A Home Security Mechanism Using Paired Keys for Sensors in IoT

Arshdeep Kaur[1] Dr. Mahendra Kumar[2]
[2]Professor
[2]Department of Electronics & Communication Engineering
[1,2]Guru Kashi University, Talwandi Sabo, Bathinda, India

Abstract— The Internet of Things is considered as the fast emerging technology which will revolutionize many industries, homes, health centers, etc. IoT is compared to an ecosystem which consists of devices for computation, hardware, software, various physical entities, living beings interacting over network. IoT's pervasive and ubiquitous nature arises many challenges in its existence. This article represents current challenges that mostly exist in IoT. Here, applications of IoT are also discussed which proves the relevance of IoT in vast number of areas. This article also describes few research directions of IoT. The homes are informed by the home monitoring database centers about their breach reported on the basis by sending reports to their phone or their emails. The Home Security monitoring data is aggregated on the servers and various types of algorithms are used for the Home Security data analysis.

Key words: IoT, RFID, WSNs

I. INTRODUCTION

In next 10 years, it is predicted that plethora things will be connected to internet which will produce huge amount of data. IoT is compared to an ecosystem which consists of devices for computation, hardware, software, various physical entities, living beings interacting over network. IoT provides a platform that works seamlessly to connect various things and people for making our lives easier. This will offer distributed environment for various applications like smart cities, smart home, smart grid, and smart wearable's, etc.

Wireless sensor-based systems square measure at work nowadays, gathering home medical information that was ne'er before accessible for analysis and delivering care to folks for whom care wasn't antecedently accessible. In these ways in which, IoT-driven systems square measure creating it doable to radically scale back prices and improve breach by increasing the supply and quality of care. During this paper, we'll explore in larger depth the role of the IoT in supply, take a detailed inspect the technological aspects that build it a reality and examine the opportunities and challenges the IoT poses for care nowadays. We'll begin with Associate in Nursing introduction to the IoT— still a comparatively new concept—but one with a growing range of sensible applications across several industries.

II. LITERATURE REVIEW

1) Bluetooth based home automation system using cell phones:

In Bluetooth based home automation system the home appliances are connected to the Arduino BT board at input output ports using relay. The program of Arduino BT board is based on high level interactive C language of microcontrollers; the connection is made via Bluetooth. The password protection is provided so only authorized user is allowed to access the appliances. The Bluetooth connection is established between Arduino BT board and phone for wireless communication. In this system the python script is used and it can install on any of the Symbian OS environment, it is portable. One circuit is designed and implemented for receiving the feedback from the phone, which indicate the status of the device.

2) Zigbee based home automation system using cell phones:

To monitor and control the home appliances the system is designed and implemented using Zigbee. The device performance is record and store by network coordinators.

For this the Wi-Fi network is used, which uses the four switch port standard wireless ADSL modern router. The network SSID and security Wi-Fi parameter are preconfigured. The message for security purpose first process by the virtual home algorithm and when it is declared safe it is re-encrypted and forward to the real network device of the home. Over Zigbee network, Zigbee controller sent messages to the end. The safety and security of all messages that are received by the virtual home algorithm. To reduce the expense of the system and the intrusiveness of respective installation of the system Zigbee communication is helpful.

3) GSM based home automation system using cell phones:

Because of the mobile phone and GSM technology, the GSM based home automation is lure to research. The SMS based home automation, GPRS based home automation and dual tone multi frequency (DTMF) based home automation, these options we considered mainly for communication in GSM. Figure shows the logical diagram of working of A. Alheraish, it shows how the home sensors and devices interact with the home network and communicates through GSM and SIM (subscriber identity module). The system use transducer which convert machine function into electrical signals which goes into microcontroller. Physical qualities like sound, temperature and humidity into some other quantity like voltage using the sensors of the system. The microcontroller analysis all signal and convert them into command to understand by GSM module. Select appropriate communication method among SMS, GPRS and DTFC based on the command which received GSM module. Figure. Mobile-based home automation from the work of A. Alheraish

4) Wi-Fi based home automation system using cell phones:

Wi-Fi based home automation system mainly consist three modules, the server, the hardware interface module, and the software package. The figure shows the system model layout. Wi-Fi technology is used by server, and hardware Interface module to communicate with each other. The same technology uses to login to the server web based application. The server is connected to the internet, so remote users can access server web based application through the internet using compatible web browser. Software of the latest home automation system is split to server application software, and Microcontroller (Arduino) firmware. The Arduino software is built using C language, which comes with the

microcontroller itself using IDE. Arduino software is capable for gathering events from connected sensors, then applies action to actuators and preprogramed in the server. Another function is the reporting and recording of the history in the DB server . The server application software package , is a web based application built using asp.net. The server application software can be either accessed from internal network or internet. This can be done if the server has real IP on the internet using any internet navigator supporting asp.net technology. Server application software is culpable of, maintain the whole home automation system, setup, and configuration. The server uses database to keep log of home automation system components, we choose to use XML files to save system log. Fig. shows the layout of the proposed home automation system.

5) Home automation using RF module:

The important goal of Home Automation System is to build a home automation system using a RF controlled remote. Now technology is accelerating so homes are also getting smarter. Modern homes are deliberately relocating from current l switches to centralized control system, containing RF controlled switches. Today traditional wall switches situated in various parts of the home makes it laborious t for the end user to go near them to control and operate. Even further it turns into more problematic for the old persons or physically handicapped people to do so. Home Automation using remote implements an easier system(solution) with RF technology. In order to accomplish this, a RF remote is combined to the microcontroller on transmitter side that sends ON/OFF signals to the receiver where devices are connected. By operating the stated remote switch on the transmitter, the loads can be turned ON/OFF globally using wireless technology.

6) Home automation using Android ADK:

The devices of home are associate to the ADK and the Connection is established between the Android device and ADK. The devices of house are link to the input/output ports of the board (EMBEDDED SYSTEM) and their current situation will have passed to the ADK. The microcontroller board (Arduino ADK) is based on the ATmega2560. It has a USB host connection to associate with Android based phones, and that is based on the MAX3421e IC. The two important features of Android Open Accessory Protocol 2.0(AOAP) are as follows: It has audio output that is from the Android device to the component and it also support for the component serves as one or more Human Interface Devices (HID) to the Android device. This paper depends upon Android and Arduino platform in which both are FOSS(Free Open Source Software). Including motion sensors for safety systems will detect an unauthorized action and it will automatically notice the user through cell phone or the security system.

7) Cloud Based home automation system:

Home Automation using cloud based system focuses on design and implementation of home gateway to collect data about data from home appliances and then send to the cloud-based data server to get store on Hadoop Distributed File System, it is process using MapReduce and use to implement a monitoring tasks to Remote user Presently home Automation System is persistently developing its resilience by assimilating the current characteristics which gratify the rising interest of the people. This paper presents the design and development of home automation system that use the cloud computing as service. The current system consists of three important units: the first part is cloud server, handle and controls the data and information of client and users and the status of devices the hardware interface module is the second part which implement the relevant connection to the actuators and sensing devices which give the physical service. Last part is Home Server, which construct the hardware device and gives the user interface. This paper focus to build the web services using cloud which is need for security and storage and availability of the data. The current system is cost efficient, reliable and comfortable which also gives a secured home automation system for entire family.

III. IoT MULTI-LAYER ARCHITECTURE:

Interaction: This layer provides interaction with the user by providing them useful output which is provided to them in very interactive manner.
Application: This layer provides satisfaction to users by providing them proper service like security, data flow management etc.
Networks: This layer will provide support to the data being transferred through wired or wireless connection.
Sensor / Actuator: At this layer, sensor will sense the data from hardware devices and all the processed data will be passed to actuator.

IV. IMPORTANT ASPECTS OF IoT:

A. Radio Frequency Identification (RFID):

Through this technology, various physical entities that are part of the system are assigned unique identification number. Things that are attached to the system are known in the network by RFID tags only.

B. Wireless Sensor Networks:

WSN's interact with the system's components using RFID. RFID tags are actually used in the WSN to better track the things. WSN's also consist of sensors, computing elements, communication channel, actuators and some powered devices. There are various challenges in WSN like fault performance, scalability, production cost, operation environment, quality of service, latency, data compression, data aggregation etc.

C. Addressing:

RFID tags and wireless technology makes it easy for the system to identify the things. But this addressing will be done by IPv4 addressing system. As more and more devices will be connected to the system and need of addressing will increase then IPv6 addressing system will come into play.

D. Middleware:

As different things are to be connected over the network, Middleware provides set of programs through which various things will be connected to each other and they will be able to communicate via message exchange also. There are various companies like WSO2, Mulesoft, RedHat and Oracle that provide service of IoT middleware.

V. MAIN CHALLENGES OF IOT:

Technology: Huge amount of data is generated by the things connected to the smart devices. Underlying networks play very important role in this. To manage this data various models like edge computing model, fog computing model etc. will provide assistance to the networks by reducing the flow of data.

A. Artificial Intelligence:

Incorporating human behavior in the system is very challenging. It is very difficult to predict the nature of the human. What type of input to use, output variables should be there, equations should be used, selecting testing statements is very problematic.

B. Security and privacy:

Security, trust, authentication, message integrity and confidentiality are the few aspects that are very important when communication is done between the devices that are part of the system. Proper policies should be there to provide access to guarantee services as these devices are working wirelessly.

C. Energy Efficiency:

Different types of devices are used in the system that is using IoT as technology; it is very difficult to compute energy generated by different devices. Solving problem of robustness and fault tolerance is very important in this technology.

D. Common standard of IoT devices:

Different IoT devices that are part of the system are manufactured by different number of manufacturers. So, it is very important that common standards should exist for easy exchange of communication between the countless devices that are part of the system.

E. Data collection and protection:

Data being collected by the system is very helpful for us in taking smart decisions. Collection of correct information makes security and privacy concerns very crucial. Secure transfer of data, unauthorized interference and misuse of data across the networks is very important for extracting right data and then making right decisions from the data.

F. Big Data:

As we are connecting more of our devices to the system, chances of data intrusion are also most likely to increase. It is believed that 50 billion of devices will be connected with in next 10 years so data privacy is very challenging as chances of data theft or leaking are more.

VI. IOT APPLICATIONS:

A. Sensing and sharing of location:

The IoT system can collect information using GPS of the IoT terminals. Its basic applications includes tracking of mobile assets, management of smart fleets, managing information that is collected from traffic system.

B. Sensing of environment:

IoT devices can sense various physical and chemical aspects of environment. Data sensed by these systems can be used in monitoring forests, volcanoes, and factory. This information can also be used for sensing patient's body also.

C. Remote Control:

Application control and disaster recovery are the applications of IoT which facilitates people a lot. This information can save many lives.

D. Ad Hoc Networking:

In the vehicular networks, the data collected from this can be very beneficial for managing vehicles. This can make roads very self-organized.

E. Smart City:

Environment monitoring, safety, food traceability, smart agriculture are the few areas that are being used as most active applications of IoT. These devices can be monitored and controlled through a computer, tablet or Smartphone.

F. Big data and Business analytics:

IoT can be merged with already existing business analytics tool which can provide good source of information for enhancing business revenues, providing customer satisfaction.

G. E-health care:

Data analytics provided by sensing human body is very helpful in monitoring one's health sitting at a distance. Various things are sensed using body sensor networks which is reducing visits to emergency rooms and frequent hospital visits.

H. Smart Grid:

IoT can provide facilitates like smart power monitoring, smart scheduling, dispatching automatic power, reading remote meters. This can help in energy saving and power management a lot.

VII. RESEARCH DIRECTIONS

A. Protocol's security in IoT layers:

Creating secure protocols in the IoT's network layer and transport layer is very crucial. Security in IPsec can provide authentication, protection, confidentiality and message and data integrity. These protocols must be implemented in encapsulated security protocol and authentication header.

B. Privacy preservation in IoT:

Secure, trust and privacy are the main aspects of privacy preservation in IoT. Some protocols are required for uniquely and securely identifying all the devices of the system. Privacy preservation becomes very important when data is passed from one system to another system.

C. Wireless Sensor Networks (WSNs):

Wireless Sensor Networks play very important role in IoT. Its research directions include choosing correct node, analyzing traffic, message exchange, various types of attacks,

malfunctioning of nodes. Lot of work is done on this area as WSNs are the backbone of IoT.

Algorithm 1: Proposed Cloud based Multi-Level Authentication Protocol

1. The user nodes powers up
2. The user node initiates the data propagation process
3. The user node sends data channel request to cloud platform data management server
4. The cloud platform data management server sends a verification key
5. The user node reply with the corresponding verification acknowledgement key
6. The cloud platform server verifies the authentication key by matching the authentication against the verification key
7. If key verification successful
   a. The user node is updated with an acknowledgement to send the data and start the time counter for secure channel period
8. Else
   a. The user node denies the data connection.
9. When the secure channel period time counter expires
   a. The cloud platform server resends the verification key to the user node SN
   b. The user node reply with the corresponding verification acknowledgement key
   c. The cloud platform server verifies the authentication key by matching the authentication against the verification key
   d. If key verification successful
      i. The user node is updated with an acknowledgement to send the data and start the time counter for secure channel period
   e. Else
      i. The user node is denied the data connection.
10. Repeat the step 9 when the data communication is running

Algorithm 2: Main Secure Transmission Algorithm

1. Collect ECG signal and compute the Heart Beat using the latter QRS detection algorithm
2. Home Sensor encrypts the Heart Beat Information using the AES algorithm
3. For the initial stage authentication, the Home Sensor sends the request for data transmission approval to the cloud Home Security record management service (CHRMS), which includes the Home Sensor ID, PIN and Home ID.
   a. If CHRMS approves the Home Sensor ID and Home ID combination along with PIN
      i. It sends the approval accepted acknowledgement (APACA)
   b. Otherwise
      i. It refuses the communication request.
4. If Home Sensor receives the APACA, it sends the encrypted home information to the server
5. Server decrypts the home information and updates the appropriate record.
6. After the authorized session time expires, the CHRMS sends the question key to the Home Sensor.
7. Home Sensor replies with appropriate answer key
8. CHRMS verifies the key and re-authorize the communication if key math successful and terminate otherwise.

VIII. Results and Discussion

A. General Simulation Scenario

The proposed solution has been implemented using MATLAB simulator 2013. The implementation has been done using the numbers of homes (or users). The proposed model has been designed for the recording of the data of 100 homes in the online portal.

Parameter	Existing Technique	Proposed Technique
Number of sensors (Homes)	1-100	1-100
Packet size	36 Byte	16 Byte
Acknowledgment size	12 Byte	4 Byte
Private, Public keys length	160 bits(RSA)	128+32 (160 bits)
Symmetric key length	128 bits	128 bits (AES)

Table 8.1: Simulation scenario

B. Result Analysis

Performance metrics are measurement standards for calculating the efficiency, quality, performance or progress of a product.Selection of correct metrics in evaluating the performance of the key management technique is vital to the results and validation of the evaluation. The nodes have been deployed in the random function without the overlapping factor avoidance. To overcome the nearest covariance to the sensor topology, the random deployment factor has been used. The effectiveness of proposed scheme has been analyzed through the following parameters:

1) Key Generation Time

The time taken by key management scheme to generate the key table of the given size is called the key generation time. The key generation time is responsible for the delay in the neighbor formation process, which results in the delayed sensor network startup.

Key Generation Time = Finish Time – Start Time

Eq. (4.1)

The key generation time is the highest among the verification and transfer time because of the random factor calculation in the proposed model. The key generation is the one time process as shown in Figure 4.1 and takes approximately 4 second during the initial phase of the communication in the Home Security sensor nodes. An average of 4 seconds is taken each time to generate key table as derived from Figure 8.2.

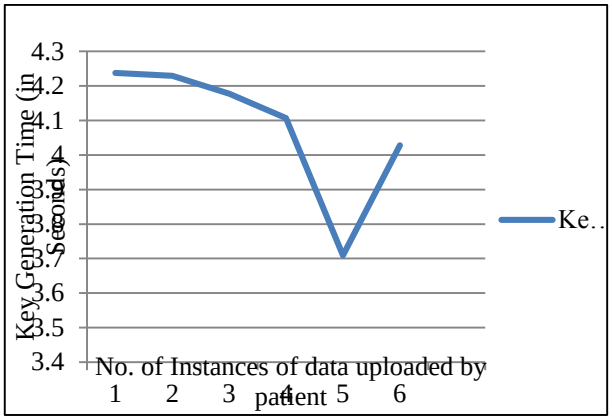

Figure 8.1: Key generation time taken through various instances.

2) Key Transmission and Verification Time

The total time taken by the cloud nodes for key sharing and key verification is termed as the key transmission and verification time. The key transmission and verification time (KTVT) adds the overhead to the communication channel between the two nodes. Lower key transmission and verification time produces the better results and adds the lower amount of overhead to the communication channel.

$KTVT = \sum_{k=1}^{N}[Tx(St) - Rx(St)] + [Rx(St) - Tx(St)] + \int_{t=1}^{N} Fx(RxK == TxK)$ Eq. (4.2)

Where, T_X = transmitting end

Rx = receiver's end

S = key index

t = time

R_xK = receiver's key

T_xK = transmitter's key.

It means the key is being exchanged every second between the two ends of the communication link in the sensor node network as shown in Figure 8.2. Key transfer time is the total time for transferring keys during authentication and verification time is for authenticating the keys. Lesser will be the transfer and verification time, lesser will be the data delay and faster will be the communication and transfer process. This key transfer and verification takes place between the cloud server and ECG sensing Home Sensor device. If the verification fails during authentication then connection request will be terminated and the system requires making a new connection request from the beginning. Key generation is one time process but key transfer and verification takes place 11 times in the whole request. It is depicted from Figure 4.3 that proposed model has taken the maximum of 2.04 seconds for the key transfer where the lowest value remains at the 2.01 seconds, whereas the key verification time has been recorded lowest at 2.07 seconds and highest at 2.15 seconds.

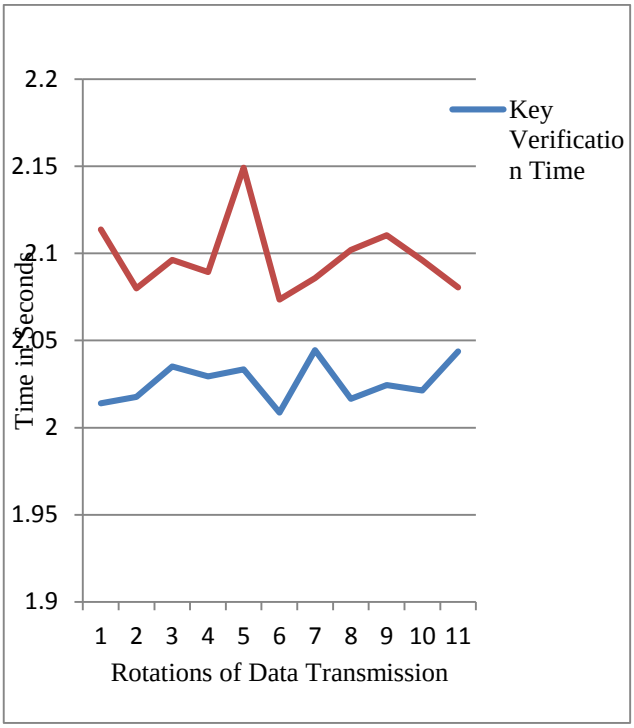

Figure 4.2: Line Graph representation of key transfer and verification time

3) Data Transmission Time

The transmission time is the time taken to upload the data to the server. It is the time taken from first bit of digital home data to last bit of data being transmitted to cloud server from Home Sensor.

Packet transmission time = Packet size / Bit rate Eq. (4.3)

The proposed model has been designed to send the home data individually to the cloud based Home Security record management service. The proposed model as shown in Figure 8.4 has been recorded with the highest transmission time of nearly .67 seconds and lowest at nearly 0.31 seconds. The curve in Figure 8.3 shows a gradual reduction in transmission time with the rise in data upload index.

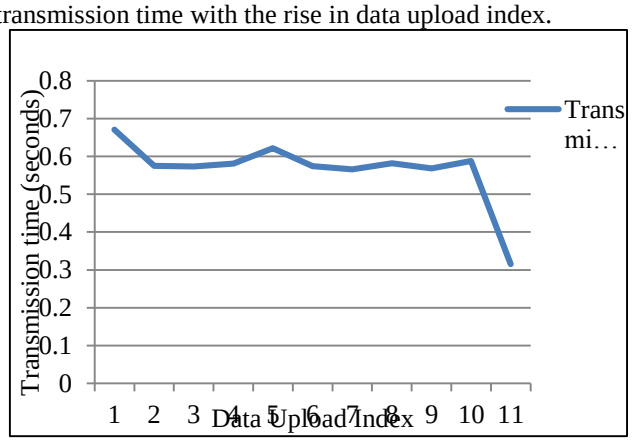

Figure 4.3: Time taken for data transmission between the client and server

4) Entropy

Entropy is the parameter, which measures the uniqueness between the keys generated to form a key table. The uniqueness is inversely proportional to the risk of guessing or key replication attacks on the communication channels. Entropy can be calculated using Eq. (4.4)

$\Delta S = \int \frac{dQ}{T}$ Eq. (4.4)

Where, T = number of selected keys
dQ = number of remaining keys produced to in the table for the key selection
S = absolute entropy.

Figure 4.4 shows the entropy comparison of the proposed scheme using the ECG signal for the home breach monitoring. The entropy of the key table in the proposed model as shown in Figure 4.5 is averaging nearly at 2.0, which defines the high uniqueness of the keys among the key table in the proposed model.

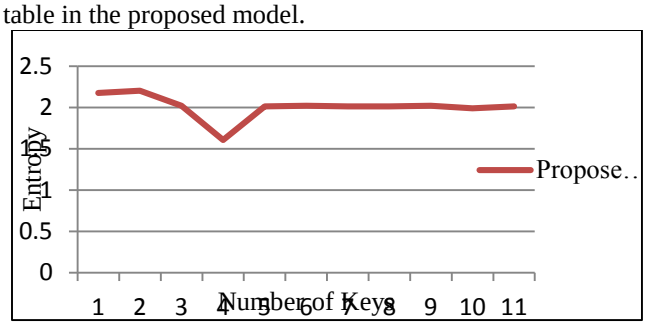

Figure 8.4: Entropy comparison of keys generated for testing subjects

5) Probability of Key Connectivity

The key connectivity is the performance metric which signifies the probability of the connection generation using the given key model. The probability key connectivity, computed using Eq. (4.5) indicates the level of connectivity and connection down time due to key connectivity. The key failure is the major concern behind the dis-connectivity caused by key management models.

$P_{conn} = PC * \oint_{n=1}^{K} N * (\frac{Sxd}{Nxd})$ Eq. (4.5)

Where, N = number of transaction or key events occurred earlier
S_{xd} = successful number of key exchange
N_{xd} = total number of key exchange
PC = probability constant.

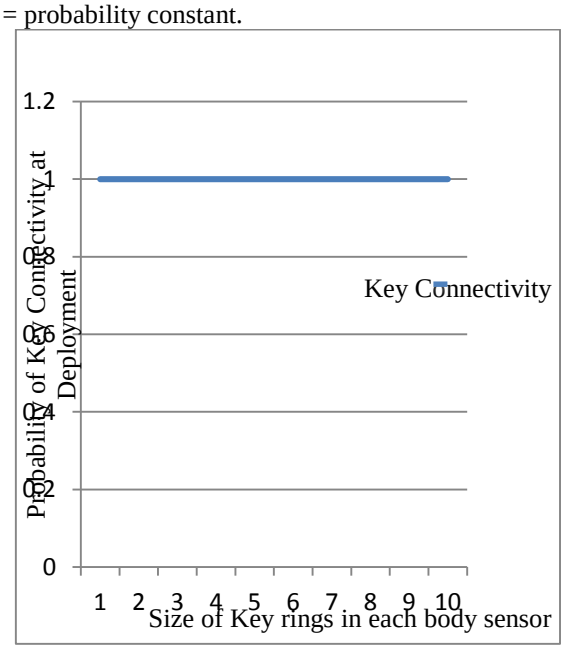

Figure 4.5: Calculation of key connectivity probability at deployment

The probability of key connectivity has been recorded at 1 for all of the data or key transactions in Figure 4.4. The key failure is the major concern behind the dis-connectivity caused by key management models. The proposed model keeps the highest efficiency in the case of key connectivity.

6) Probability of Key Exposure

The probability (P) of key exposure signifies the probability of the keys being exposed to the hackers during the communications. The key exposure may cause the long-term information leakage affect to the home specific Home Security communications. The less is the number of keys, the higher is the probability of the key exposure.

$P_{Exposure} = \sum_{n=1}^{K} N * Hx\ (\frac{NHx}{Nxt+Nxf})$ Eq. (8.6)

Where, N = number of transactions or key events occurred
H_x = total number of hacking attempts
NH_x = number of compromised keys
N_{xf} = number of failed keys
N_{xt} = current index volume of key data.

The proposed model key exposure probability, as shown in Figure 8.6, is falling down with increase in number of keys exchanged. The proposed model is using the cryptographic key exchange between the Home Sensor and cloud Home Security system. The decreasing probability of key exposure as shown in Figure 8.6 is indicating the effectiveness of the proposed key exchange.

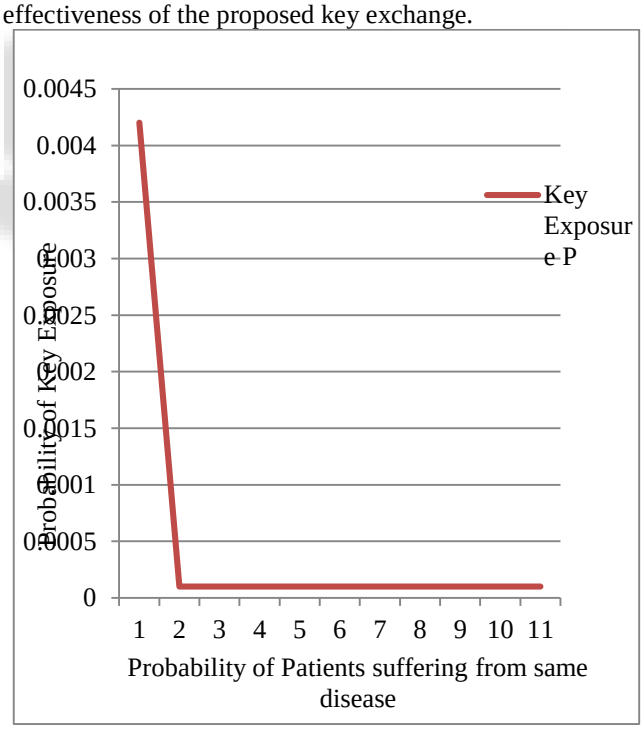

Figure 8.6: Calculation of key exposure probability

7) Probability of Key Selection

The probability of key selection is the parameter to calculate the chances of a key being selected from the key table. The probability should be lower in order to reduce the redundancy of the keys being propagated between the two nodes. The probability of the key selection can be defined as following:

$P_{sel} = \sum_{k=1}^{N} \frac{P(A \cap B)}{P(A)}$ Eq. (8.7)

Where, P_{sel} = probability of key selection
P =probability

A = total key cases
B = favorable number of key selection cases

The probability of key selection in the figure 8.7 is the probability calculated to find the chances of an individual key being selected for the key exchange process. The probability curve begins from the maximum value of 1 to less than 0.2 in the last transaction as shown in Figure 8.7. The low probability of a key being selected during each transaction shows the robustness of the proposed key exchange model. The average key selection probability has been calculated at 0.2929, whereas the median value defines the averaging factor at 0.2, which is very much adaptable for a balanced and good key management scheme.

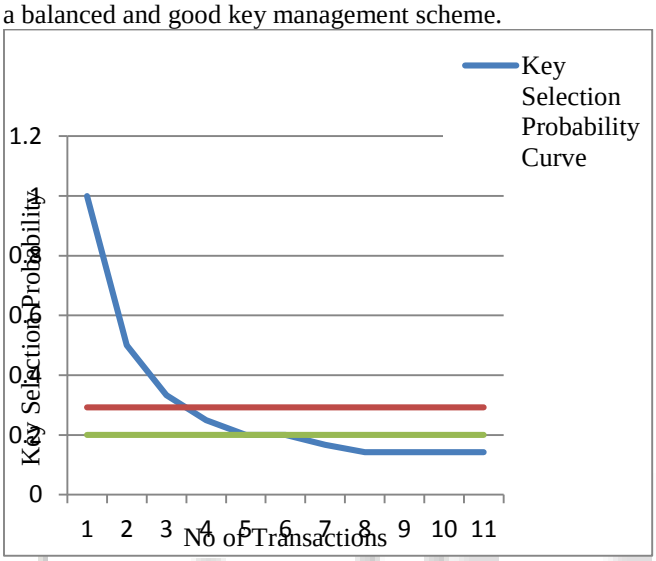

Figure 8.7: Calculation of Key selection probability

8) Memory Usage

Memory usage is the parameter to indicate the memory allocation for the runtime resources of the key management applications, computed using Eq. (8.8). The memory usage or memory size is indicated by the allocated memory before and after the execution of the key management scheme.

Memory Usage= Ma-Mb Eq. (8.8)

Where, Ma = memory usage after processing

Mb = memory usage before processing.

The memory usage has been recorded in the bits. The average memory usage has been recorded at almost 9 Mb (8.46 Mb) of the memory to run the whole key exchange process and median memory usage is 9.00 Mb.

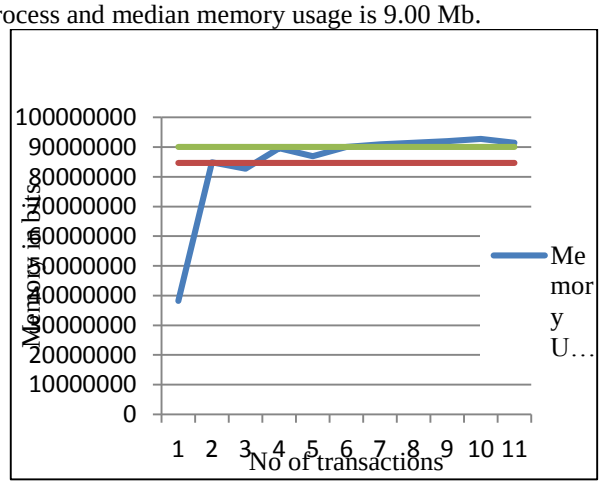

Figure 8.8: Memory consumption by the proposed scheme in the Home Security network

IX. Conclusion

The implementation of IoT in various spheres of life will improve our quality of life. As IoT system has the ability of extensions and can be enhanced very easily that is why they can provide services in many fields like security, education, logistics, healthcare etc. There also exists need to work upon various challenges of IoT to improve its applications. Its ubiquitous nature will increase its applicability in various fields. Its research directions can also provide us various areas where its work can be extended and make it deployable worldwide.

References

[1] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant and K. Mankodiy,2018:Towards fog-driven IoT eHealth : Promises and challenges of IoT in medicine and healthcare. *Future Generation Computer Systems*, *78*, pp.659-676.

[2] S. Upadhyay, " ONGOING CHALLENGES AND RESEARCH OPPORTUNITIES IN INTERNET OF THINGS (IOT)", In International Journal of Engineering Technologies and Management Research, *Vol.5 (Iss.2: SE): February, 2018*, ISSN: 2454-1907 .

[3] Lee and K. Lee, 2015. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), pp.431-440.

[4] D. Bandyopadhyay and J. Sen, 2011. Internet of things: Applications and challenges in technology and standardization. *Wireless personal communications*, *58*(1), pp.49-69.

[5] S. Chen,H. Xu, D. Liu, B. Hu, and H. Wan, 2014. A vision of IoT: Applications, challenges, and opportunities with china perspective. *IEEE Internet of Things journal*, *1*(4), pp.349-359.

[6] Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash 2015. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, *17*(4), pp.2347-2376.

[7] K.K.Venkatasubramanian, A. Banerje, & S. K. Gupta, (2008, April). EKG-based key agreement in body sensor networks. In INFOCOM Workshops 2008, IEEE (pp. 1-6). IEEE

[8] J . Wan, C . Zou, S . Ullah, C . F . Lai, M . Zhou, & X . Wang (2013). Cloud-enabled wireless body area networks for pervasive Home Security. IEEE Network,27(5), 56-61.

[9] H. Wang, D. Peng, W. Wang, H. Sharif, H.H.Chen, & A. Khoynezhad, (2010). Resource-aware secure ECG Home Security monitoring through body sensor networks. Wireless Communications, IEEE, 17(1), 12-19.

