

**AN INTELLIGENT CONTEXT AWARE BASED
ACCESS CONTROL FRAMEWORK TO
PREVENT ATTACKER NODES IN INTERNET OF
THINGS**

Dissertation submitted in fulfilment of the requirements for the Degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

By

AMRITPAL KAUR

11610832

Supervisor

ISHA MALIK



School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

December 2017



TOPIC APPROVAL PERFORMANCE

School of Computer Science and Engineering

Program : P172::M.Tech. (Computer Science and Engineering) [Full Time]

COURSE CODE : CSE548 REGULAR/BACKLOG : Regular GROUP NUMBER : CSERGD0047

Supervisor Name : Isha UID : 17451 Designation : Assistant Professor

Qualification : M.E Research Experience : 7 years

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Amritpal Kaur	11610832	2016	K1637	7837471911

SPECIALIZATION AREA : Networking and Security Supervisor Signature: Isha 17451

PROPOSED TOPIC : An intelligent Context Aware based Access Control framework to prevent attacker nodes in Internet of Things

Qualitative Assessment of Proposed Topic by PAC		
Sr.No.	Parameter	Rating (out of 10)
1	Project Novelty: Potential of the project to create new knowledge	7.50
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	7.75
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	7.50
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	7.50
5	Social Applicability: Project work intends to solve a practical problem.	7.75
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	7.75

PAC Committee Members		
PAC Member 1 Name: Prateek Agrawal	UID: 13714	Recommended (Y/N): Yes
PAC Member 2 Name: Deepak Prashar	UID: 13897	Recommended (Y/N): Yes
PAC Member 3 Name: Raj Karan Singh	UID: 14307	Recommended (Y/N): NA
PAC Member 4 Name: Pushendra Kumar Pateriya	UID: 14623	Recommended (Y/N): Yes
PAC Member 5 Name: Sawal Tandon	UID: 14770	Recommended (Y/N): NA
PAC Member 6 Name: Aditya Khamparia	UID: 17862	Recommended (Y/N): NA
PAC Member 7 Name: Anupinder Singh	UID: 19385	Recommended (Y/N): NA
DAA Nominee Name: Kuldeep Kumar Kushwaha	UID: 17118	Recommended (Y/N): Yes

Final Topic Approved by PAC: An intelligent Context Aware based Access Control framework to prevent attacker nodes in Internet of Things

Overall Remarks: Approved

PAC CHAIRPERSON Name: 11024::Amandeep Nagpal

Approval Date: 04 Nov 2017

ABSTRACT

IoT(Internet of Things) is a network of internet connected objects or things, which are capable to gather and interchange information by using ingrained sensors. The things in Internet of things may be any item, an animal or a person. IoT provides many services, however on the further hand threats regarding the security are also growing. Therefore, this report represents the survey and analysis of access control mechanisms in the field of Internet of things to amplify security concerns. The access control mechanisms are utilized to enable the secure and reliable access to the network resources, which provides the primary role in imposition of security layer over IoT networks. Here the various types of access control models, framework and protocols are described. Moreover, comparison between various access control mechanisms is made analyzing their performance levels. On the basis of shortcomings observed in the existing model, the proposed model covers the access control policy on each node of IoT by using context awareness. The context aware approach is included to intelligently monitor the context and behavior type of the IoT nodes in the network, which is further used to determine the rate of data transfer among the network nodes. This research work will simplify the node recognition procedure by using the ontology, which will be used to describe the node identity, node's network performance and data transmission procedures. Later, future scope is presented for upcoming research in the area of access control in IoT.

DECLARATION STATEMENT

I hereby declare that the research work reported in the dissertation proposal “AN INTELLIGENT CONTEXT AWARE BASED ACCESS CONTROL FRAMEWORK TO PREVENT ATTACKER NODES IN INTERNET OF THINGS” in partial fulfilment of the requirement for the award of Degree for Master of Technology in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor Mrs. Isha Malik. I have not submitted this work elsewhere for any degree or diploma.

I understand that the work presented herewith is in direct compliance with Lovely Professional University’s Policy on plagiarism, intellectual property rights, and highest standards of moral and ethical conduct. Therefore, to the best of my knowledge, the content of this dissertation represents authentic and honest research effort conducted, in its entirety, by me. I am fully responsible for the contents of my dissertation work.

AMRITPAL KAUR

11610832

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the M.Tech Dissertation/dissertation proposal entitled “AN INTELLIGENT CONTEXT AWARE BASED ACCESS CONTROL FRAMEWORK TO PREVENT ATTACKER NODES IN INTERNET OF THINGS”, submitted by **AMRITPAL KAUR** at **Lovely Professional University, Phagwara, India** is a bonafide record of her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

(Isha Malik)

Date:

Counter Signed by:

1) Concerned HOD:

HoD's Signature: _____

HoD Name: _____

Date: _____

2) Neutral Examiners:

External Examiner

Signature: _____

Name: _____

Affiliation: _____

Date: _____

Internal Examiner

Signature: _____

Name: _____

Date: _____

ACKNOWLEDGEMENT

I would like to convey my most heartfelt and sincere gratitude to my mentor Isha Malik of Lovely Professional University, for her valuable guidance and advice. Her willingness to motivate me contributed tremendously to achieve the goal successfully.

I would also like to thank dear God and my parents who have always inspired and encouraged me to achieve my goal successfully.

AMRITPAL KAUR

TABLE OF CONTENTS

CONTENTS	PAGE NO.
PAC form	ii
Abstract	iii
Declaration Statement	iv
Supervisor's Certificate	v
Acknowledgement	vi
Table of Contents	vii
List of Figures	ix
List of Tables	x
CHAPTER1: INTRODUCTION	1
1.1 INTRODUCTION OF INTERNET OF THINGS	1
1.2 ACEESS CONTROL IN IOT ENVIRONMENT	2
1.3 ATTACKS ON INTERNET OF THINGS	2
1.3.1 SPOOFING ATTACK	2
1.3.2 BRUTE FORCE ATTACK	2
1.4 TYPES OF ACCESS CONTROL MECHANISM	3
1.4.1 DISCETIONARY ACCESS CONTROL(DAC)	3
1.4.2 MANDATORY ACCESS CONTROL(MAC)	4
1.4.3 ROLE-BASED ACCESS CONTROL(RBAC)	5
1.5 ONTOLOGY PRINCIPLES	7
1.6 CONTEXT AWARENESS IN DATA TRANSMISSION IN IOT	8

TABLE OF CONTENTS

CONTENTS	PAGE NO.
CHAPTER2: REVIEW OF LITERATURE	9
2.1 EVALUATION OF IOT SECURITY	9
2.2 ACCESS CONTROL IN IOT	10
2.2.1 ROLE BASED ACCESS CONTROL	11
2.2.2 ATTRIBUTE BASED ACCESS CONTROL	12
2.2.3 CAPABILITY BASED ACCESS CONTROL	12
2.2.4 OAUTH PROTOCOL IN IOT	13
2.2.5 COMMUNITY DRIVEN ACCESS CONTROL	14
2.3 ONTOLOGY BASED ACCESS CONTROL MODELS	16
CHAPTER3: SCOPE OF THE STUDY	18
CHAPTER4: OBJECTIVE OF THE STUDY	19
CHAPTER5: RESEARCH METHODOLOGY	20
5.1 TOOLS USED	20
5.2 METHODOLOGY	20
5.3 FLOW CHART	22
CHAPTER6: EXPECTED OUTCOMES	23
CHAPTER7: SUMMARY AND CONCLUSION	24
REFERENCES	25

LIST OF TABLES

TABLE NO.	TABLE DESCRIPTION	PAGE NO
Table 1.1	Comparison between access control mechanisms	7
Table 2.1	Existing access control mechanism in Internet of Things	15

LIST OF FIGURES

FIGURE NO.	FIGURE DESCRIPTION	PAGE NO.
Figure 1.1	IoT Information Cycle	1
Figure 1.2	Discretionary Access Control	4
Figure 1.3	Mandatory Access Control	5
Figure 1.4	Role-Based Access Control	6
Figure 2.1	Access Process with Trust Degree	10
Figure 2.2	CapBAC example	13
Figure 5.1	Flow Chart Representing Methodology	22

CHAPTER 1

INTRODUCTION

1.1 Introduction of Internet of Things

In computing systems, a large amount of information is produced over the network applications, where the larger amount of data is created or generated, processed to yield the results, data transfers and its storage over the network, distributed or local storage in the modern enterprise networks. The demand of connectivity is rising in the data-driven applications across the world, which must combine the number of data handling techniques to properly manage the network data. The internet of things (IoT) networks are growing now-a-days, and building their way in many applications such as data collection in weather, pollution & water monitoring, resource management in smart city transportation & fire control management, healthcare applications, etc. The IoT networks are consisted of various nodes with limited resources, abundant resources, home appliances, wireless sensors, sensor and actuators, etc. This confirms the level of heterogeneity across the IoT networks, which is very difficult to handle with uniform communication standards.

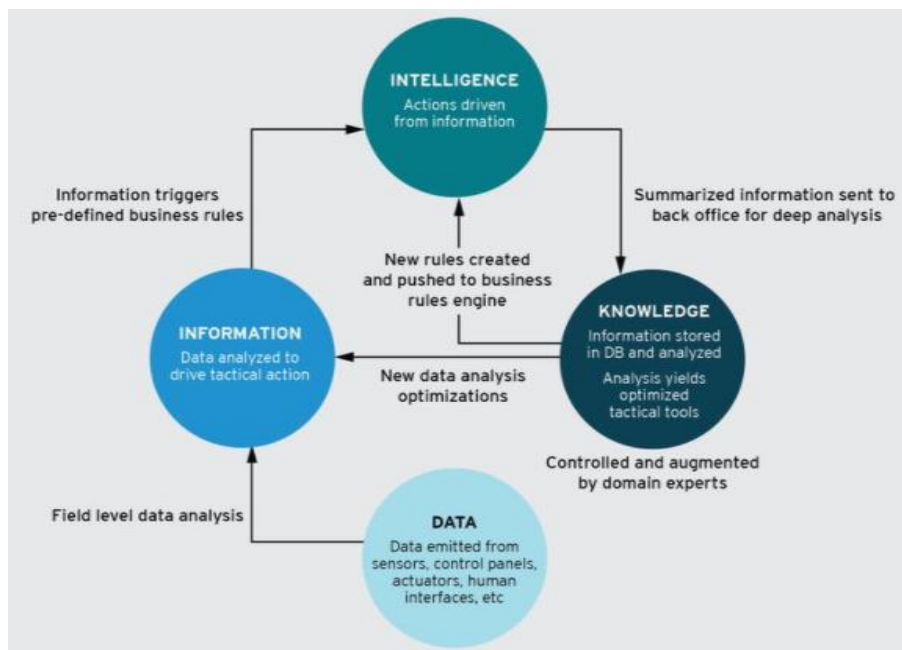


Figure1.1: IoT information cycle

1.2 Access Control in IoT Environments

The access control mechanisms are utilized to enable the secure and reliable access to the network resources, which provides the primary role in imposition of security layer over the IoT networks. An ideal access control mechanism must be dynamic in nature and capable enough to understand the different perspectives of data communications in the given network. The perspectives of the data communication includes the data transfer rates, packet loss rate, throughput, delay and related parameters. Such factors vary for sensing, heterogeneity (IOT nodes manufactured by different manufacturers), highly dynamic environments, complex network structure, distance from the base station, etc. Hence, all these factors must be analyzed in the access model in order to provide the balanced and dynamic security to IOT environments.

1.3 Attacks on Internet of Things

In this part, the various attacks on access control in IoT are described, which involves the various types of attacks on the IoT environments:

1.3.1 Spoofing Attack

All cycle creates an alternate access control period, and information of previous period keys does not permit finding of future period keys. In this attack, hacker node tries to break into the network by bypassing the access control protocol. In the spoofing attack, the information is spoofed from alternate sources for the sake of acquire the unauthorized access to the resources the network.

1.3.2 Brute Force Attack

This attack is used to break into the network by decoding or guessing the information used to take unauthorized access. The bit-to-bit decoding is performed under this technique. This bit-wise information guessing and exploration can create the final access codes to gain the access to the network resources.

1.4 Types of Access Control Mechanisms

1.4.1 Discretionary Access Control (DAC)

The DAC model, which is used for access control is considered as controlled measure to control the access the network resources, where the access requesting nodes are within or outside of the network segment. For the purpose of access control under DAC, the limited access is provided to the selected set of users, specific user types or essential property holding users in order to avoid the network breaches. DAC strategy has a tendency to be extremely adaptable and is generally utilized as a part of the business and government areas. Be that as it may, DAC is known to be innately feeble for two reasons. In the first place, assigning the access of some media to the user is to provide the user authority to acquire the data stored in the file or object. For example, if the access to the media or data owned by Bob is provided with the access to Ann, there will no authority of Bob afterwards to prevent the Ann from using the data in different ways, such as row duplication, data acquisition, etc. Hence, it has been found that DAC is not capable of analyzing the user's behavior after assigning the access to the specific user. Also, the DAC mode is learnt to lack against the malicious codes, such as Trojan horses, which are transferred as the files or zipped data. The following points can explain the major drawbacks in the DAC model:

- The information can be duplicated after acquiring the access to the specific data, which does not analyze the user's behavior.
- No layer of security has been applied under DAC for the authority or usage of the target information.
- The benefits of acquiring the data files from the data source, once the affiliation of the file is provided to the user after the access estimation mechanism.

Get to Control Lists (ACLs) and proprietor/gathering/different get to control components are by a long shot the most widely recognized system for actualizing DAC strategies. Different systems, despite the fact that not composed because of DAC, may have the capacities to execute a DAC approach.

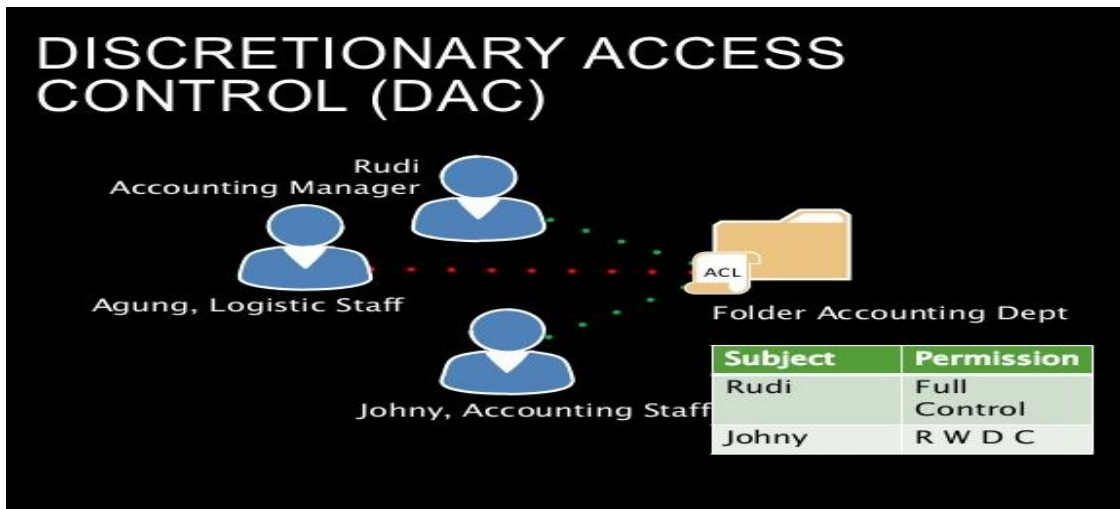


Figure 1.2: Discretionary Access Control

1.4.2 Mandatory Access Control (MAC)

The MAC models are usually designed to apply the essential access control verification for all of the requesting nodes on the given wireless network. The MAC model does not keep any exceptions to grant access to the network resources or services and applies the similar level of security with required information verification on all of the wireless network nodes. First implementations of the MAC models are proposed by Bell and LaPadula, which were designed to focus upon the application of the mandatory verification, whereas Sandhu is known to further improve the MAC model known as BLP. Sandhu's BLP model is primarily designed by implementing the encapsulation layer over the Bell-LaPadula model. All of the MAC models focus upon granting the access on the basis of subjective information. The very sensitive information clusters are usually designed to implement the MAC model, because there are no exceptions considered to grant the access to some of the users. The security labels are applied over all of the nodes after the verification of the required information for the purpose of authentication, which is usually verified using the confidential information such as login credentials, layered authentication keys, pre-shared keys, node ID, connection ID, etc.

There is another popular MAC model other than BLP, known as Biba model, which uses the integral information to consider the authenticity of the users or nodes before assigning the required access to the network resources or services.

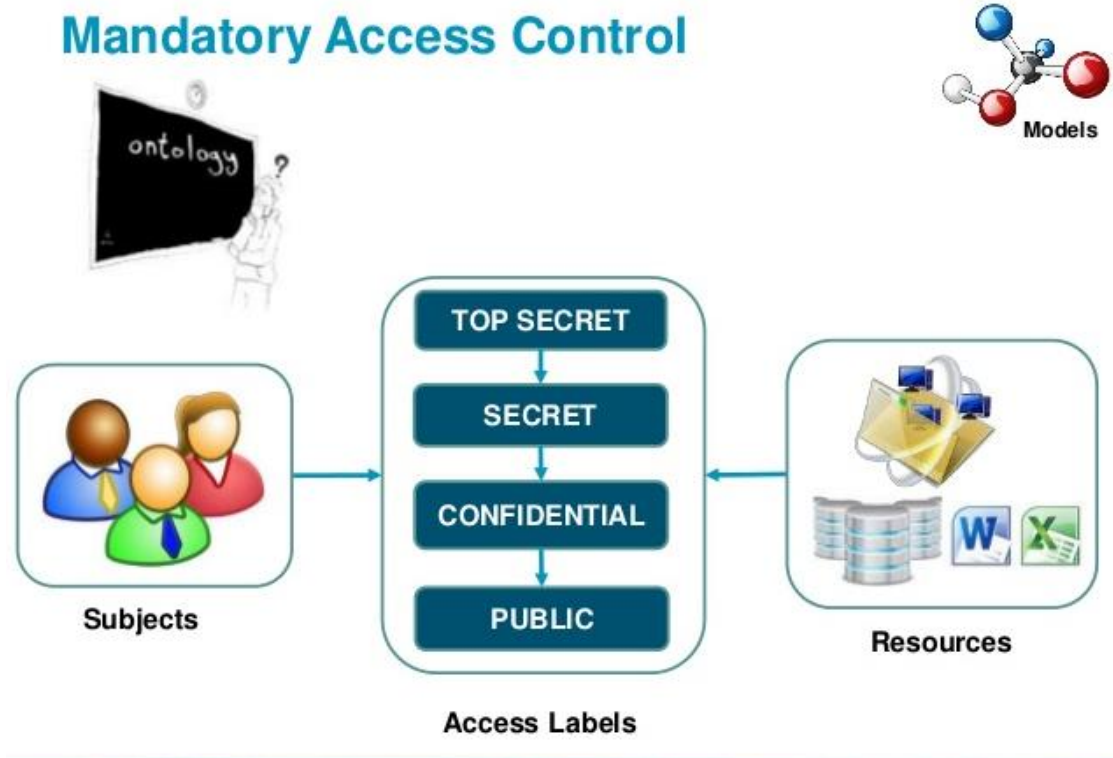


Figure1.3: Mandatory Access Control

1.4.3 Role-Based Access Control (RBAC)

On account of the unbending idea of MAC, where clients had next to zero control over the get to control approach, and the issues related with arrangement changes in DAC, early get to control models couldn't meet useful prerequisites of business associations. It was additionally understood that in vast associations information is not possessed by singular clients, but rather by the association itself, in this way access to information ought to think of one as' position in the hierarchical progression. This motivated further work, an aftereffect of which was (RBAC) Role-Based Access Control. In spite of fact that RBAC is in fact a type of non-optional get to control, late PC security messages regularly list RBAC as one of the three essential get to control approaches (the others are DAC and MAC). Early work on part based get to control backpedals to 1988, when Lochovsky and Woo characterized parts and sorted out them into a chain of command [LW88]. Throughout the years, numerous specialists have proposed models for RBAC. While the distinctions in these models are very huge, the centred idea remains genuinely reliable between them.

In RBAC, get to choices depend on the parts that individual clients have as a feature of an association. Clients go up against allotted parts, (for example, specialist, medical caretaker, teller, or chief). The use case of the different segments of the network can control the flexibility and creation of the information upheld under the specific security cases and strategies and for streamlining the security administration handle. A client sets up a session and enacts some subset of parts doled out to him/her. The authorizations accessible to the client in a session are those allocated to all the dynamic parts in that session. Under RBAC, clients are conceded participation into parts in light of their skills and duties in the association. At the point when a client is related with a part, the client can be given no more benefit than is important to play out the employment; since a hefty portion of the duties cover between work classifications, most extreme benefit for each occupation class could cause unapproved get to. This idea of slightest benefit requires recognizing the client's occupation capacities, deciding the base arrangement of benefits required to play out those capacities, and confining the client to an area with those benefits and nothing more.

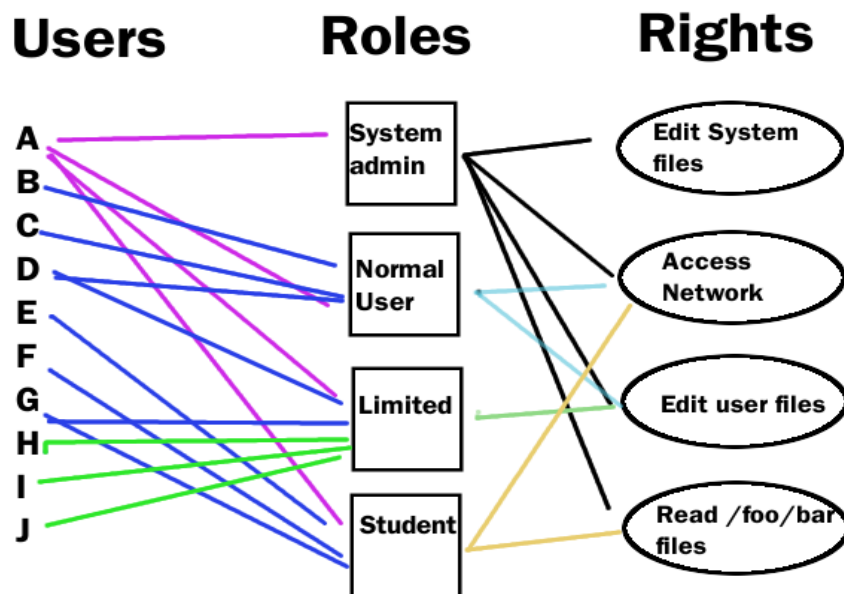


Figure 1.4: Role Based Access Control

The comparison between various access control mechanisms is describe in the table 1.

Table 1.1: The comparison between access control mechanisms

Schema Title	Functions	Security Hardening	Remarks
Discretionary access control	Applied over the selected users or connections requesting the network for uniform access.	Applied over the selected users in the networks. Hardens the security against the connection originating from out of the network. Local connections are accumulated on IP policies only.	<ol style="list-style-type: none"> 1. Must be applied over the networks with highly dependable staff on premises. 2. Should include the hybridization with other access control mechanism in the case of multiple departments in the local network.
Mandatory access control	Applied over all of the users or connections requesting the network for uniform access.	Applied over all of the incoming connections in the network. No access control redemption policy for selected users. Applied over the highly sensitive networks like, military, space agencies, intelligence agencies, etc.	<ol style="list-style-type: none"> 1. Evolution of the mandatory access policies with physical and dynamic access information and access keys must add more strength to the networks. 2. Mandatory access control mechanisms require very high computational power and authentication time, hence unable to apply over normal networks.
Role-based access control	Applied over all of the users or connections requesting the network for versatile access.	Applied over the organizational networks with multiple hierarchies and versatile departments. Role based access is provided to the different users, which ensures the access to different kinds of data varying from user to user according to the role. Multiple roles can be applied to some of the users in the special cases.	<ol style="list-style-type: none"> 1 Role based access control must be very flexible to handle the complex role combinations. 2 Role based access control mechanism are required to collect the pre-assigned database to map the users and their roles.

1.5 Ontology Principles

The ontology description method to collect the knowledge about the internet of things (IoT) has been discussed, which can be used to accomplish the multiple tasks, such as access control, etc. The fundamental focus of this report is to describe

multifaceted ontology for the purpose of dynamic composition and service discovery. The proposed descriptive ontology model is the knowledge-driven paradigm, which has been derived to capture the IoT network details with few properties described in the following section. The main aim of this model is described to create the balance among the trade-off in the internet of things, which can be designed based upon the following four principles:

- i. Lightweight:** Due to the processing limitations of the IoT nodes, the lightweight ontology mechanism is very important. In this model, the lightweight ontology method is proposed with highest level of expressiveness and security aspects.
- ii. Completeness:** The aim of this model is to create the high description ontology for IoT network, which can impose the high integrity and synchronization level for the common tasks such as data exchange, command synchronization, etc.
- iii. Compatibility:** The high compatibility of the new ontology model with existing ontology model is highly entailed.
- iv. Modularity:** The incorporation of the modular approach adds the higher level of flexibility and manageability for the expanding IoT networks. The modular approach enables the possibilities of evolution, extension and amalgamation with the external ontologies.

1.6 Context Awareness in Data Transmission for IoT

The IoT enables the connection between the sensor nodes and centralized application servers with internet based interactions. These IoT networks are considered the decentralized networks, as there nodes are spread across the wide area in the real-world, where it's not possible to manage them centrally. The major challenge faced by the context data distribution among the network, which is also known as "Quality of Context (QoC)". While working on the QoC, the major challenge arises with the management of privacy among the context owners. In this report middleware framework has been proposed to address the primary issues related to complexity related to security of the context data over the large-scale IoT networks.

CHAPTER 2

REVIEW OF LITERATURE

2.1 Evolution of IoT Security

Gubbi, Jayavardhana et.al. [1] has worked upon the description of the various aspects and architectural properties of internet of things. In this paper, the centralized approaches are discussed for the IoT models. These centralized approaches utilize the cloud computing environments to store and manage the information, which adds another dimension to the IoT networks. The IoT scalability and dynamic nature makes it further difficult for the implementation and management security protocols on the larger scale.

Ye, Ning et.al. [2] has developed efficient and scalable authentication protocol for the IoT environments. This paper proposes the ECC (elliptic curve cryptography) based IoT access control model empowered with additional authentication algorithm. The session management is also incorporated in this security management protocol, which protects this from the non-session based attacks. The proposed approach is attributed-based access control (ABAC) model, which utilizes the various security and network related attributes to take the access decisions.

Hernandez-Ramos et.al. [3] has worked on the access control mechanism among the internet of things environments on the basis of their distributed capability. The (CBA) Capability Based Access control analyzes the ability of the network node or segment to grant the desired access. This solution utilizes the authorization certificates, life cycle management and authentication process control. This scheme is designed as the capability-based access mechanism, which enables the access control in the distributed IoT networks. The authorization certificates are encrypted with the ECC encryption method. This scheme is enough capable to meet the scalability and manageability requirements in the IoT environments.

Mahalle, Parikshi N. et.al. [4] has worked upon the hybrid access control mechanism, which provokes the usage of capability and identity along with authentication for the IoT environments. This paper offers the new security scheme based upon authentication based access management model. This model is designed with the capability to protect against the various network attacks including denial of service (DoS), MITM (man-in-the-middle), etc.

Mahalle, Parikshit N. et.al. [5] has proposed the access control model based upon trust alongside the fuzzy approach to deploy over the internet of things. This paper offers the fuzzy based trust approach for access control in IoT environments. This fuzzy based approach identifies the users and assigns them the different trust levels, which are observed on the basis of their network behaviour.

2.2 Access Control In Internet of Things

Y. Lee et al. [6] the author has described various access control models such as UCON (Usage Control) is used for distinct access control requirements. UCON is used for familiar and unfamiliar end –users. Requirements and circumstances are used for decisions in UCON. In UCON, there are mainly three parameters for any action and which are authority, duty and status. Next access control model is CapBAC model. In this model where the objects want to interconnect with the server, the target node gives a token to that particular device. The client device can access the server for particular time. The time is specified at the token.

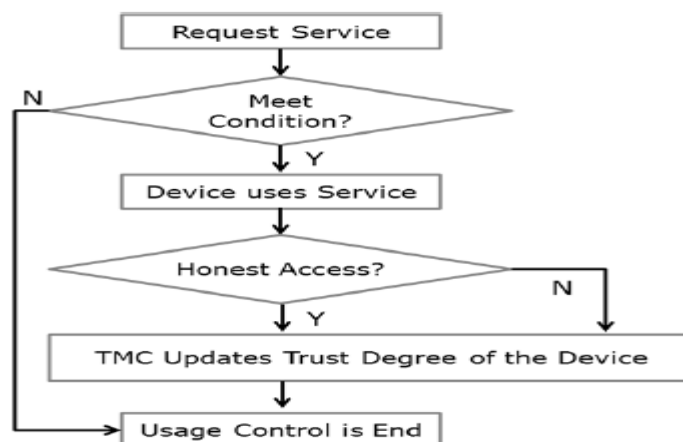


Figure 2.1: Access Process with Trust Degree

In Access control based on UCON (using trust degree) the server provides access to the devices on the basis of trust. That means if a device access the server according to the access control policies TMC (Trusted Management Center) feedback is given to that device. An ACM (Access Control Model), which is used to refresh the degree of trust. In Distributed Capability Based Access Control PDP (Policy Decision Point) server is used for centralized access control system. When any device want to access the server, the device send its situation data to the PDP server and PDP perform specific action. In Adaptive Access Control the policy of access is based on the risk and believes on the query. User can use the wrong paths, so there is a need to check the risky queries.

2.2.1 Role Based Access Control

M. Tamboli et al. [7] discuss that in IoT, all the things are resource constrained. When these devices communicate with each other there is a need of more safety, because dissimilar devices, sensors and actuator are used. For this, the main aim of the author is to provide a access control for devices, which contain constrained resources by using CoAP[Constrained Application Protocol] structure. In this approach services are accessed by tickets. Tickets are the IDs of the devices, which is unique for each service. Here Kerberos protocol is used together with CoAP, which decreases verification period and ticket permitting interval. Elliptic Curve Digital Signature Algorithm [ECDSA] is also presented, which enhance the confidentiality. This plan reduces the communication overhead and authentication interval.

A. Saxena et al. [8] discuss SMAC which stands for Simple Messaging and Access Control, in which all the aspects for access control introduce. SMAC is used at the communication layer, so there is no need for further access mechanism at the destination. Here port numbers of device are used as capabilities. All the work is done in a centralized fashion. The SMAC server offers a huge amount of computer-produced ports signifying message networks. But, as the ports are presented externally, when someone grasps the port number for transfer messages to a station, he can to eavesdrop for messages upcoming to that station from further consumers. This shortcoming can be overcome by a little adapting the hint to practice two-port networks. In its place of only one port, the networks require two ports unique for attending and one more for transfer. The two ports are mathematically related.

Though, it is actual tough to discover the new without identify a top-secret key. SMAC has advantages for example distributed access control database, light-load termination points, easy- revocation and things detection, generating it fit for IoT.

H. Che et al. [9] In this paper, the author explains the Role Based Access control to security the computer networks in a hierarchy. Some authors describe cryptography key for security in IoT. But when a group of devices are used in IoT, there is a need of some new security mechanism. So in this paper the author describe the result by using hierarchy Role based access control model for security in area of IoT. Given proposal increase the performance, decrease storage requirements and cost for implementing devices, which are Structure as a combination of IoTs with a safe hierarchy key administration.

2.2.2 Attribute based access control method

M. Hemdi et al. [10] describe that by the expansion of (IoT) and habit of little powered strategies such as devices a huge amount of individuals are consuming IoT structures in their home environment and companies to have additional control above their equipment. But the security of data in IoT environment is a major threat, when the IoT devices are misplaced and robbed. In this paper author explains that how we can protect our data from illegal consumers. For that they proposed an Attribute based access control method. This mechanism imposes some protocols in system so that the system Observe illegitimate access. Through measuring certain characteristics of the consumer like access period, MAC address, username, and secret code, the method will put on some of ABAC rules to assured that the customer who is demanding to access the data is legal.

2.2.3 Capability Based Access Control

B. Chan et al. [11] define S-CBAC stands for Secure-Capability Based Access Control model, which is used in IoT things in distributed environment. This model is mainly used for group access. In S-CBAC, user access mutual service which is functioning at numerous devices by using a single token. In S-CBAC, IPsec channel technique is used to transfer all datagram packets with the Encapsulating Security Payload (ESP) header. This maintains the confidentiality of data. In this model a group of devices is created those produce a common service. A requestor who wants

to access these services can access any device of the group by using a only one token. The devices and services are categorized by the addresses. Furthermore, S-CBAC forces unique local Address (ULA) to maintain group access.

S. Patelet al. [12] in this paper authors describe the mechanism for security, and privacy and access control. Different types of things are communicates with each other in IoT environment. Therefore the main requirement during the implementation of the framework is to keep up the security and protection of these things. In this paper, the crucial methods to assure protected transmission among devices are access control and authentication. Aimed at this determination the author defines the Elliptic Curve Cryptography with mutual authentication and Capability based access control model to assure defend authorization. An AVISPA tool is used to check this protocol. AVISPA tool presents that the given protocol is secure enough for reply attack, node capture attack, DoS attack and man-in middle attack.

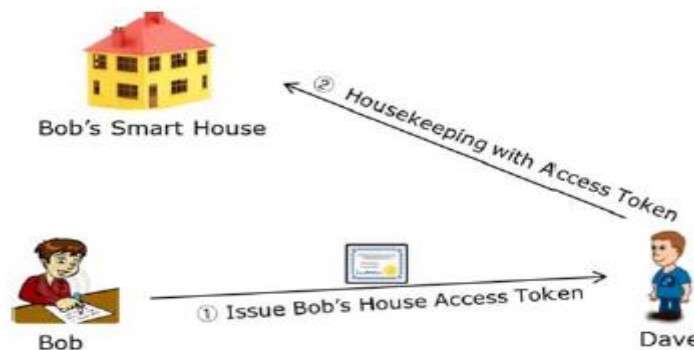


Figure 2.2: CapBAC example

2.2.4 OAuth Protocol

S. Kinikaret al. [13] In IoT huge number of things (devices) are communicate with each other with the help of internet. These devices are constrained devices, so they have a limited storing ability and computing control. Due to these restrictions it is a challenge in IoT environment to offer robust authorization procedures. So to solve this problem, authors introduce a framework that implement a service with the help of open authentication protocol. As compare to another authentication methods OAuth is very smooth and protected method, which verifies the end users and allow them to use

the confidential data of the system. This protocol gives a substitute entry for the cyberspace enjoyers to log in to the internet sites like Skype, Gmail, Facebook, twitter accounts without displaying their identifications. OAuth actions by means of an intermediate on behalf of the customer, giving the facility by an access token that allows particular account data to be used.

F. Fernandez et al. [14]. In this paper authors describe the access control model which is depend on OAuth 2.0 protocol. OAuth2 is an Open Authorization protocol which is uncomplicated and safe approach, that confirms consumers and permit admission for their safe records giving the facility with an admission symbol. In OAuth 2.0 protocol, all the data send or receive with the help of tokens, when there are number of users are involved. The main necessities for internet of things are flexibility and safety which are satisfied by the particular model.

S. Emerson et al. [15] Now a days, Internet of Things become a most popular subject in the research The adaptation of the Internet of Things in daily routine is increased day by day because it provide better adaptability and uncomplicated life style. Many functions of IoT promote a large number of security problems. For this the authors here discuss about a way that gives a protected authenticated method, which depends on OAuth 2.0 protocol. This planned method defends IoT system from illegal users with the helps security administrator using OAuth 2.0 protocol. Furthermore, this method offers tractability in dealing IoT systems. The security administrator offers verification facility for several IoT systems, which can also aid to decrease the cost to keep protected database in IoT systems.

2.2.5 Community Driven Access Control

D. Hussein et al. [16] Given paper suggests a different framework for access control for devices in IoT in a distributed environment, which is called community-driven access control. As of an IoT viewpoint, the thought of community looks appropriate. This theory is motivated from the statement that IoT things are infrequently completely inaccessible. As an alternative, they work in aggregation with another things and facilities to complete a mutual task. In the particular paper they frame on the notion of public to describe the idea of privileges. Actually, the

significance of access control in IoT will be highlighted, because huge amount of linked things rises as well as IoT commercial models converted into refined model. In the given paper they give specified needs for performing access controls in IoT, without the need of specific access control procedure. The following table shows the existing access control mechanism in IoT.

Table 2.1: Existing Access Control Mechanism in IoT

Author, Publisher & Year	Technique Proposed	Problem Addressed	Brief Review
Castellani, Angelo P. IEEE, 2010 [17]	This article presents the case study on the versatile architectures and protocols for IoT networks.	The new technique is designed to meet the requirements of IoT in the highly flexible and expandable environment.	IPv6 based IoT architecture is analyzed for its ability to tackle the diverse and heterogeneous IoT networks.
Grønbæk, Inge, IEEE, 2008 [18]	This article discusses the IoT architecture and the needs of APIs for data exchange.	Diverse interconnection problems in the IoT are covered in this paper with QoS based IP networking in IoT.	This scheme involves the network architecture with multi-homing ability in the mobile networks constructed with dynamic membership of the network nodes in internet of things.
Debaty, Philippe, IEEE Personal Communications 2001 [19]	This paper discusses the correlation of people, places and things using the internet.	The context based approach is proposed, which utilizes the diversified network properties including location, identity and device capabilities.	This scheme focuses upon the web presence in the terms of people, places and things in the best interconnection ability.
Babar, Sachin, Springer 2010 [20]	This paper discusses the secure ontology aware IoT model for data protection networks.	Proposed security model and risk classification for the Internet of Things (IoT)	The given paper gives an outline, exploration and classification of confidence and secrecy threats in IoT.
Atzori, Luigi, Elsevier 2010 [21]	This paper discusses the related technologies and communication solutions for the multiple archetypes in the IoT networks.	This review is coordinated to those that one need to approach this mind boggling order and add to its improvement	The give paper deliberates the different approaches and technologies for the vigorous and dynamic connectivity of the IoT nodes in the complex architectures.
Kortuem, Gerd, IEEE Internet Computing 2010 [22]	The order of the network architectonics for the connectivity of objects is discuss here.	Smart objects are managed as the building blocks to construct the internet of things	This paper describes the actions, strategy, and procedure responsive smooth items and shows in what way the particular architectural notions maintain gradually difficult application.

2.3 Ontology Based Access Control Model

Wang, Wei et.al. [23] has worked upon the representation and description of the network ontology for IoT to acquire comprehensive data from IoT nodes. Primary objective of this research is to describe the ontology on the basis of resources to maximize the network utilization to gather the maximum information in the IoT domain. Key idea of this model is to describe the standard service properties to represent the scalability oriented features with context aware intelligence access control mechanism. The multivariate ontological feature descriptor has been deployed in this knowledge driven architecture to control the access among the internet of things (IoT) network.

Hachem, Sara et.al. [24] has worked upon the innovative ontological extraction method for IoT networks. In this paper, the authors have worked upon the service oriented middleware application of ontology based IOT network model to describe the flexibility and synchronization ability. The primary focus has been kept upon the ontological modelling of IOTs to describe the variety of features to describe the identity of the nodes along with their network based performance. The multivariate feature descriptor based ontology will be utilized to create the middleware approach.

Alberto Huertas et.al. [25], This paper is expected to give an answer for creating context-aware keen applications protecting the clients' security in the Internet of Things (IoT). In this logic, author display a framework called Semantic Web-based Context Management (SeCoMan) went for offering an arrangement of predefined enquiries to offer applications with data about internal position of clients what's more, objects, and in addition context-aware facilities. SeCoMan utilizes a semantic-arranged IoT vision in which semantic knowledge show a vital part. Indeed, SeCoMan utilizes Semantic Web for displaying representation of things, thinking over information to surmise new learning, what's more, characterizing context-aware strategies. SeCoMan likewise characterizes a layered design, including capacities identified with the administration of the clients' security in a way that suit IoT prerequisites, furthermore not influencing framework execution nor presenting unreasonable overheads.

Lim, Léon et.al. [26] has worked upon the enhancement of internet of things (IoT) with context awareness in the data propagation and distribution network. In this scheme the quality of context (QoC) approach has been utilized to control the context of the data, node or network for the particular traffic flow. This scheme has been designed with the higher order adaptability to handle complex network model consisted of the heterogeneous large-scale IoT environments. The owners of context and the end-customers are linked with the QoC approach, which describes the global, device based and physics based ontological descriptors are deployed to implement the attribute based access control and to determine the legitimate users, and that all in the reasonable expense.

Hosseinzadeh, Shohreh et.al. [27] has worked upon the development of the context-aware mechanism for role-based access control to create the smarter networks, which implements the security framework with semantic ability. In this paper, the data security and privacy model has been developed over the hybrid ontological structure, which includes the device level ontology and web ontology language (OWL), which is deployed over the C Language Integrated Production System (CLIPS). Main aim of the proposed model is designed to create the higher context-aware model with role-based access control abilities and to achieve the higher efficiency.

CHAPTER 3

SCOPE OF THE STUDY

The on-demand services are increasing across the IoT networks, which are increasing the requirement of the network connections in the data-driven applications in various fields. The growth of IoT networks are designed to collect the various kinds of data for weather, water & pollution monitoring, smart city resources management, home automation, healthcare applications, etc. The IoT networks are consisted of various nodes with limited resources, abundant resources, home appliances, wireless sensors, sensor and actuators, etc. This confirms the level of heterogeneity across the IoT networks, which is very difficult to handle with uniform communication standards. The efficient security implementation using context aware based access control model for IoT environments based scheme has been proposed. The context aware based access control model approach is designed to utilize the ontological knowledge data efficiently in order to optimize the performance of IoT computing environment. This IoT approach is required to recognize the type network nodes, network parameters and other features to employ the authorization based network security. This framework will simplify the node recognition procedure by using the ontology, which will be used to describe the node identity, node's network performance and data transmission procedures.

CHAPTER 4

OBJECTIVE OF THE STUDY

In this work, we have found the research gaps that are outlined in section 3. The following objectives are identified to meet the above mentioned research gaps. In this research, few of the following objectives will be considered.

- i.** To perform comparative analysis of existing ontology based IoT access control models based on their functions.
- ii.** To propose an intelligent context aware based access control model for taking real time decisions on efficient authorization of IoT devices.
- iii.** To analyze the performance of proposed mechanism for IoT access control and security management in terms of throughput, delay and packet drop ratio.

5.1 Tools Used

The tool which will be used to implement this work is MATLAB (MATRIX LABORATORY) simulator. A computer equipped with i3/i5/i7 processor with 4GB RAM and 40GBs of empty space on disk is required to run MATLAB simulator.

MATLAB is an information investigation and perception apparatus which has been outlined with capable help for networks and grid operations. MATLAB has phenomenal illustrations capacities, and its own capable programming language.

MATLAB permit concentrating and functioning on applications as opposed to on programming points of interest. It empowers to take care of numerous numerical issues in a small amount of the time it would take you to compose a program in a lower level language. . MATLAB betters comprehend and apply ideas in applications running from industrial and arithmetic to chemistry and financial aspects

5.2 Methodology

The following steps would be incorporated in order to achieve the objectives defined in section 4:-

i. Literature Survey

This step involves the study of literature on the various ontology based models in the IoT domain. Various types of the IoT models would be covered under this step, which primarily involves the access control models and traffic management using the IoT ontology. The shortcomings and advantages of the existing models are studied, which helps to create the full proof system design for IoT access control and traffic management.

ii. Ontology Representation

This step involves the building and construction of ontology from the IoT networks. The parameters or properties of the IoT nodes, manufacturing details, network standards, network performance, etc are studied in the existing models in order to understand their importance. Afterwards, the useful information parameters would be selected for the construction of ontology base knowledge data to manage the IoT networks.

iii. Simulation Design of Prototype Network

The prototype network would be constructed to simulate the IoT networks, which is used for the testing of the IoT access control model and traffic management model. The prototype network must involve the heterogeneous nodes in at least two domains, such as healthcare, vehicular network, house security, weather, pollution, etc. Their storage and information processing would be performed on the servers installed on different locations in the city, which produces the higher complexity of data management.

iv. Machine Learning based Ontology Classification

The machine learning based ontology classification model must be capable of recognizing the individual nodes, security level, network performance of individual nodes, calculate the possible traffic paths, understanding traffic flows, etc in order to take the network decisions. The machine learning model would be used to ensure the network security in the IoT network with access control mechanism and traffic management.

v. Performance Evaluation

The performance of the network would be evaluated by using the network parameters of appropriate parameters. The parameters concerned with security and performance of the IoT network would be considered for the evaluation of the system performance.

5.3 Flow Chart

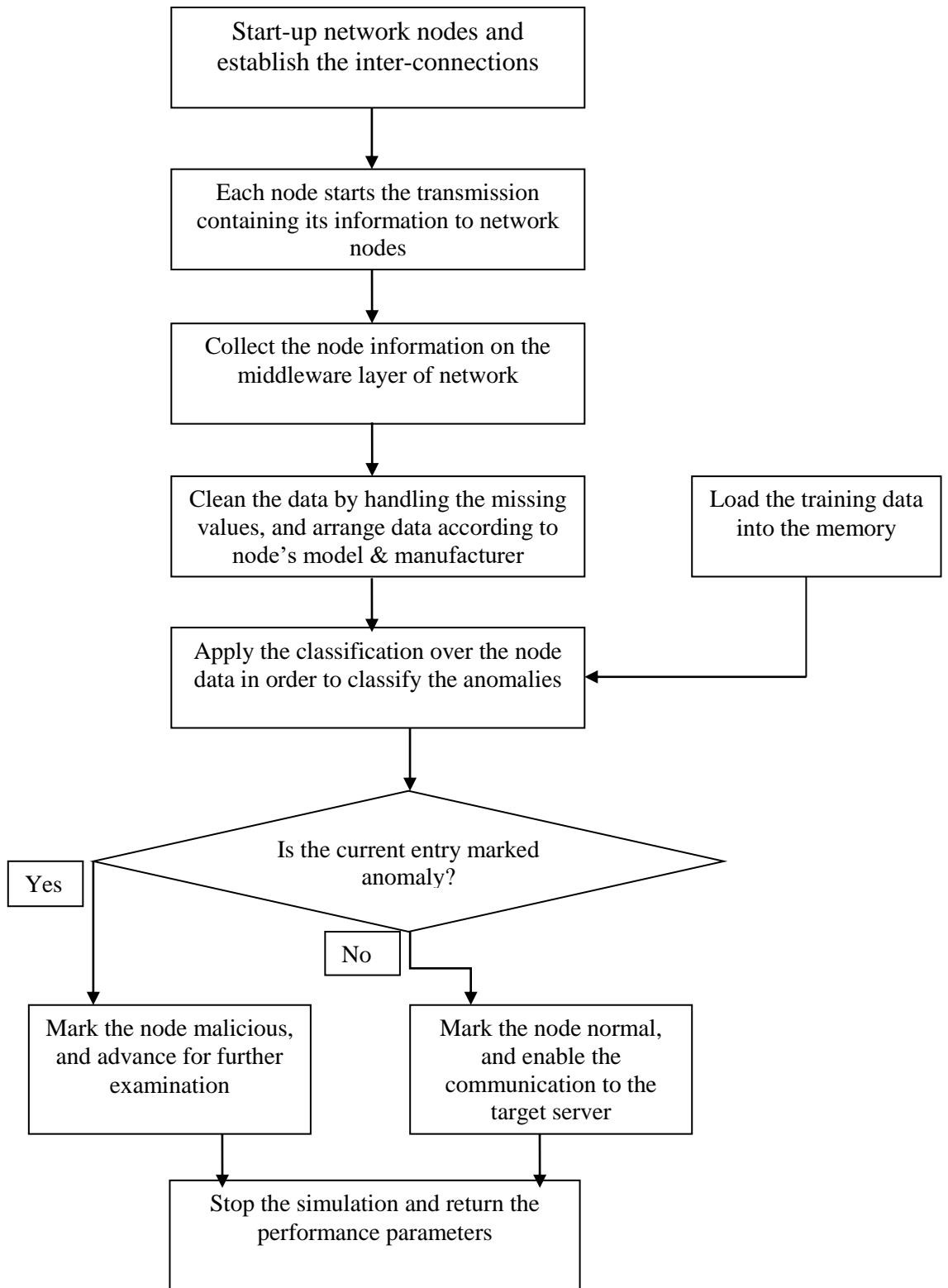


Figure5.1: Flow Chart Representing Methodology

CHAPTER 6

EXPECTED OUTCOMES

The context based access control framework will implement access control strategy on each node of IoT by using context awareness. The context aware approach is included to intelligently monitor the context and behavior type of the IoT nodes in the network, which is further used to determine the rate of data transfer among the network nodes. The nodes that will not follow the policy according to the context will not be provided the access to the network resources under this access control framework. This work will simplify the node recognition procedure by using the ontology, which will be used to describe the node identity, node's network performance and data transmission procedures.

The proposed framework is scalable and flexible, which means it can be applied to the variety of IoT networks formed from heterogeneous nodes. Using intelligent learning process, the framework will effectively recognize the attacker nodes in order to prevent them from accessing the network resources. This research work will increase the network performance, which can be measured in the terms of throughput, delay and packet drop ratio.

- i.** The proposed framework is expected to improve the ability to take access control decisions in real time. This will make it efficient and applicable to the networks equipped with higher number of nodes.
- ii.** This research will improve the network performance in terms of throughput, packet drop ratio and delay.

CHAPTER 7

SUMMARY AND CONCLUSION

With the advent in technology with every passing day along with the internet usage all over the world, the scope of IoT is evolving bright. IoT makes our life smart, easier, faster and comfortable. On the other hand, the invisibility of the information gathering, management and distribution procedures raises fears. The confidentiality and safety of IoT consumers could be easily sacrificed. Therefore, the main purpose of this report is to survey the access control in Internet of Things. Here various types of access control models, framework and protocols are described, which are used in IoT.

The proposed work will begin with the simulation of IoT network topology, which further undergoes the ontology specific deployment. The ontology analysis model will be designed, which will analyze the ontology of each node to determine the attacker nodes on the basis of their behavior. The context aware ontology approach will regularly monitor the node performance, which will help to find the anomaly (or attacking behavior) of the target node. This research work will improve the network performance, which can be measured in the terms of throughput, delay and packet drop ratio.

REFERENCES

- [1] Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. "Internet of Things (IoT): A vision, architectural elements, and future directions." *Future generation computer systems* 29, no. 7 (2013): 1645-1660.
- [2] Ye, Ning, Yan Zhu, Ru-chuan Wang, and Qiao-min Lin. "An efficient authentication and access control scheme for perception layer of internet of things", *14th IEEE Annual Consumers Communication & Networking Conference Sensors* 13, Year: 2014
- [3] Hernandez-Ramos, Jose L., Antonio J. Jara, Leandro Marin, and Antonio F. Skarmeta. "Distributed capability-based access control for the internet of things." *Journal of Internet Services and Information Security (JISIS)* 3, no. 3/4 (2013): 1-16.
- [4] Mahalle, Parikshit N., Bayu Anggorojati, Neeli R. Prasad, and Ramjee Prasad. "Identity authentication and capability based access control (iacac) for the internet of things." *Journal of Cyber Security and Mobility* 1, no. 4 (2013): 309-348.
- [5] Mahalle, Parikshit N., Pravin A. Thakre, Neeli Rashmi Prasad, and Ramjee Prasad. "A fuzzy approach to trust based access control in internet of things." In *Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronics Systems (VITAE), 2013 3rd International Conference on*, pp. 1-5. IEEE, 2013.
- [6] Yung-kyung Lee; Jae-deok Lim; Yong-jeon; Jeon-nyeo Kim, "Technology Trends of Access Control in IoT and Requirement Analysis", *2015 International Conference on Information and Communication Technology Convergence (ICTC)*, Year: 2015
- [7] Mohsin B Tamboli; Dayanand Dambawade, "Secure and efficient CoAP based authentication and access control for Internet of Things (IoT)", *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Year: 2016

- [8] Amitabh Saxena; Pradeepkumar Duraisamy; Vikrant Kaulgud, “SMAC: Scalable Access Control in IoT”, *2015 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, Year: 2015.
- [9] Hsing-Chung Che; Chia-Hui Chang; Fang-Yie Leu, “Implement of agent with role-based hierarchy access control for secure grouping IoTs”, *2017 14th IEEE Annual Consumers Communication & Networking Conference (CCNC)*; Year: 2017
- [10] Marwah Hemdi; Ralph Deters, “Using REST based protocol to enable ABAC within IoT systems”, *2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Year: 2016
- [11] BortingChen; Yu-Lun Huang; Mesut Gunes, “S-CBAC: A secure access control model supporting group access for Internet of Things”, *2015 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, Year: 2015
- [12] Sudha Patel; Dhiren R. Patel; Ankit P. Navik “Energy efficient intergrated authentication and access control mechanism for Internet of Things”,*International Conference on Internet of Things and Application (IOTA)*, Year: 2016
- [13] Swati Kinikar; Sujatha Terdal, “Implementation of open authentication for oT application”, *2016 International Conference on Inventive Computation application, year: 2016*, Volume: 1
- [14] Federico Fernandez; Alvaro Alonsa; Lourdes Marco; Joaquin Salvachua, “A model to enable application-scoped access control as a service for IoT using OAuth 2.0”, *2017 20th Conference on Innovations in Clouds,Internet and Networks(ICIN)*, Year: 2017
- [15] Shamini Emerson; Young-Kyu Choi; Dong-Yeop Hwang; Kang-Seok Kim; Ki-Hyung Kim, “An OAuth base authentication mechanism for IoT networks”, *2015 International Conference on Information and Communication Technology Convergence (ICTC)*, Year: 2015
- [16] Dina Hussein; Emmanuel Bertin; Vincent Frey, “A Community-Driven Access Control Approach in Distributed IoT Environments” *IEEE Communication Magazines*, Year: 2017, Volume: 55, Issue: 3
- [17] Castellani, Angelo P., Nicola Bui, Paolo Casari, Michele Rossi, Zach Shelby, and Michele Zorzi. "Architecture and protocols for the internet of things: A case study." *In Pervasive Computing and Communications Workshops (PERCOM*

- Workshops*), 2010 8th IEEE International Conference on, pp. 678-683. IEEE, 2010.
- [18] Grønbaek, Inge. "Architecture for the Internet of Things (IoT): API and interconnect." *In Sensor Technologies and Applications, 2008. SENSORCOMM'08. Second International Conference on*, pp. 802-807. IEEE, 2008.
- [19] Debaty, Philippe, and Deborah Caswell. "Uniform web presence architecture for people, places, and things." *IEEE Personal Communications* 8, no. 4 (2001): 46-51.
- [20] Babar, Sachin, Parikshit Mahalle, Antonietta Stango, Neeli Prasad, and Ramjee Prasad. "Proposed security model and threat taxonomy for the Internet of Things (IoT)." *Recent Trends in Network Security and Applications (2010)*: 420-429.
- [21] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." *Computer networks* 54, no. 15 (2010): 2787-2805.
- [22] Kortuem, Gerd, Fahim Kawsar, Vasughi Sundramoorthy, and Daniel Fitton. "Smart objects as building blocks for the internet of things." *IEEE Internet Computing* 14, no. 1 (2010): 44-51.
- [23] Wang, Wei, Suparna De, Ralf Toenjes, Eike Reetz, and Klaus Moessner. "A comprehensive ontology for knowledge representation in the internet of things." *In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, pp. 1793-1798. IEEE, 2012.
- [24] Hachem, Sara, Thiago Teixeira, and Valérie Issarny. "Ontologies for the internet of things." *In Proceedings of the 8th Middleware Doctoral Symposium*, p. 3. ACM, 2011.
- [25] Alberto Huertas Celdran, Felix J. Garica Clemente, Manuel Gil Perez, and Gregorio Martinez Perez, "SeCoMan: A Semantic-Aware Policy Framework for Developing Privacy- Preserving and Context-Aware Smart Applications." *IEEE System Journal*, Vol. 10, No. 3 Year:2016.
- [26] Lim, Léon, Pierrick Marie, Denis Conan, Sophie Chabridon, Thierry Desprats, and Atif Manzoor. "Enhancing context data distribution for the internet of things using qoc-awareness and attribute-based access control." *Annals of Telecommunications* 71, no. 3-4 (2016): 121-132.

- [27] Hosseinzadeh, Shohreh, Seppo Virtanen, Natalia Díaz-Rodríguez, and Johan Lilius. "A semantic security framework and context-aware role-based access control ontology for smart spaces." In *Proceedings of the International Workshop on Semantic Big Data*, p. 8. ACM, 2016.
- [28] Kumar, Adarsh, Krishna Gopal, and Alok Aggarwal. "Simulation and analysis of authentication protocols for mobile Internet of Things (MIoT)." In *Parallel, Distributed and Grid Computing (PDGC), 2014 International Conference on*, pp. 423-428. IEEE, 2014.
- [29] Lee, Jun-Ya, Wei-Cheng Lin, and Yu-Hung Huang, "A lightweight authentication protocol for internet of things.", In *Next-Generation Electronics (ISNE), 2014 International Symposium on*, pp. 1-2. IEEE, 2014.
- [30] Abomhara, Mohamed, and Geir M. Koiem. "Security and privacy in the Internet of Things: Current status and open issues." In *Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on*, pp. 1-8. IEEE, 2014.
- [31] Ali, S. T., Sivaraman, V., & Ostry, D., "Authentication of lossy data in body-sensor networks for cloud-based healthcare monitoring", *Future Generation Computer Systems*, 35, 80-90, Year: 2014
- [32] Khan, F. A., Ali, A., Abbas, H., & Halder, "A Cloud-based Healthcare Framework for Security and Patients' Data Privacy Using Wireless Body Area Networks", *Procedia Computer Science*, 34, 511-517, N. A. H. (2014).
- [33] Peng, X., Zhang, H., & Liu, J., "An ECG Compressed Sensing Method of Low Power Body Area Network" *TELKOMNIKA Indonesian Journal of Electrical Engineering*, 12(1), 292-303, Year: 2014
- [34] Hernandez-Ramos, Jose L., Marcin Piotr Pawlowski, Antonio J. Jara, Antonio F. Skarmeta, and Latif Ladid. "Toward a Lightweight Authentication and Authorization Framework for Smart Objects." *Selected Areas in Communications, IEEE Journal on* 33, no. 4 (2015): 690-702.