

A Stride Concerning Effective Retainment Of Privateness For Astute Homes

*Dissertation II - submitted in partial fulfilment of the requirements for the
Degree of*

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

By

Manikya Sinha

Registration No. 11307158

Supervisor

Ms. Rohini Lohia



School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

Month: November Year: 2017



TOPIC APPROVAL PERFORMA

School of Computer Science and Engineering

Program : 1202D::B.Tech -M.Tech (Dual Degree) - CSE

COURSE CODE : CSE548

REGULAR/BACKLOG : Regular

GROUP NUMBER : CSERGD0360

Supervisor Name : Rohini Lohia

UID : 22208

Designation : Assistant Professor
(Contract Basis)

Qualification : _____

Research Experience : _____

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Manikya Sinha	11307158	2013	K1309	8847497132

SPECIALIZATION AREA : Programing-II

Supervisor Signature: _____

PROPOSED TOPIC : A Stride Concerning Effective Retainment of Privateness in Astute Homes.

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	7.33
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	6.00
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.	6.67
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	7.33
5	Social Applicability: Project work intends to solve a practical problem.	7.00
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	7.00

PAC Committee Members		
PAC Member 1 Name: Kewal Krishan	UID: 11179	Recommended (Y/N): Yes
PAC Member 2 Name: Raj Karan Singh	UID: 14307	Recommended (Y/N): NA
PAC Member 3 Name: Sawal Tandon	UID: 14770	Recommended (Y/N): NA
PAC Member 4 Name: Dr. Pooja Gupta	UID: 19580	Recommended (Y/N): NA
PAC Member 5 Name: Kamlesh Lakhwani	UID: 20980	Recommended (Y/N): Yes
PAC Member 6 Name: Dr.Priyanka Chawla	UID: 22046	Recommended (Y/N): NA
DAA Nominee Name: Kuldeep Kumar Kushwaha	UID: 17118	Recommended (Y/N): Yes

Final Topic Approved by PAC: A Stride Concerning Effective Retainment of Privateness in Astute Homes.

Overall Remarks: Approved

PAC CHAIRPERSON Name: 11024::Amandeep Nagpal

Approval Date: 10 Nov 2017

DECLARATION STATEMENT

I hereby declare that the research work reported in the dissertation proposal “**A STRIDE CONCERNING EFFECTIVE RETAINMENT OF PRIVATENESS FOR ASTUTE HOMES**” in partial fulfillment of the requirement for the award of Degree for B.Tech-M.tech in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor **Ms. Rohini Lohia**. 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.

Signature of Candidate

Manikya Sinha

Registration No. 11307158

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the B.Tech-M.Tech Dissertation proposal "A STRIDE CONCERNING EFFECTIVE RETAINMENT OF PRIVATENESS FOR ASTUTE HOMES", submitted by **Manikya Sinha** at Lovely Professional University, Phagwara, India is a bonafide record of his original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

Signature of Supervisor

Name:.....

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 might want to thank my supervisor **Ms. Rohini Lohia** of the Computer Science and Technology at Lovely Professional University Phagwara. The way to Supervisor's office was constantly open at whatever point I kept running into an inconvenience spot or had an inquiry regarding my exploration or composing. She guided me in the course at whatever point she thought I required it.

TABLE OF CONTENTS

1. INTRODUCTION	1
1.1 INTERNET OF THINGS	1
1.1.1 Challenges in IOT.....	2
1.1.2 IOT Technologies.....	2
1.1.3 Applications of IOT.....	2
1.2 CLOUD COMPUTING.....	3
1.2.1 Types of Models.....	3
1.2.1.1 Deployment Models.....	3
1.2.1.1.1 Public Cloud	3
1.2.1.1.2 Private Cloud	3
1.2.1.1.3 Community Cloud.....	3
1.2.1.2 Service Models.....	3
1.2.1.2.1 Infrastructure-as-a-Service (IaaS).....	3
1.2.1.2.2 Platform-as-a-Service (PaaS).....	4
1.2.1.2.3 Software-as-a-Service (SaaS).....	4
1.3 SMART HOME.....	4
1.3.1 Challenges in SMART HOMES.....	5
1.3.2 Technologies that powers SMART HOMES.....	6
2. REVIEW OF LITERATURE.....	7
3. SCOPE OF STUDY	21
4. OBJECTIVE OF STUDY	23
5. PROPOSED RESEARCH METHODOLOGY	24
6. SUMMARY AND CONCLUSION	26
7. EXPECTED OUTCOMES	27
References.....	28
Appendix.....	31

LIST OF FIGURES

Figure 1.1.1 IOT Architecture	1
Figure 1.1.2 Shows Increase in IOT use	2
Figure 1.3.1 Showing Survey on demand	4
Figure 1.3.2 Showing market growth in US dollars	5
Figure 1.3.3 Showing some technologies powering the smart homes.	6
Figure 5.1 Showing the work flow of activity recognition	24
Figure 5.2 Showing the stage I process	25
Figure 5.3 Showing the stage II process	25

ABSTRACT

The smart/astute home is the future home for us and our next generation. The smart/astute home is called because of the involvement of the technology in it. In a smart/astute home we have number of devices which are connected to one another wirelessly or wired. Each device connected there would be having the sensors in them which are working days and nights to sense the changes made over the physical devices to which they are connected. Over working for hours they generates lots of the data that kept on growing from day to day and year to year and according to Moore's law to data size doubles every year. This much amount of data cannot be handled by our traditional data processing system's to which in this era a new technology emerges that is big data which comes with big data revolution that changes the world. Now a days we are using the sensors for different purposes like measuring the speed, weight, human health etc. Today's whole industry runs over sensors and in future the upcoming businesses will run totally on sensors. The IOT also empowers the smart/astute home. IOT helps the management of the sensor and making the better use of it. In this report I have done a survey over how cloud computing work for smart/astute home. I covered it's types and models. I studied about data analytics in that I found how it is used to provide privacy and security in smart/astute home. In this report a brief survey of everything is presented in review of literature chapter and a proposed workflow of my proposed solution is presented in research methodology section which will aid in conserving privacy in smart/astute homes.

Keywords: Cloud Computing, Internet of Things, Privacy, Smart/Astute Home.

1.1 INTERNET OF THINGS

IoT is term has changed the era since 1990's when the first machine used in 1930's that is a feedback machine or we say automation. Internet of things means interconnected devices or interworking of the devices whether it's a car, building, home, company department's, mobile phone, smartphone, watches etc. means anything which can be interconnected and can be connected to a network comes under internet of things.. In many schools and colleges the student where introduced with it and are asked to come up with new ideas to solve the day to day problems.

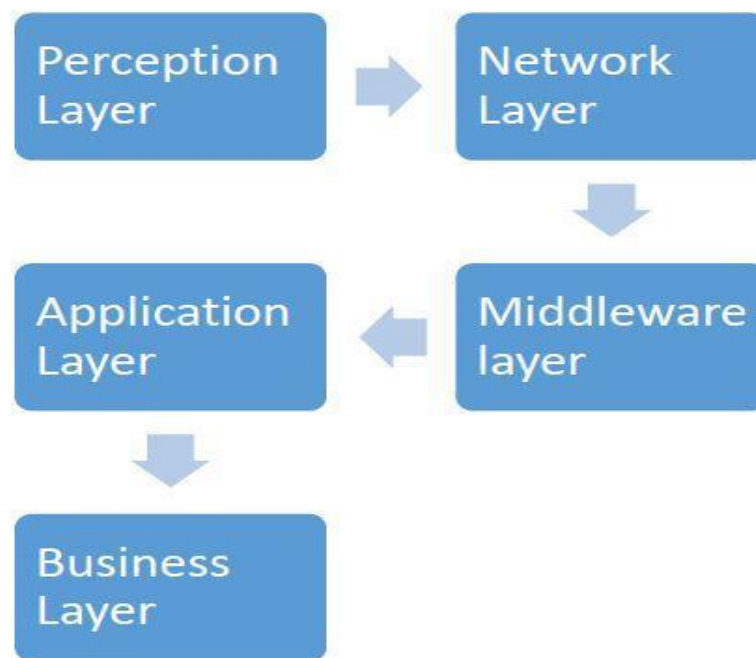


Figure 1.1.1 IOT Architecture

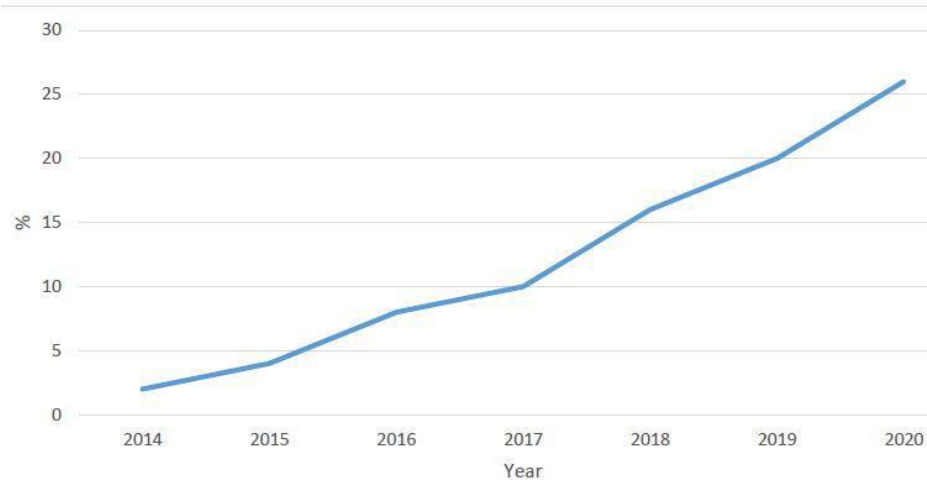


Figure 1.1.2 Showing Increase in IOT uses

The IOT allows us to ease our life. According to author in [9] following challenges, technologies and applications are discussed given below.

1.1.1 CHALLENGES IN IOT.

1. Energy, Data and Performance Management.
2. Security of Sensors and maintenance of IOT devices.
3. Deployment and Communication issues.

1.1.2 IOT TECHNOLOGIES.

1. Bluetooth, ZigBee, Near Field Communication.
2. Raspberry Pi and Arduino
3. Long Term Evolution, Light fidelity and Transport Layer Security.

1.1.3 APPLICATIONS OF IOT.

1. Smart health, city, mobile devices, teacher, school bag, kitchen, retail and home.
2. Border activity monitoring and guided missile creation.
3. IOT analytics, Media, Cloud and Fog computing.

1.2 CLOUD COMPUTING

The term Cloud alludes to a Network or Internet. Cloud computing gives us an open door by which we can get to the applications as utilities over the web. It enables us to make, design, and modify the business applications on the web [5].

1.2.1 TYPES OF MODELS.

1. Deployment Model

2. Service Model

1.2.1.1 DEPLOYMENT MODELS.

Deployment models are used for providing access to the cloud and were portrayed as open, private and group cloud.

1.2.1.1.1 PUBLIC CLOUD

Cloud enables frameworks and administrations to be effectively open to the overall population. Public cloud might be less secure due to its transparency.

1.2.1.1.2 PRIVATE CLOUD

The cloud empowers structures and organizations to be accessible inside an affiliation. It is more secured because of its private nature.

1.2.1.1.3 COMMUNITY CLOUD

The people group cloud enables frameworks and administrations to be available by a gathering of associations.

1.2.1.2 SERVICE MODELS.

Service models are utilized to describe the kind of administrations gave by the cloud. Its sorts are IaaS, PaaS and SaaS.

1.2.1.2.1 INFRASTRUCTURE – AS – A - SERVICE (IAAS)

Provide access to basic assets for example, physical machines, virtual machines, virtual capacity and so forth.

1.2.1.2.2 PLATFORM - AS - A - SERVICE (PAAS)

PaaS gives the runtime condition to applications, advancement and arrangement apparatuses, and so on.

1.2.1.2.3 SOFTWARE – AS – A - SERVICE (SAAS)

Show licenses to use programming applications as a help of end-customers.

1.3 SMART HOME

Smart home or say Smart connected home. A home of dream, ease of comfortability, secure home, lots of facility and making us lazy. Every person in this world thinks of a home for his/her family and in that scenario the SMART HOME come into picture. According to some study in US shows market demand of smart homes.

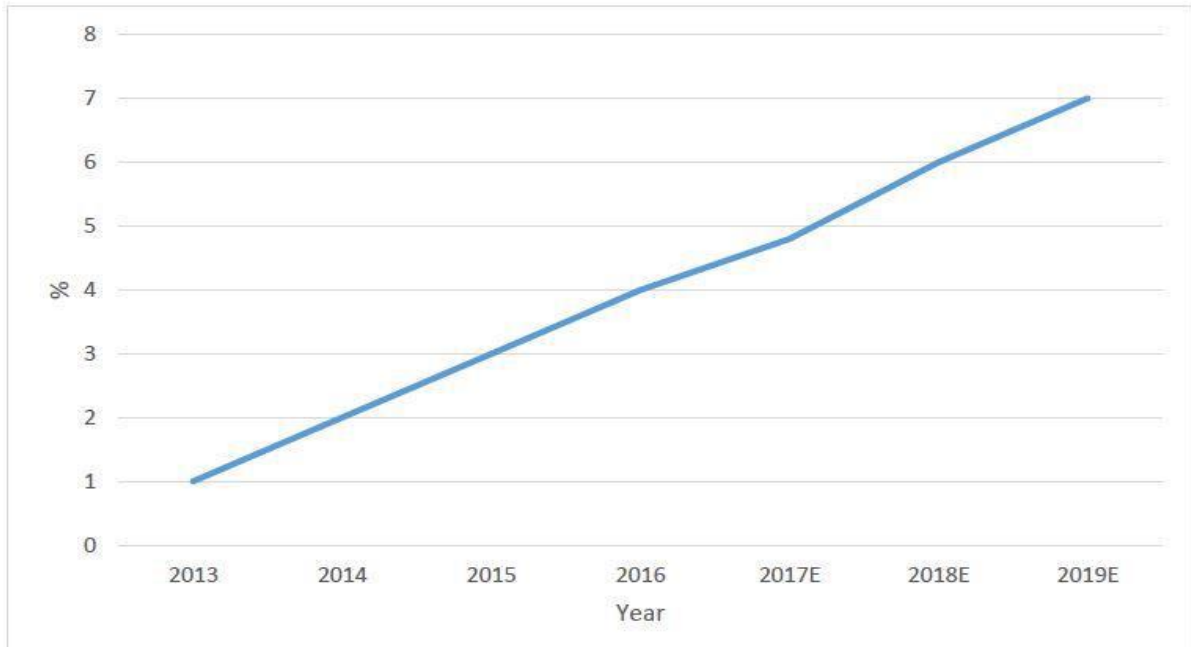


Figure 1.3.1 Showing Study on demand

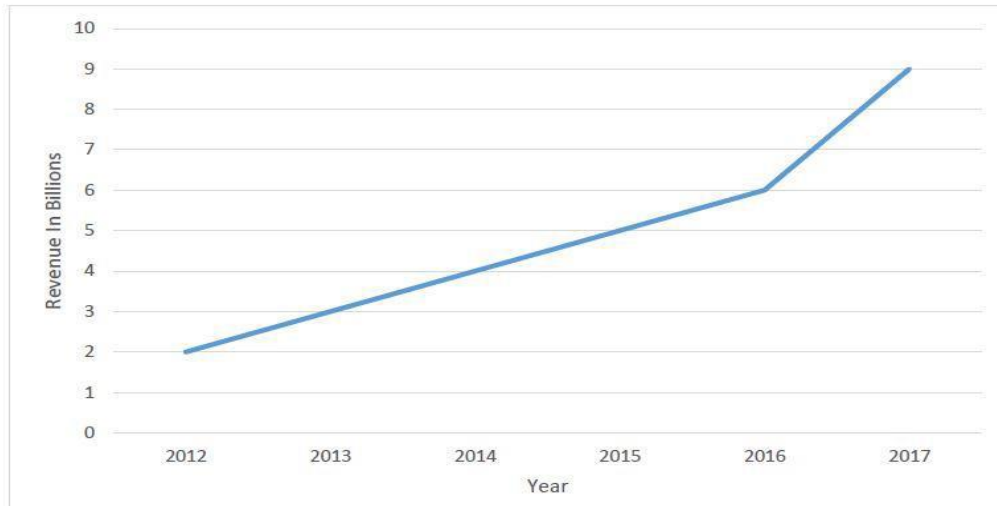


Figure 1.3.2 Showing market growth in US dollars

SMART HOMES means a home where every devices are connected to one another in a way that user can access and control the devices from wherever he/ she can. This way he/she can not only manage his/her home but also be SMART all the time about his/her family and taking care of it while working/sleeping means anytime and anywhere. Suppose you are in toilet and you forgot to switch off the TV then here comes your SMART phone through which you can control those TV and can switch it off while sitting in the toilet. According to author in [10] and [11] following challenges and technologies that empowers the SMART HOME is discussed.

1.3.1 CHALLENGES IN SMART HOMES.

1. Security, Privacy and Scalability.
2. Energy, Performance and Identity Management.
3. Risk assessment methods and Communication issues between devices.

1.3.2 TECHNOLOGIES THAT POWERS SMART HOMES.

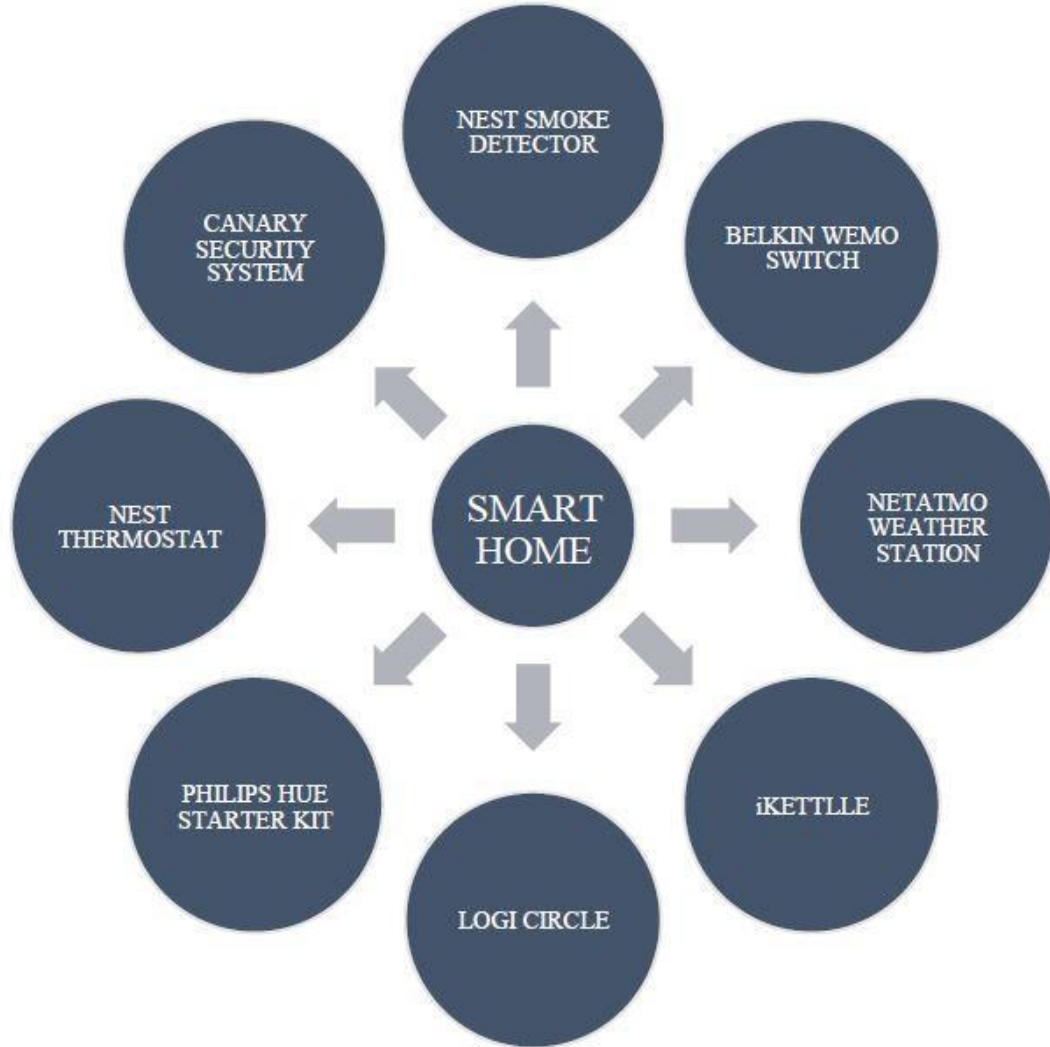


Figure 1.3.3 Showing technologies that empowers modern smart homes

CHAPTER 2

REVIEW OF LITERATURE

No	Title	Year	Author	Summary
1	Big Data Infrastructure for analyzing data generated by WSN	2014	Lidice Garcia Rios and Jose Alberto Inker Giges	This paper bring up what's massive information and wireless sensor network and the way an enormous information is gathered, hold on and analyzed with the assistance of wireless detector network. This paper uses hadoop as associate open supply framework for its implementation it uses arduino plates for sensors. This essentially deals with data processing that's done by stream processing module and analyzing of information that's done by map scale back model that works on distributed setting. The stream process was through with the assistance of storm, it's associate open supply tool that accommodates 2components spouts that browse the flow information and pass it to bolts that will operation over the information. Storm supports java, ruby,

				Python, JavaScript, Perl and php. The map scale back model helps the exploitation of multiprocessing over a distributed setting, it integrates functionalities that's map and scale back and abstract the complexities.
2	Execution Analysis Of BigData Gathering in WSN using an EM Based Clustering Scheme	2015	K. R. Ra. Babu, S. G J, P. Samuel, S. Jos	This paper deals with increasing the maximum utilization of sensor for data collection dealing with energy and data issues. The paper proposes an altered EM bunching calculation that arrangements with the issues. This paper depicts related work over grouping plan and system design and portrays their advantages and disadvantages. This paper uses Gaussian distribution for setting up of nodes in distributed environment and present an analysis in a tabular format of the results collected over the 8 mobile sinks and compares the results. This paper present graphical reports of its results. This paper deals with providing a good QOS and it propose the

				<p>further modification of em based method that can be extended to dynamic nodes as here static nodes are used. In this paper a distance property is used to reduce energy consumption and faster data processing. This paper introduces mobile sink based clustering. Movement of mobile sink, is set by using travelling salesman problem.</p>
3	<p>Would sensors be able to Collect Big Data? An Energy-Efficient BigData Gathering algorithm for WSN</p>	2017	S. Rani	<p>This paper tells about bdeg algorithm, which is an energy efficient algorithm that deals with real time data collection. During this multiple energy/routing algorithmic rule are mentioned and compared. During this paper the clustering issues are mentioned very well. The bdeg calculation utilizes beneficiary flag quality and connection quality marker. Bdeg calculation utilizes multihop strategy in which an information is transmitted through different expectations. Its demonstrates the issue of separation that causes vitality misfortune which is relative to</p>

				<p>the separation between hubs. This paper has given different directing calculations correlation with bdeg calculation. Grouping hubs are 10. The paper indicate encourage extent of lessening the aggregate separation for information transmission and will think of some as more parameters to enhance the bdeg.</p>
4	A Study on BigData Analytics, Challenges, Open Research Issues and Tools	2016	K. Ahmed	<p>This paper deals with challenges in bigdata analytics and open research issues. It defines 4v's in terms of velocity, veracity, volume and variety. The challenges discussed in this paper are data storage and analysis, knowledge discovery and computational, scalability and data visualization, information security. The open research issues are iot, cloud computing, bio inspired computing, quantum computing.</p>
5	BigData in Cloud Computing. features and issues	2016	P. C. Neves	<p>This paper talks the correlation between the large information and cloud computing is represented. The comparison</p>

				between nokia and redbus is made over why they moved to cloud and big data due to the benefits, the major issues shown are security privacy, heterogeneity, data governance and disaster recovery, scalability and elasticity, exaflop computing, QOS.
6	BigHealth Application System based on Health Internet of Things and BigData	2016	Y. Ma	This talks about big health based upon iot and big data. In this paper multiple application of big health has been described. The domain of big health covers health product, health service, and health real estate. Health finance, it consist of three layers. perception layer, transport layer, cloud service (support sub layer + application sub layer + machine interaction technology). Challenges discussed are versality between iot and hardware, creation of a framework and middleware services.
7	A Review on Big Data Analysis and Internet of Things	2016	U. Ahsan	In this paper the author talked about a review over the big data and iota and their challenges and solution that are currently

				presented. In this paper the description of iot is given like what is iot all about, also the author presents a layer architecture for iot. The research fields are security protocols, efficiency algorithm, massive scaling, architecture scheme, error handling capability, openness, and role of human also applications of iot. health care system, smart building, and connected vehicles.
8	Multiple BigData Processing Platforms	2016	B. R. Chang, H. F. Tsai, Y. S. Chang, C. F. H.	In this paper comparison of multiple data processing platform have been discussed that is hadoop, hive, impala, spark, hue. This paper provides a platform for selection appropriate model for appropriate processing of the data according to the need.
9	A study on iot	2016	P. T.	This paper on iot is defined in details. This paper classified as subdivision like evolution of iot, application, security and privacy concern and future trends. A generic design has been provided as; business layer, application layer,

				<p>middleware layer, network layer, perception layer. Some protocols square measure delineated that square measure used like message queue measurement transport helps in reducing the traffic, constraint application protocol that helps for M-2-M communication. Applications of iot noncommissioned as transportation, smart home, smart city, life style, retail, agriculture, sensible works, provide supply chain, emergency, user interaction, healthcare, culture and commercial enterprise, surroundings and energy.</p>
10	<p>A Case Study on the Trade Offs between Security, Scalability, and Efficiency in SmartHome Sensor Networks</p>	2016	T. R.	<p>This paper talks about security in terms of data integrity and data confidentiality. In this paper security is considered in terms of over wired and over wireless. In case of wired it talks about security and scalability and over wireless it talks only about security. It uses SSL algorithm for security between the sensors it measures the security in three parts using</p>

				timestamp and using NTP protocol.
11	On Privacy and Security Challenges in Smart Homes	2016	J. B.	The paper points privacy and security challenges for good homes. This paper talks concerning talks concerning 3 level service level, communication level, device level and also the security problems at these levels. Like at device level. resource constraints, headless nature, tamper resistant packages, communication level. heterogeneous protocols, dynamic characteristics, Service level. Longevity expectation. Some mitigation approaches are shown and future research field are discussed that are identity management, risk assessment methods, information flow control approaches, security management methods. In this privacy of the user is a major concern and should be respected.
12	Network IDS with numerous data processing techniques	2016	D. Gupta	Describes about network security and its goal to design a software that monitors the

				network activities. Focuses on confidentiality and integrity protection. This paper tells the use of linear regression and k-means clustering to automatically generate rules to fight the malicious activities. A comparative analysis has been made.
13	Data Mining with Big data	2014	X. Zuang	This paper talks about HACE theorem which tells about BIG DATA revolution and it proposes a BIG DATA processing model which involves various data mining perspective. In this they try to deal with the challenging issues in the data-driven model and also in the BIG DATA revolution. In this paper they have analyzed the challenges at data level, model level and system level.
14	Research of Wireless Sensor Network and Big Data Analysis based Continuous Pulse Monitoring System for Efficient Physical Training	2016	Hong Liang Yuan, Jun Wang, Qiang An, Shi Liang Li	This paper talks about how we can measure heart beat at abnormal conditions using zigbee and big data analytics, the pulse of individual is passed by sensors using zigbee to big data which provides the required solutions to those

				<p>symptoms received. For economical gathering of knowledge they need researched ikon electricity primarily based dynamic associate degreed continuous heart rate watching and an anti-jamming ways.</p>
15	Efficient assortment of massive information in Wireless sensing element Network	2016	S. V. Halde	<p>This paper talks about how we can collect efficiently the data in various applications of Wireless Sensor Network. This paper talks about BIG DATA and challenges in Wireless Sensor Network provides an efficient solution for solving the data gathering problem. This paper also provides a tabular result of the success of the technique researched using some routing protocols.</p>
16	Privacy Preserving Data Analytics for Smart Homes	2013	C. Rong	<p>In this paper the security has been implemented using IOT and big data. In this paper the identity of a person is stored in the form of hash values which is then used to identify the person identity the author suggested that the person's identity should be checked twice using generalization and suppression</p>

				and an approach has been proposed during complete data life cycle.
17	Towards a Model of Secure Smart Homes	2015	P. Davidsson	In this a paper a general model has been proposed through which we can see how security using IOT works in smart homes and A risk analysis has been down to find those associated threats in smart homes and various related work has been discussed like digital trace which helps in building user identity.
18	Internet of Things. Security and Privacy Issues and Possible Solution	2016	PISHVA	This paper tells us how Internet can become security threats using digital traces of user. This paper also provides countermeasures to solve those problems and to overcome the security breaches in the network of smart home and an appropriate security model has been proposed.
19	Study on Security in Internet of things challenges	2017	M. Sain	This paper talks about security breaches and IOT works till date and provides some future research work in security of smart homes. It talks security in three forms that is at

				communication level, application level and data level.
20	Network - Level Security Control in Smart Homes.	2015	V. Sivaraman	This paper talks about what are the different threats in security of smart homes, and how a network level security is better than other levels also, it suggest a model on how to implement the security in smart homes.
21	Security Requirements for Internet of Things (IoT)	2017	S. Jaiswal and D. Gupta	This paper talks about different security aspects of IOT with respect to E-health the security issues discussed are Data Freshness, Fault Tolerance, Self – Healing, Resilience, Authentication, Anonymity, Reliability, Trust. Also IOT healthcare security device security varies with IOT network security like speed of computation, scalability, communication channel, security updates. Acase study of Remote Patient Monitoring is presented in this paper
22	A Review of Smart Homes : Past, Present, and Future	2012	M. B. I. R.	The author presents an summary of previous sensible home analysis also because of the associated technologies. A snappy exchange on the building squares of sensible

				homes and their interrelationships is presented. Exceptional calculations from various fields and their noteworthiness are disclosed by their extent of utilization in brilliant homes. This paper also provides set of guide lines to the for future smart home developers etc.
23	Analytics of Residential Electrical Energy Profile	2017	S. Latif, A. Shabani, A. Esser, A. Martkovich	This paper talks about how analytics being used to describe the power consumption at circuit level can predict the reading of device level. Here MIT REED project data set has been taken which is used for analytics and predicting the trend of the uses. In this paper each home items has been grouped as a profile which is than used to analyze the trends in the usage.
24	Privacy-Preserving Data Analytics in Cloud-Based Smart Home with Community Hierarchy	2017	Y. T. Lee, W. H. Hsiao, Y.S. Lin, and S.C. T. Chou	In this paper the author is trying to optimize the performance of cloud based home automation using the community hierarchy model, They also have investigated the fleeting, spatial and between-family unit collaborations.

25	Privacy – by - Design Framework for Assessing IOT Applications and Platforms	2016	B. Nuseibeh	In this paper the author is trying to set guidelines for IOT to fulfill the privacy concerns and the security gaps.
26	An Efficient Privacy Protection Solution for Smart Home Application Platform	2016	G. Zhang	In this the author talked about privacy in smart homes, he proposed an efficient solution regarding security of the user while comparing the current solution with the proposed solutions, the measured criteria for comparison was security consisting of two attacks man-in-the-middle and external attacks and the response time, presented a graph of comparing the http, https, http-CA over response time.
27	A Novel Approach Based on Time Cluster for Activity Recognition of Daily Living in Smart Homes	2017	Y. Liu	In this paper author have taken temporal and spatial features of the elderly people and uses analytics in accordance with machine learning for the proposed work. In this paper they have taken time cluster and activity records as parameters and through that they are trying to help the elderly people in their daily routine works.

CHAPTER 3

SCOPE OF STUDY

According to author in [11] first smart home was having a kitchen computer which can cook many dishes, it was launched in 1969 and offered by Neiman Marcus and since that time many researcher and business man working together to provide a secure home to society and making money out of it for example Apple's Home Kit, Google's Weave/Brillo and Samsung's Smart Things. While doing business businessman tends to hide the security faults in SMART HOMES and if a researcher of their company present it to them they tell him/her to hide it. According to a recent study many/multiple threats have been found that's bugs in SMART HOMES as we are using the technologies but with new technologies new threats also emerges. Many researcher have research scope in this field that could be solved with the help of many mathematical and conceptual techniques like with the help of artificial neural network, big data, cloud computing and IoT. The study is done for making the SMART HOME more secure and detecting the threats that are vulnerable for us and our family it could be like a thief or anyone which harm our love ones. This study will help me in designing a security technique that will help me/anybody making my/their home more secure. SMART HOMES are the future homes for our upcoming generations. The scope of the study made in dissertation-II is to find a problem that could be removed/solved with the help of latest technologies till date using the IOT tools and techniques and. The IOT will help in making the home smart and DATA analytics will help in making the use of analytics to help in analyzing the data for the need. Many author have proposed many work for making the smart home secure. According to author in [10], he works on scalability and security of smart home and with the help of SMILE company which makes smart homes items, he presents a research work on how can we secure the SMART HOME and make it scalable means whenever we need some extra resources whether in terms of hardware or software his work will help in doing that. Furthermore many author have described how can we implement the DATA Analytics and IOT can be collaborated together to solve our day to day problems. According to author in [5] a research work is presented on finding the challenges that leads to security threats in SMART HOMES. He proposes some upcoming research areas in which upcoming researcher can work on making

the HOME more secure. The DATA Analytics concept has changed the world the way we know today. The author in [1] & [2] provides an algorithm on how we can make a sensor more energy efficient so that it can efficiently be used in SMART HOMES. In paper [25] author has prescribed a set of guidelines for future smart home developer or makers for due to systematic lags.

CHAPTER 4

OBJECTIVE OF STUDY

The objective of this study is to make our home smart and secure with the help of latest tools and technology. This study is done to find out the security problems in smart homes as these security threats are hidden by the company's while selling these home products but with the help of this study and study the problem in the security would be removed. This is done for the purpose of building a smart home more secure and more comfortable home. Smart Home is a new technology which helps us to make our home the way we want and like a professional. My primary focus is on the privacy issues in the SMART/ASTUTE HOME as every user likes to have his/her own privacy and dreams of a secure home. My objective is to find the loop holes in the security of the smart home and will aim toward resolving those problems.

PROPOSED RESEARCH METHODOLOGY

According to paper [27] the work flow is shown below.

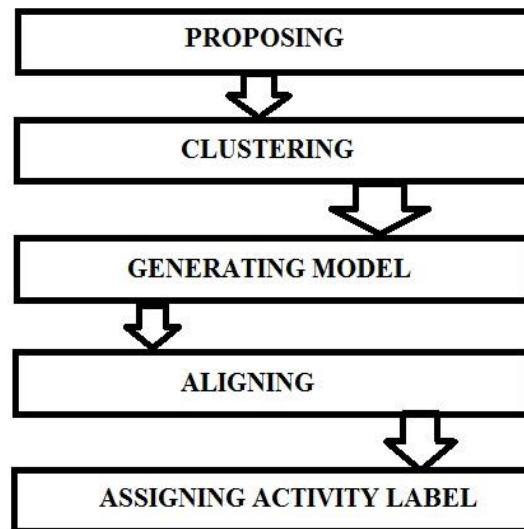


Figure 5.1 Showing the work flow of activity recognition

The first task Proposing used to generates a set of activity records are divided into training and test dataset. Clustering clusters the training data and test data. Generating Model generates a recognition model for each training cluster. Aligning a technique for optimal alignment between recognition models and the test cluster set. Assigning Activity Label, assigns an activity label to each activity record of the test set. According to it I have proposed a work plan show below.

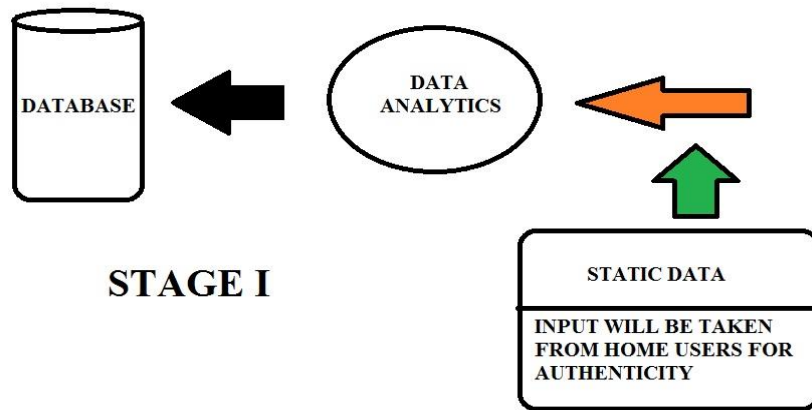


Figure 5.2 Showing the stage I process

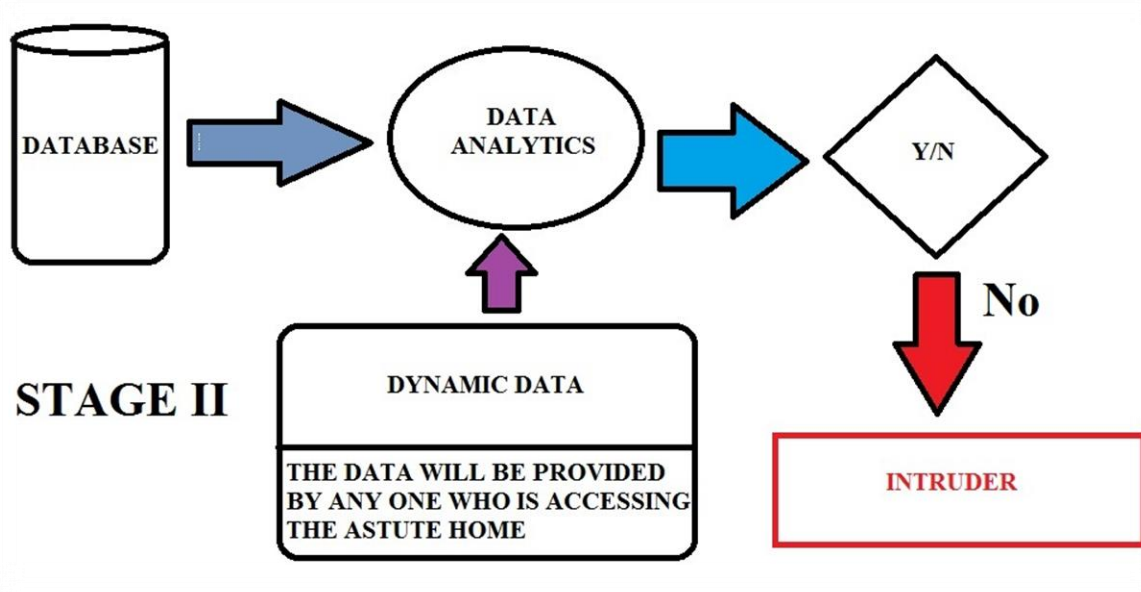


Figure 5.3 Showing the stage II process

In stage I the static data of the authentic user is stored in database which will be used to analyze the humans based upon their activity and timing pattern like using time cluster. In stage II the stored data will be matched with the dynamic data of the humans who will be accessing the astute homes if data not matched then the red alert we got our Intruder.

CHAPTER 6

SUMMARY AND CONCLUSION

I proposed an approach that can aid in solving the privacy issues and to detect the threat in smart/astute homes for maintaining the privacy of the user based upon my selected base paper that uses data analytics with the help of machine learning algorithms to detect the users daily routine and to aid in their daily work focuses the old age people as the target. Multiple researchers are using data analytics to solve the smart home privacy issues with the help of either machine learning or deep learning.

CHAPTER 7

EXPECTED OUTCOMES

Expected outcome of this study is to preserve the privacy by means of data analytics by analyzing the routines of users and then using the analyzed result to detect any misbehavior in the pattern of their routines whether the user accessing the smart/astute home components is authentic or not.

REFERENCES

- [1] L. G. Rios and J. A. I. Diguez, "Big Data Infrastructure for analyzing data generated by Wireless Sensor Networks," 2014 IEEE Int. Congr. Big Data, pp. 816 – 823, 2014.
- [2] S. G. J, S. Jose, R. B. Raman, and P. Samuel, "Performance Analysis of Big Data Gathering in Wireless Sensor Network Using an EM Based Clustering Scheme," 2015 Fifth Int. Conf. Adv. Comput. Commun., vol. i, pp. 109–113, 2015.
- [3] S. Rani, S. H. Ahmed, I. Member, R. Talwar, and J. Malhotra, "Can Sensors Collect Big Data ? An Energy Efficient Big Data Gathering Algorithm for WIRELESS SENSOR NETWORK," vol. XX, no. X, 2017.
- [4] D. P. and K. Ahmed, "A Study on Big Data Analytics. Challenges, Open Research Issues and Tools," Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 2, pp. 511–518, 2016.
- [5] P. C. Neves, B. Schmerl, J. Cámara, and J. Bernardino, "Big data in cloud computing. Features and issues," Int. Conf. Internet Things Big Data, IoTBD 2016, pp. 307–314, 2016.
- [6] Y. Ma, Y. Wang, J. Yang, Y. Miao, and W. Li, "Big Health Application System based on Health Internet of Things and Big Data," IEEE Access, vol. XX, no. c, pp. 1–1, 2016.
- [7] B. Ragothaman, S. Prabha, E. Jose, and B. Sarojini, "A Study on Big Data and Internet of Things," Avinashilingam - UGC Spons. Two Day Natl. Conf. Internet Things, pp. 174–179, 2016.
- [8] B. R. Chang, H. Tsai, Y. Chang, and C. Huang, "Multiple Big Data Processing Platforms," no. 3, pp. 207–211, 2016.
- [9] S. Kraijak and P. Tuwanut, "a Study on Iot Architectures, Protocols, Applications, Security, Privacy, Real-World."
- [10] T. Reichherzer, A. Mishra, E. Kalaimannan, and N. Wilde, "A Case Study on the Trade-Offs between Security, Scalability, and Efficiency in Smart Home Sensor Networks," pp. 222–225, 2016.

[11] J. Bugeja, A. Jacobsson, and P. Davidsson, “On Privacy and Security Challenges in Smart Connected Homes,” 2016.

[12] L. M. L. de Campos, R. C. L. de Oliveira, and M. Roisenberg, “Network Intrusion Detection System Using Data Mining,” 2012, vol. 311, pp. 104–113.

[13] X. Wu, X. Zhu, G. Wu, and W. Ding, “Data Mining With Big Data” no. Ibm 2012, 2013.

17

[14] H. Yuan, J. Wang, J. Liu, and S. Li, “Research of Zigbee and Big Data Analysis based Pulse Monitoring System for Efficient Physical Training 2 Zigbee based Pulse Monitoring and Analysis System,” vol. 80, no. December, pp. 2357–2361, 2016.

[15] S. V Halde, “Efficient Collection of Big data in WIRELESS SENSOR NETWORK.”

[16] A. Chakravorty, T. Wlodarczyk, and C. Rong, “Privacy Preserving Data Analytics for Smart Homes,” 2013 IEEE Secur. Priv. Work., pp. 23–27, 2013.

[17] A. Jacobsson and P. Davidsson, “Towards a model of privacy and security for smart homes,” IEEE World Forum Internet Things, WF-IoT 2015 - Proc., pp. 727–732, 2016.

[18] D. Pishva, “Internet of Things . Security and Privacy Issues and Possible Solution,” ICACT Trans. Adv. Commun. Technol., vol. 5, no. 2, pp. 797–808, 2016.

[19] M. Sain, Y. J. Kang, and H. J. Lee, “Study on Security in Internet of things, state of the art and challenges,” pp. 699–704, 2017.

[20] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, “Network-level security and privacy control for smart-home IoT devices,” 2015 IEEE 11th Int. Conf. Wirel. Mob. Comput. Netw. Commun. WiMob 2015, pp. 163–167, 2015.

[21] S. Jaiswal and D. Gupta, “Security Requirements for Internet of Things (IoT),” pp. 419–427.

[22] M. R. Alam, S. Member, M. B. I. Reaz, and M. A. M. Ali, “A Review of Smart Homes – Past , Present , and Future,” no. June 2015, 2012.

- [23] S. Latif, A. Shabani, A. Esser, and A. Martkovich, “Analaytics of Residential Electrical Energy Profile,” no. December 2006, pp. 3–6, 2017.
- [24] Y. Lee, W. Hsiao, Y. Lin, and S. T. Chou, “Privacy-Preserving Data Analytics in Cloud-Based Smart Home with Community Hierarchy,” vol. 63, no. 2, pp. 200–207, 2017.
- [25] C. Perera, C. McCormick, A. K. Bandara, B. A. Price, and B. Nuseibeh, “Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms,” 2016.
- [26] Y. Liu, G. Zhang, W. Chen, and X. Wang, “An Efficient Privacy Protection Solution for Smart Home Application Platform,” pp. 2281–2285, 2016.
- [27] Y. Liu, D. Ouyang, Y. Liu, R. Chen, “SS symmetry A Novel Approach Based on Time Cluster for Activity Recognition of Daily Living in Smart Homes.”

NB - Naive Bayesian

kNN - k-nearest neighbor

C4.5 - Clustering 4.5 Algorithm

RF - Random forest

HMM - Hidden Markov model