter
Description: Trust negotiation between a blood pressure sensor and pulse oximeter to diagnose hypertension in patients
Scenario 5 (SC-5): Arthritis
Sensors: Weighting scale sensor and the patient's posture sensor
Description: Trust negotiation between weighting scale sensor and the patient's posture sensor allows diagnosing the Arthritis in patients.
Scenario 6 (SC-6): Chronic Bronchitis
Sensors: airflow sensor, blood pressure, and spirometer
Description: Trust negotiation among the airflow sensor, blood pressure, and spirometer sensor allows identifying patients suffering from Chronic Bronchitis.
Scenario 7 (SC-7): Coronary heart disease
Sensors: glucometer sensor, electrocardiogram, and weighing scale
Description: Trust negotiation among glucometer sensor, electrocardiogram, and weighing scale allows diagnosing patients suffering from coronary heart disease.
Scenario 8 (SC-8): Epilepsy
Sensors: electromyogram, pulse oximetry, glucometer sensors
Description: Trust negotiation among electromyogram, pulse oximetry, glucometer allows diagnosing patients suffering from epilepsy.

Scenario 9 (SC-9): Motor Neurone disease
Sensors: electromyogram, electrocardiogram, glucometer
Description: Trust negotiation among electromyogram, electrocardiogram, glucometer sensor, Galvanic Skin Response allows diagnosing patients suffering from motor neuron disease.
Scenario 10 (SC-10): Sclerosis
Sensors: electrocardiogram, electromyogram, galvanic skin Response
Description: Trust negotiation among electrocardiogram, electromyogram, Galvanic Skin response allows diagnosing a patient suffering from Sclerosis.
Scenario 11 (SC-11): Osteoporosis
Sensors: pulse oximetry and blood pressure
Description: Trust negotiation between pulse oximetry and blood pressure sensors allows diagnosing a patient suffering from Osteoporosis
Scenario 12 (SC-12): Paget disease
Sensors: electrocardiogram and human body temperature
Description: Trust negotiation between electrocardiogram and human body temperature sensors allows identifying patients suffering from Paget disease.
Scenario 13 (SC-13): Parkinson's disease
Sensors: electrocardiogram, glucometer sensor, galvanic skin response
Description: Trust negotiation among electrocardiogram, glucometer sensor, galvanic skin response allows identifying patients suffering from Parkinson's disease.
Scenario 14 (SC-14): Chronic kidney disease
Sensors: glucometer sensor, electrocardiogram, blood pressure
Description: Trust negotiation among glucometer sensor, electrocardiogram, blood pressure allows diagnosing patients suffering from Chronic kidney disease
Scenario 15 (SC-15): Deep Vein Thrombosis
Sensors: the patient's position and posture sensor, blood pressure, and glucometer sensor
Description: Trust negotiation among patient's position and posture sensor, blood pressure, and glucometer sensor allows diagnosing patients suffering from Deep Vein Thrombosis.
Scenario 16 (SC-16): Shingles
Sensors: pulse oximetry, electromyogram, and glucometer sensor
Description: Trust negotiation among pulse oximetry, electromyogram, and glucometer sensor allows diagnosing patients suffering from Shingles
Scenario 17 (SC-17): Cholesterol
Sensors: pulse oximetry, electromyogram, and glucometer
Description: Trust negotiation among weighing scale, patient's position and posture sensor, and blood pressure sensor allow diagnosing patients suffering from Cholesterol.
Scenario 18 (SC-18): Carcinoma lung diseases
Sensors: glucometer sensor, weighing scale, and airflow sensor
Description: Trust negotiation among glucometer sensor, weighing scale, and airflow sensor allow to diagnose patients suffering from Carcinoma lung diseases.
Scenario 19 (SC-19): Cirrhosis liver diseases
Sensors: pulse oximetry, weighing scale, and glucometer sensor
Description: Trust negotiation among pulse oximetry, weighing scale, and glucometer sensor allow to diagnose patients suffering from Cirrhosis liver diseases.

Scenario 1 (MA-1): Denial of service
Sensors: Any two sensors (Glucose sensor, Pulse oximeter)
Description: IoT devices being resource constrained; the goal of the denial of service attack is to make the service unavailable. Rogue glucose Sensor is trying to flood with malicious requests to pulse oximeter so it can drain the battery power.
Scenario 2 (MA-2): Distributed Denial of service
Sensors: Multiple sensors (Glucose, EMG, Temperature, Body position, Pulse oximeter
Description: The goal of distributed denial of service is like a denial of service attack except rather a single object trying to flood another object. In DDoS, multiple objects try to attack the targeted object by flooding repetitive traffic requests. Rogue glucose, snore sensor, temperature sensor, EMG Sensor, body position sensor flood repetitive request messages to pulse oximeter sensor to drain its battery and crash the application to make the service unavailable.
Scenario 3 (MA-3): Malicious input
Sensors: The goal of this attack is to send malicious input so should make the output unusable or in this case to breach the final trust decision
Description: Glucose sensor sending malicious peer recommendations to the
objects, to which the system never interacted to make the decision unusable.
Scenario 4 (MA-4): Disgruntled object
Sensors: Glucose and temperature sensors
Description: The goal of the attack is to send malicious traffic deliberately to change the trust decision in favor of the disgruntled object. The glucose sensor is sending peer recommendations in favor of a temperature sensor to arrive at biased trust decision in favor of temperature sensor.
Scenario 5 (MA-5): Compromised object
Sensors: Multiple sensors
Description: The goal of the attack is to send malicious traffic deliberately to breach the entire system and make it unusable. The glucose sensor is sending arbitrary and random trust values against other sensors to breach the trust negotiation process.
Scenario 6 (MA-6): Spoofing
Sensors: Multiple sensors
Description: Spoofing allows a malicious object to impersonate another object on a network to bypass authorization checks or steal data. Glucose sensor impersonates as a temperature sensor and sends recommendations to breach the trust negotiation process. The module is applicable only if the privacy parameter in Hexagon framework does not opt for anonymous access.
Scenario 7 (MA-7): Attack with Botnet
Sensors: Any sen**sor**
Description: Any compromise with botnet may disrupt the entire system and cause malfunction of the trust negotiation framework. The glucose sensor is infected with a botnet and sending arbitrary packets to other sensors in the network to compromise.

Scenario 8 (MA-8): Privilege escalation attacks
Sensors: Any sensor
Description: Privilege escalation attack allows the application to gain elevated access to a resource or action. It targets the flaw in the design decisions of the framework. Glucose sensor gains elevated privilege in peer recommendation module and start endorsing itself.
Scenario 9 (MA-9): Rogue device
Sensors: Glucose and Anesthesia sensor
Description: The Rogue device is an unauthorized device connected to a network that poses a risk to the network. Each rogue device will try to perform unintended actions to create havoc in the network. anesthesia monitoring sensor is sending the miscellaneous value to the configuration module to alter the existing baseline of the system.
Scenario 10 (MA-10): Brute force attacks
Sensors: Any Sensors
Description: Brute force attack uses trial and error approach or permutations and combinations to attack a resource by generating many requests with possible fuzzy sets.
Temperature sensor tries to brute force reputation rating of others to improve the overall reputation in the system.
Scenario 11 (MA-11): Targeted attacks
Sensors: Any sensors
Description: Reverse engineering is the process of unveiling the design by deconstructing the architecture to extract internal details of the system. Reverse engineering the iOS mobile app to perform targeted attacks. Glucose sensor application is reverse engineered to change the default behavior by changing the past interactions.
Scenario 12 (MA-12): Malicious requests
Sensors: Any sensor
Description: Malicious requests include broadcasting a message into network asking the peers to response for an operation which never took place. Glucose sensor broadcasting a peer recommendation for an action which did not take place.
Scenario 13 (MA-13): Integrity of the sub-system
Sensors: Any sensor
Description: Integrity is the process of providing assurance to ensure the system works accurately. SpO2 sensor performing unintended actions to impair the processes of the system leads to breach to integrity.
Scenario 14 (MA-14): Malicious database entries
Sensors: Any sensor
Description: Hexagon framework stores past interactions from peers in the database. The data aids in taking trust negotiation. Injecting malicious data in the database will breach the framework.
Scenario 15 (MA-15): Application attacks
Sensors: Any sensor
Description: Application attacks are the flaws in application and
Scenario 16 (MA-16): Deadlock and starvation
Sensors: Any sensor
Description: The processes in one object had dependency and blocked to gain access to a resource leads to deadlock and starvation. Glucose sensor sends a request to scale the sensor for the weight of the patient. Weighing sensor process is expecting the value from body position sensor to compute the BMI index of the same patient causing a deadlock situation.
Scenario 17 (MA-17): Performance degradation
Sensors: Any sensor
Description: Performance degradation may cause due to a wide array of reasons like the use of heterogeneous devices and issues with latency, congestion, errors in network or protocols used, etc. Performance degradation may result in non-availability of the system.
Scenario 18 (MA-18): Elevation of privileges
Sensors: Any sensor
Description: Elevation of privileges attack allows the application to gain more access to a resource or action. It targets the flaw in the design decisions of the framework. Temperature sensor gains elevated privilege in peer recommendation module and start endorsing itself.
Scenario 19 (MA-19): Attacks on Privacy
Sensors: Any Sensor
Description: Patients healthcare data is highly sensitive in nature and should be handled with care. Any breach with the direct and indirect vital parameters may not only breach the privacy of the patient but also non-compliant against HIPAA, NIST, ISMS and GDPR standards.
Scenario 20 (MA-20): Invalid format
Sensors: Any sensor
Description: Invalid format is the attack pattern of sending messages in an unacceptable format. These messages failed to get interpreted correctly and interrupted maliciously. Glucose sensor broadcast reputation request and the value received is in an invalid format.
Scenario 21 (MA-21): Ransomware Attacks
Sensors: Any sensor
Description: Ransomware is a kind of malicious program that threatens to block victims access by encrypting the data unless a ransom is paid. All data in the knowledge base is encrypted and cannot be decrypted without paying the ransom.
Scenario 22 (MA-22): Breach to sensitive data
Sensors: Any sensor
Description: sensitive data need to be protected with right authentication and authorization controls. Any unauthorized access leads to breach to the data. Any breach to knowledge base leads to leakage in sensitive data.
Scenario 23 (MA-23): Application layer fragmentation attacks
Sensors: Any sensor
Description: Fragmentation attack allows overlapping packets or missing packets that do not allow the application to reassembly. Glucose sensor broadcasts a message seeking peer recommendations and the message sent by the peer has missing fragmentation that causes it to crash.
Scenario 24 (MA-24): Heuristic Attacks
Sensors: Any sensor
Description: Heuristic attacks represents an attack based on innovative vectors rather conventional chosen vectors. These are targeted attacks where an attacker trying to hack parameters in a sensor is an example for the heuristic attack.
Scenario 25 (MA-25): Zero-day attacks
Sensors: Any sensor
Description: Zero attack in information security is an application attack that exploits the previously unknown vulnerability. Unknown vulnerability in the glucose sensor may cause zero-day.

IV. RESULT AND DISCUSSION

The simulation for the above scenarios was run for the presented model to discover malicious interactions. Out of 44 scenarios that run randomly across the Hexagon framework, the framework achieved 79.24% positive results in identifying malicious interactions and failed to identify 11 interactions. The below scatter plot shows the discovery of failed malicious interactions (in red color) Vs. interactions found successfully (in green color) The negative correlation shows the number of interactions with the malicious objects decreased over a period due to increase in the knowledge base database as shown in figure 3.

V. CONCLUSION

Trust has been a fancy research topic and was studied in multiple domains. The study presented the trust negotiation methodology to derive the trust value for an Internet of Things. The primary objective of the methodology is to depict the human notion of trust using computational algorithms to derive at the final value.

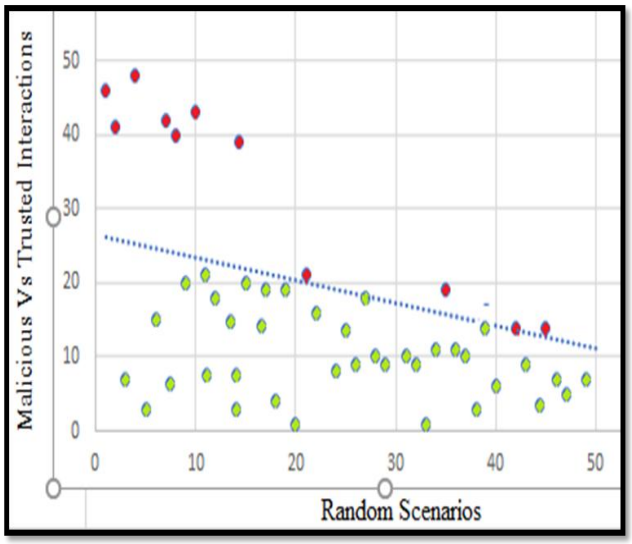

Figure 3 Correlation coefficient graphs for interactions with malicious Vs. trusted ones

The study describes the design, architecture, development, and deployed of the methodology along with various use case scenarios, and calculation of trust value using fuzzy logic with patient monitoring healthcare sensors in the IoT environment. This paper presents the testing its functionality with patient monitoring healthcare devices in critical care areas and presents the analysis results used at the hospital.

In our literature survey, we identified that most of the existing work is not validated against information security threats and can be easily reverse engineered. On the other hand, the existing research is largely restricted to mathematical projections and lack of practical implementations. The proposed Hexagon framework is not only fully implemented but validated against malicious use cases. The accomplishment of the study is to achieve 79.24% positive results in identifying malicious interactions, and the model improves over a period.

ACKNOWLEDGMENT

The authors would like to thank General Electric Healthcare and Philips Healthcare support staff for helping us to measure, analyze patient healthcare monitoring sensors to experiment with various scenarios as part of the study.

REFERENCES

1. Jesse M. Ehrenfeld, Maxime Cannesson, Monitoring Technologies in Acute Care Environments: A Comprehensive Guide to Patient Monitoring Technology (2014)
2. J F Payne, J P Crul, Patient Monitoring (1970)
3. Jasvini R. Jayendran Pillai, Lee Yeng Seng, Nur Shazana Binti Abdul Rahman, Patient Monitoring System Using Cloud System And Arduino Atmega (2018)
4. Ashton, Kevin, That 'Internet of Things'Thing. RFID Journal. 22. 97-114 , (2009)
5. A. Alrawais, A. Alhothaily, C. Hu and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," in IEEE Internet Computing, vol. 21, no. 2, pp. 34-42, Mar.-Apr. 2017.
6. 6. A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," in IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp. 586-602, 1 Oct.-Dec. 2017.
7. H. Kim and E. A. Lee, "Authentication and Authorization for the Internet of Things," in IT Professional, vol. 19, no. 5, pp. 27-33, 2017.
8. M. Shahzad and M. P. Singh, "Continuous Authentication and Authorization for the Internet of Things," in IEEE Internet Computing, vol. 21, no. 2, pp. 86-90, Mar.-Apr. 2017.
9. B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu and R. Ranjan, "IoTChain: Establishing Trust in the Internet of Things Ecosystem Using Blockchain," in IEEE Cloud Computing, vol. 5, no. 4, pp. 12-23, Jul./Aug. 2018.
10. Nallani Chakravartula, Raghu & Lakshmi V, Naga, Trust Management Framework for IOT Based P2P Objects, International Journal of Peer-to-Peer Networks. 8. 17-24. 10.5121/ijp2p.2017.8302. (2017)
11. Raghu Nallani Chakravartula & V, Naga Lakshmi, Secure configuration service in an IoT-based ad-hoc medical device, International Journal of Computer Engineering & Technology (IJCET), Volume 9, Issue 2, March-April 2018, pp. 99–105 (2018)
12. Raghu Nallani Chakravartula & Naga Lakshmi, Authentication, Authorization and Availability (AAA) of IoT-based ad-hoc medical devices, International Journal of Computer Science & Information Technology Research Excellence, Vol. 8 Issue 2, Mar.– Apr. 2018, (2018)
13. Hung T. Nguyen, Elbert A. Walker, A First Course in Fuzzy Logic, Third Edition, (2011)
14. Timothy J. Ross, Fuzzy Logic with Engineering Applications, Third Edition, (2013)

AUTHORS PROFILE

Raghu Ram Nallani Chakravartula, is currently heading the information security and compliance in Mirra Healthcare, USA. He has 16+ years of information security and compliance experience and in the past, he is associated with GE Healthcare, Philips Heathcare and many others. He is research scholar at GITAM university and his research interest include IoT Security. He has more than 23 certificates in infosec domain and published 11 papers in International journals and got 1 pending patent on his name.

Prof. V. Naga Lakshmi, is heading the Department of computer science in GITAM (Deemed to be university). She published more than 18 technical papers in international journals and 21 technical papers in national and international conferences. She received various awards and recognitions for her research work that she carried throughout the career.