Authentication, Authorization, and Access Control using Voice Biometric in Smart Homes

By

Hasnain Kabir

00000318553

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of PhD in Information Security

July 2022

Thesis Acceptance Certificate

Certified that final copy of MS Thesis written by **Syed Hasnain Kabir** Registration No. **00000318553** of **Military College of Signals** has been vetted by undersigned, found complete in all respects as per NUST Statutes/ Regulations/ MS Policy, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members and local evaluators of the scholar have also been incorporated in the said thesis.

Signature: ___________________________________

Name of Supervisor: **AP Dr. Fawad Khan**

Date: ____ Jul 2022

Signature (HOD): ______________________________

Date: _______________________________________

Signature (Dean/Principal) ______________________

Date: _______________________________________

Declaration

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

Dedication

“In the name of Allah, the most Beneficent, the most Merciful"

I dedicate this thesis to my mother, wife, and teachers who supported me each step of the way.

Acknowledgments

First and foremost, I want to convey my heartfelt thanks to supervisor, assistant professor Dr. Fawad Khan, for his valuable input, unwavering support and advice during my thesis work. I am extremely thankful for his valuable remarks and suggestions for improving my thesis work.

I'd want to express my heartfelt gratitude to everyone who has helped me resolve my doubts and provided moral support during this master's thesis project. Dr. Faisal Amjad, Dr. Shahzaib Tahir and Dr. Shibli Nisar, in particular, for their insightful thoughts and kind input.

At the end, I am grateful for unwavering support and encouragement of my family for allowing me to continue on this journey. Indirect assistance of my family was a major contribution to my thesis.

Abstract

Progressions in information and communication technologies (ICT) have led to the emergence of Internet of Things (IoT) and became one of the most powerful communication paradigms of the 21st century. A smart home or home automation technology is a combination of different IoT devices for comfort of human and security of homes through a remote interface using wireless transmission, thereby enabling users to control and monitor from a browser or smartphone. Therefore, access control must be strengthened in smart homes to protect the security and privacy aspects which can be achieved by implementing authentication and authorization mechanisms. The existing research on the subject suggests till now, multiple individual techniques like passwords, Pin code etc have been employed to cater for access control, however, the low processing and power requirement to these systems make these systems vulnerable to different type of attacks. A system needs to be crafted to enhance the element of security and user friendly usability in a smart home. Our purposed scheme, ***Authentication, Authorization, and Access Control using Voice Biometric in Smart Homes*** is an implementation of fingerprint and voice recognition together for authentication, authorization and access control. The main focus of this scheme is on access control in smart homes using voice biometric authentication along with mitigation of threats due to unauthorized access and non authentication of a user which includes Masquerade Attacks, Replay Attacks, Denial-of-Service Attacks, Spoofing attacks, Man-in-the-middle attacks and Impersonation attacks. We have used BAN logic analysis to validate the scheme's correctness. This scheme prevents system from replay attack by adding time stamp in request message. The performance analysis i-e computation cost and communication cost comparisons of our scheme with other schemes shows that efficiency of proposed scheme is more than other schemes.

Keywords: Internet of Things, Smart Homes, Access control, authentication, authorization, voice recognition, fingerprint.

Table of Contents

List of Figures

List of Tables

Abbreviations

IoT	-	Internet of Things
ICT	-	Information and Communication Technologies
DoS	-	Denial-of-Service
MITM	-	Man-in-the middle
BAN Logic	-	Burrows–Abadi–Needham Logic
CPSA	-	Cryptographic Protocol Shapes Analyzer
ISM	-	Information Security Management
DH	-	Diffie-Hellman
BIOFIHS	-	Biometrics Fingerprint for Home Security
GUI	-	Graphic User Interface
ASV	-	Automatic Speaker Verification
LPCCs	-	Linear Prediction Cepstral Coefficients
MFCCs	-	Mel-Frequency Cepstral Coefficients
DTW	-	Dynamic Time Warping
SVM	-	Support Vector Machine

Chapter 1

Introduction

1.1 Background

Progressions in information and communication technologies (ICT) have led to the emergence of Internet of Things (IoT) and became one of the most powerful communication paradigms of the 21st century. In IoT domain, due to strong communication and computing capabilities of devices which we use in our daily life become part of the internet. IoT provide smooth interactions between different types of devices which include sensor, security cameras, home appliances and much more [1].

A smart home or home automation technology is a combination of different IoT devices for comfort of human (which includes automation of lights, heaters, air conditioning, windows, speakers, cooking kits and various other home appliances) and security of homes (which includes monitoring of cameras, door locks, alarms system, motion Sensors and various other devices) through a remote interface using wireless transmission, thereby enabling users to control and monitor from a browser or smartphone. Therefore, access control must be strengthened in smart homes to protect the security and privacy aspects which can be achieved by implementing authentication and authorization mechanisms.

Authentication is a process in which identity of a user is verified by some mechanism to grant access to resources in an information system. There exist several authentication mechanisms like Passwords, PIN code, RF identification and biometric. A user is either who they claim to be or someone else. Thus the output of the authentication process is either a yes or no. Authorization is a process that user (who is already authenticated) is allowed to have access to a resource, it determines what a user is and to what level of resource he is authorized to access? Access control is a process that prevents the user from accessing anything that he is not authorized to access. Basically, access control enforces authorization.

Let’s consider a smart home scenario with following smart devices, smart TV, lights, AC, fan, washing machine, microwave oven and security cameras are installed in it. Smart homes have two types of users, adult and child. Both users want to operate smart devices and gets authenticated and authorized to operate smart device, but here we want adult can use all smart devices installed in smart home and child can operate limited devices except washing machine and microwave oven. So here access control policy will be implemented and if child will try to operate a washing machine or microwave oven, system will deny the command and he will unable to use it.

Among all available authentication mechanisms, biometric is more reliable authentication mechanisms but to make it more powerful it must be used with a combination of two factor authentication like fingerprint authentication and passwords or OTP, PIN etc.

1.2 Problem Statement

1.2.1 Problem Description

With the fast pace of advancement in IoT technologies, the fusion of smart devices to build smart homes has been on the rise. There are numerous categories of devices which can make our lives easier and better at home e.g climate control, smart kitchen, entry exit systems and many more. This gives rise to the problem of authentic, authorize user and access control, i-e who can control what? The existing research on the subject suggests till now, multiple individual techniques like passwords, Pin code etc have been employed to cater for access control, however, the low processing and power requirement to these systems make these systems vulnerable to different type of attacks. A system needs to be crafted to enhance the element of security and user friendly usability in a smart home.

1.2.2 Research Question

Is it possible to have a comprehensive mechanism that can simultaneously authenticate, authorize and manage access levels of different users by making use of a multi factor authentication system using passwords and biometrics?

1.2.3 Purpose/ Research Objectives

The purpose of this research is to

- Analyzing already implemented user authentication, authorization & access control scheme in IoT based smart homes.
- Proposing a scheme for **Authentication, Authorization, and Access Control using Voice Biometric in Smart homes**.
- Implementation of fingerprint and voice recognition together for authentication, authorization and access control.
- Mitigate threats (Masquerade Attacks, Impersonation attacks, Denial-of-Service Attacks, Spoofing attacks, Man-in-the-middle attacks and Replay Attacks) due to unauthorized access and non authentication of a user.

The area of application of this research work includes:

- Smart Homes
- Health Industry
- Transport Industry
- Military and Critical Installations

- Government and Private Organizations using Information and Communication Technologies (ICT) services
- Banking Sector

1.3 Motivations for Research

This study is motivated because of fast pace of advancement in IoT technologies, the fusion of smart devices to build smart homes has been on the rise. So with new technologies there are many new challenges and security issues arise in the field which are required to be overcome. As Smart homes are emerging industry which is a sub field of IoT because it is built by the combination of different IoT devices which connected to a network and internet for remote access. So when smart devices are connected to a network it is vulnerable to different types of security issues which is an important concern of users that access to data and devices must be protected by implementing some security mechanism to authenticate and authorize a valid user to have access to operate certain Smart (IoT) device according to policy defined by owner.

1.4 Scope

The scope of this research will be solely on the use of voice biometric recognition for authorization and access control with addition of fingerprint biometric for two factor authentication. As smart home system includes IoT devices (sensors, actuators, and user devices), local server, database, owner, users and system is connected to internet for remotely access by a valid and authorized user may arise following threats: Masquerade Attacks, Impersonation Attacks, Denial-of-Service Attacks, Spoofing attacks, Man-in-the-middle attacks and Replay attack. In addition to above mentioned scope, mitigation of these threats will be part of this research to enhance the security of smart homes to deal with increased cyber-attacks/ crimes in this field.

The impacts of proposed framework will be to:

- Provide a more effective authentication, authorization and access control scheme for smart home
- Minimise the impact of cybersecurity incidences
- Increase stakeholders' confidence

Chapter 2

Related Works

A smart home technology is an emerging technology in the field of IoT for comfort and security of home for end users. IoT devices are produced by companies in a rush to fulfill the demand of users without integration of security practices. Consequently, there is a great increase in vulnerable IoT devices which can be exploited by adversary. Almost all smart devices have same functionalities of main features but explicit feature may have difference like home assistant and smart door locks offer different services but both are may be Linux based nodes. These devices have limited storage, computation and power etc which makes to encounter different challenges and rise the security issues in smart homes. This scenario is aggravated by the unambiguous placement of service backdoors by vendor in these smart devices exploited by botnets. Moreover, naive criminal groups have exploited these vulnerabilities in IoT devices for launching different type of attacks [2].

In this chapter, we will discuss some research done by different authors on authentication, authorization and access control scheme in IoT environment. Moreover, at the end of this chapter we will summarize the strong or weak points of each scheme.

2.1 Authentication Schemes

Sanaz Kavianpour et al. [3] a literature review and comparison of several authentication techniques for IoT security. Firstly, they have briefly defined security requirements in IoT perimeter which includes data freshness, confidentiality of data, integrity of data, unbreakable service, user and device authentication, availability of data and services, non-repudiation, user authorization, forward secrecy, attack resistance, data anonymity and scalability. They have identified four questions for the research and carried out search for paper which are related to authentication schemes in IoT to do literature reviews and comparison of different schemes to answer those questions. The four questions are Identifications of security threats in the IoT perimeter?, Security issues/challenges in IoT authentication schemes?, Authentication techniques developed for IoT architectures? Security evaluation criteria and parameters used for IoT authentication?

To address first question they have identified and listed following threats that can compromise an IoT device are DoS, impersonation, man-in-the-middle, changing password, offline password guessing, eavesdropping, smart device stolen and gateway node bypassing attacks.

To address second question they have identified following authentication issues/ challenges in cloud-driven IoT along with solutions which are Limited computation power and memory storage in IoT is a challenge which can be overcome by employing lightweight cryptographic operations like AES and one way hash function, Energy requirement like battery backup is challenge in IoT so a lightweight cryptography authentication scheme can overcome this issue, Scalability is also one of the important challenge in IoT because of gradually increase in devices which can be overcome by developing a scheme working on smart sensing device augmentation, Mobility is a challenge as wearable sensing devices are connected to different networks which can be overcome by developing a mobility complaint security techniques for IoT, Support for heterogeneous devices due to different devices with different computation capability which can be resolved by developing a lightweight authentication scheme, in an IoT whenever a device is removed or added a challenge of dynamic security updates occurs, notification must be send to all old devices to update in their memory which can be done by employing P2P networks and mutual authentication mechanisms. Security and privacy is one of the most important challenge in IoT because of stored data can be used for different kinds of analysis which can be resolved by applying machine-learning approaches.

To address third question they have discussed different cloud-based IoT authentication schemes, lightweight authentication schemes and weakness of each scheme, discussed decentralized blockchain-based authentication have limitations like adding a new service or a device, finally they have discussed different multifactor authentication and remote user authentication schemes based on biometrics along with weakness in each scheme.

To address fourth question different types of security analysis have been utilized to verify that scheme is safe from various kinds of attacks. Following tools are used to analysis which includes Proverif, BAN Logic, CPSA, AVISPA and ROR Model. In the end conclusion can be derived that various authors have proposed different authentication schemes to mitigate the authentication challenges and security issues in IoT but every scheme is susceptible to one of the above-mentioned security threats and still there is a need to research to develop a scheme that resolves authentication issues in IoT.

El-hajj et al. [4] provided a literature review of different IoT authentication schemes. Firstly, they have discussed different IoT architecture models and they have selected three layered (Application, Network and perception layer) model for this research work. Further they have highlighted important IoT security issues which includes user and data authentication, user authorization, data integrity, data confidentiality, non-repudiation, data and service availability and data privacy. They have enlisted the security challenges and security requirement in IoT according to three layered architecture model.

Firstly, the possible attacks on perception layer are Fake Node/ Sybil, Replay, Node Capture, DDoS, Side-Channel, DoS, and Mass Node Authentication attacks. Keeping in view, possible attacks on perception layer following are security requirements i-e user authentication, device authentication, data encryption, secret key agreement and confidentiality of data. Secondly, the possible attacks on Network layer are MITM, DoS, Eavesdropping, Sniffing, Hello Flood attacks and Black/ Gray/ Worm

Hole. Keeping in view, possible attacks on Network layer following are security requirements i-e security of media of communication, data routing security, user authentication, management of security key and intrusion detection. Thirdly, the possible attacks on application layer are access to data and data authentication, data privacy and user identity.

Keeping in view, possible attacks on application layer following are security requirements i-e data and user authentication, user authorization and ISM. Then they have classified IoT authentication schemes based on similar characteristic i-e Authentication factor (identity based, context based physical or behavioral), token and non token based authentication, procedure for authentication (one, two or three way), architecture used for authentication (distributed or centralized) Hardware based (Implicit hardware-based like PUF or TRNG and Explicit hardware-based like TPM) and procedure based authentication. Lastly, they did a survey of authentication scheme used in different IoT domains which includes smart grids, RFID and NFC-Based Applications, Vehicular Networks, Wireless Sensor Networks, Generic IoT Applications, Mobile Network and Applications, and smart homes. They have identified that in IoT authentication a number open issues are still left which need to research to develop a scheme that resolves authentication issues in applications layer and network layer of IoT.

A. Siswanto et al. [5] proposed a home security system architecture based on fingerprint biometric known as BIOFIHS. The proposed architecture includes following components sensor for fingerprint scanning, microcontroller, router, server, smartphone and connection to the Internet. The function of component used in architecture are: The fingerprint sensors receives images of fingerprints and creates template of biometric using digital data to further stores it in database. Input and output commands are regulated by microcontroller board which is used as the hub. Fingerprint data is being retrieved and process by Hub and also communicates with the server. The wireless network router is used to transfer data from microcontroller to server. Then server will process data and runs application. Smart home is controlled and monitored using smartphone. They have implemented this proposed architecture at home door and car garage. Firstly the user will register fingerprint data and store it in database on server and result of the scanning is processed by scanner and stores it in on server then digital records of fingerprint are processed to produce a list of unique pattern features and stores in database. When authorized user need to open the door or garage, they will scan their fingerprints using sensors, then pattern be matched with stored fingerprint database. If fingerprint matches then server will send approval signal of granting access to microcontroller for unlocking home door or car garage. This process can be done by using smartphone for remotely granting access and if malicious activity is performed for opening of door or garage notifications on smartphone will also be sent to the authorized user.

F. Afandi et al. [6] proposed voice recognition and biometric authentication scheme for smart homes, they claim that only registered persons can access and control the locking system of home using voice recognition via android. The system has three levels of system security. According to them first security level is a login system in which only users who have been registered can enter the application to use the system. The second level placed for security is use of biometric because every person have unique biometric which cannot be matched with other person. The last security level is use of a unique speech command which is known to certain users. Furthermore, system has a history tracking control system which is used to record the history of doors opened and closed with time mentioned along with user name. The system design and methodology includes hardware design using NodeMCU ESP8266 12E chip equipped wifi module, software design to interface with hardware, Google speech recognition was used to convert speech to text form and the compare it with code and then act accordingly, biometric authentication for security check is used fingerprint identification. The scheme has been implemented in two different stages, in first stage android application has been tested which focuses biometric authentication and speech control. In second stage system hardware has been tested for controlling the relays. Experimental result shows that the three security levels provide enough security to smart home that if adversary tries to break-in to the system, it will not be an easy to do it. The realtime monitoring and history record control system and storing of data in database server worked with 100% success. The indoor speech command tests without noise works good between 0.5 - 13 cm and outdoor speech command tests works good between 0.5 – 5 cm but if range is increased above this range then performance starts decreasing which means that increasing distance of mouth from smartphone will results decrease in performance. System will have failure if one of the words from speech command is not read properly or missed.

R. Dinar et al. [7] has proposed an authentication scheme for smart homes based on voice command and PIN code through smartphone. The proposed home automation system to unlock the door consist of three main hardware components which includes android smartphone, bluetooth module and arduino board. Smartphone using Bluetooth technology is used to communicate with arduino board via android application. A software interface has been created with MIT app inventor web based to operate the system and speech command is used to open and close the door. They have tested two methods for unlocking the door which are speech authentication and pin authentication and using android application user can select one method from these to unlock the door. Google speech library helps to convert spoken word to text in speech command authentication.

Yan Meng et al. [8] presented a novel system for detection of voice liveness to perform user authentication. Smart home architecture consists of four major components which includes smart home devices, hub, cloud server and interface for user. They have discussed several attacks on the voice interface to gain unauthorized access and carry out over-privileged actions in order to compromise the privacy of the user. They have classified five attacks on different interfaces and discussed the existing proposed countermeasures. Attacks on Physical Layer, Network Layer, Mobile Applications and Voice User Interface are jamming attack, wireless traffic analysis, over-privileged attack, un-authorized device access and spoofing attack. They have proposed a framework for voice liveness detection based on wireless signal known as WiVo against spoofing attack. WiVo differentiate between authentic and fake commands by sensing mouth motion of user and verifies voice liveness. They have implemented WiVo on a SmartThings platform and claims WiVo achieves 96% accuracy with false acceptance rate of 1%.

Lei Zhang et al. [9] presented a VMask (voice mimicry) attack that fools ASV in smart homes by injecting malicious voice command that will act as a legitimate user. They observed that ASV is vulnerable to subtle perturbations when it uses deep learning models. VMask is built on the concept of adversarial examples. VMask works on addition of slight perturbations to voice recordings which can mislead the ASV. They have implemented VMask on VGGVox and Microsoft Azure Speaker Verification (MSASV) by enabling VMask to attack Siri (ASV) in two different scenarios black and grey box. They claim VMask achieved 100% success rate during grey box scenarios and 70% success during scenarios of black box.

Salahaldeen Duraibi et al. [10] presented Identity Authentication Model based on Voice Biometric for IoT Devices. The system is split into two phases i-e enrollment and verification phases. Five steps are performed in the voice enrollment phase which includes data capturing (data collect), pre-processing, extract features, create template and store template in database. The process of collecting voice is converting speaker's voice into digital form and sent it for processing to a computing device. Voice data is collected in two ways which are fixed text and random number string and pre-processing is performed to remove noise from the original voice. LPCCs and MFCC techniques have been used for extraction of features from user voice. During create template and store template steps, templates are created and are stored in a voice recognition database which includes some of them as VidTimit database and MEEI database. Five steps are performed in the verification phase which includes data capturing (data collect), pre-processing, extract features, match template and matching decision. During template matching process, fourier transformation is used for matching the voice of identity claimer’s with stored voice templates. In matching decision process, system will decide that voice match is accepted or it is rejected. False negative or False positive errors occurs during this process. In false-negative error, system unable to identify an authorized or valid user and in false positive error, system granting access to a non-authorized user. The author has presented an automatic voice biometric authentication system used to remotely manage and monitor IoT devices. Proposed scheme has two phases, training phase and verification phase. During enrollment phase, voice of owner is captured during this step using smartphone and converting files with a suitable file format as a output. Removal of noise from collected voice is carried out during pre-processing using threshold based de-noising method. Features are extracted using MFCC technique in which voice signal are divided into frames and then applying a hamming window for each frame. After feature extraction, voice model is trained and stored in database. During verification/recognition phase, voice data is collected and feature extraction is performed via smartphone using same method during enrollment phase. For authentication voice is matched with trained voice model stored in database to make decision to reject or accept voice. The proposed scheme has not yet been implemented in intended environment, so this is only a conceptual model.

Changchun Yang et al. [11] proposed Control System Design for Smart Home Based on Wireless Voice Sensor. Basically they have combined different embedded technologies like ZigBee wireless communication, GSM communication, voice recognition technologies. To make a complete management system for all electrical appliances at house, ZigBee wireless communication Technology has been used to control, monitor and security of appliances. Voice recognition technology has been used in this scheme to control smart home. They have designed two sets of control schemes to make system user friendly. First is voice control scheme, which has been designed in a way that control commands are stored in voice library of interface from where user will read the control commands and commands will be automatically recognized by system. On successful recognition of command, smart home appliances are controlled by user. Second is button control scheme, smart homes appliances can be controlled by users using keys on the interface. Two computers are used in this scheme, upper computer and lower computer. The upper computer is used for data storage, audio collection, voice commands recognition (Hidden Markov Speech Recognition Model is used for voice recognition) and family members confirmations. The lower computer collects real-time environmental information and smart homes devices are wireless controlled using this computer. When system is turned On, system will confirm the family members by voice and control command will be formed by result of voice recognition and environmental data in real time together. To control smart appliances, command will be send by upper computer to lower computer using serial port. In this paper, they have shown results that smart devices are correctly controlled by family members through commands and real-time environmental data together. The system used star-shaped network topology and worked perfectly, if sensors are increased largely, the system cost will increase because system will require large number of node to collect information.

Sitalakshmi Venkatraman et al. [12] presented Use Cases for Smart Home Automation based on Voice-Control System. They have focused on three issues of smart home that includes an integration of voice-based control for different underlying technologies to make its usage easy, users have security and privacy issues in smart home and users have not exploited full potential due to lack of knowledge of machine intelligence. To resolve these issues, a model is proposed in which IoT services and wireless technologies are integrated together to make a smart home secure and voice-controlled using AI. The model aims to address limitations which includes cost effective and user friendly interface with end to end security, customized VPN, speech recognition using voice-controlled AI system. The architecture of this scheme consists of three components. IoT devices, customized VPN and mobile interface work together using the Raspberry Pi platform. This scheme has three main key contributions which includes AI engine based on voice recognition to control and operate smart home devices remotely using smartphone by training a robot with user voice to work as a personal assistant. Proposed model provides end to end security and all third party threats regarding privacy issues has been addressed and system is easy to configure with low cost. To demonstrate the practical feasibility of secure and user friendly system was illustrated in home environment by taking number of use cases.

Ahmed Ismail et al. [13] proposed Speech Recognition based Smart Healthcare System through DTW and SVM. This paper presents voice controlled system for elderly, disabled people and patients using voice recognition. Raspberry Pi is used for controlling home appliances through smartphone. The proposed scheme has enhanced the speech recognition process using SVM with DTW algorithm. The system enables elderly peoples to control smart devices with an accuracy of 97% speech recognition using machine learning-based system. The SVM-DTW model for accessing and controlling smart home appliances have following advantages which includes user authentication for accessing smart device, probability of recognizing voice has been increased, an efficient speech recognition scheme by combination of SVM and DTW. The proposed scheme consists of three components i-e a smartphone, a controller station and smart home devices. User give voice command using smartphone to the controller station and all smart home devices are connected to control station (acts as a router) and passes voice command to concerned devices. The proposed scheme has accuracy of 97% of voice recognition which is higher than SVM system accuracy i-e 79%. The system has limitation that if a user voice is affected due to illness then system has difficulty to recognition of user voice.

2.2 Authorization Schemes

Bogdan et al. [14] proposed a security-oriented framework for IoT Smart-Home application which consist of basically three components to ease the process of adding new device in smart home and an additional layer of security for smart home. Secure Cloud module is presented because cloud platform collects all data directly from smart devices, edge devices and gateways. The way in which authentication of IoT, authorization of user and access to data/ information being managed by cloud may arise several possible vulnerabilities. So to counter those vulnerabilities a secure cloud module was proposed, in which two scenarios taken into account as the setup phase. First is direct registration of IoT devices in the cloud by the user and secondly, registration IoT devices by user through the secure cloud module. For authorization purpose user smartphone is utilized as authorization device for command issued by cloud. A multi stage identification mechanism has been proposed for smart home in which if child device generates an unauthorized command then it will relay that command for authorization to parent node and will allow if parent node allows it. Lightweight SDP controller module is used for implementing a security mechanism to identify and authenticate device using smartphone which helps to reduce the chance of interaction with malicious device. Non-repudiation feature is missing because smartphone and the IoT device are using same DH key sharing along with authentication. Moreover, no authentication has been implemented between user and smartphone.

A. Munir et al. [15] proposed a smart home offline security and automation system using biometric (face and speech recognition). In proposed scheme face recognition was used for opening of door and speech recognition was used to control the smart devices installed in smart home i-e to turn ON/ OFF a room light or fan. In face recognition a database has been created by adding 100 images of a user in different light conditions and angles in grey scaled and rectangular feature of the face. Face recognition was used to unlock the door and for implementation they have connected camera with doorbell, so whenever a doorbell is ring, camera will be activated and capture the image. Captured image is sent to the system for feature extraction and compared with database of system. If captured image and database records are matched i-e result of comparison of two images remains within the defined threshold then system will open the door lock otherwise system will activate the alarm. In speech recognition they have used innovation V3 module to covert text to speech and speech to text. They have discussed that two main factors which affected the performance of speech recognition are voice recognition and command recognition. They have observed that system was unable to differentiate voice command given by which user to switch ON/OFF the home appliances. Moreover, system cannot be trained same command with different voices because V3 module only store 80 commands. There is another issue which they have faced is that after ‘trigger’ command only one word is trained and recognized by V3 Module i.e. ‘room’, ‘kitchen’ or ‘parking’ etc. The proposed system was an offline using wifi router though system was not connected to internet but still it is vulnerable to different kinds of attack if adversary may able to connect to internal networking system.

William Jang et al. [16] proposed an IoT device design guidelines for manufacturers for provision of efficient access control for user. They have discussed two scenarios each for authentication and authorization that highlights the requirement of flawless authentication and access control. The authentication issues are highlighted in first two scenarios: First Scenario, malicious access by family members, Online Purchase by a child using voice purchasing PIN. Second Scenario, unintentional access by guests. Guest borrows owners phone to make call and during call he went near to the bedroom door of owner and smart lock bedroom recognizes owners phone and unlocks the door. Next two highlight authorization issues: Third Scenario, issue of authorization among roommates. Alice has gaming device and share it with roommate by setting up a guest account which will be removed upon logout. Fourth Scenario, home sharers have issue of authorization and precedence among them. Bob is owner of house and shares it with Charlotte and created a separate account of smart home devices for Charlotte. Charlotte has changed device settings and now Bob is unable to use devices. Above scenarios can help in understanding that due lack of flexible access controls and ineffective authentication provides unauthorized users to grant access to the primary account. Keeping in view the above scenarios, recommends device manufacturers to conduct interviews with the end users of devices to understand the setting in which the devices will be used and manufactures gets enough knowledge of advantages and disadvantages before implementing access controls in devices.

Maanak Gupta et al. [17] proposed an authorization framework for VIoT connected through cloud. Users of internet of vehicles have same privacy and security concerns as in smart homes (IoT) because access to data and smart car must be only to authorized and valid users. The framework for authorization of smart car was proposed where interaction between different entities has not been pre-defined and also presented access control design for smart cars. Furthermore, they have discussed requirement of cloud services for vehicles (vehicular clouds concept) and defined approaches for various kind of access control models to implement it on different layers of access control design and authorization framework. Different scenarios have been discussed which includes single and multi-cloud scenarios to assess the requirement of access control for smart cars connected through vehicular cloud.

Salah Zemmoudj et al. [18] proposed IoT based authorization model for smart hospitals. Data of patient is sensitive and access to data can have different type of consequences, therefore, access to data and information must be controlled and only allow to valid or authorized users for smooth working of services at hospitals. They have developed two protocols to protect patient’s data, first protocol is developed to protect personal information, health record of patient and location during stay at hospital is named as context-aware pseudonym service. Second protocol is developed for authorization based on context, role and trust to control the information sharing related to health of patient. The main purpose of this protocol is to monitor doctor’s interaction with patient’s smart bracelet to obtain necessary data for examination. Context is used in protocol to generate different roles along with values of trust. At a time one role activates if value of trust is greater than threshold value.

Mang Su et al. [19] proposed an authorization scheme based on encryption for IoT nodes in cloud platform. All data collected from various nodes in IoT environment is processed and stored on cloud servers has increased IoT computation abilities with new security and privacy challenges. Nodes are more vulnerable due to energy limitations which help attackers to hijack instead of attacking data centers. So if node is hijacked, uploading and downloading data from server should be restricted to avoid damage to data and server privacy. To resolve this issue, they have proposed authorization scheme using proxy re-encryption for IoT nodes on cloud server. In this scheme, cloud server is responsible for data storing and re-encryption by utilizing cloud computing which results in reducing the cost of nodes. They have determined uploading and downloading re-encryption algorithms, downloading algorithm will generate encrypted text from data server for nodes and uploading algorithm will generate encrypted text from nodes for data server. Generation of Keys for re-encryption is divided into two parts, one is with cloud servers and other is with authentication server. During authorization updation, authentication server deletes his part which results that generation of re-encryption keys from missing parameters are not possible and ensures updation of authorization.

2.3 Access Control Schemes

Nor Syazwani Md Noh et al. [20] proposed a biometric (voice recognition) scheme for smart home to enhance security and increase efficiency with minimum manual effort. The proposed system works on human biometric voice command as input for system to switch ON/ OFF home appliances (fan and lamp). The system has been divided into two main parts which includes speech recognition phase and control system phase. Feature extraction and pattern matching are two main modules in the speech recognition. The proposed system has three parts, input and processing of user voice, speech recognition process and hardware interface. Software development for processing of user voice includes data acquisition, signal processing of speech data and GUI development. Hardware development includes designing of system and construction of circuit. Signal processing on speech data includes preprocessing, segmentation of audio signal, audio feature extraction and data classification. Creation of voice database includes collection of voice samples in different scenario like normal voice of person, sore throat voice and voice in fever. Finally, result shows that the identification process has accuracy more than 85% for the offline system and intruder among register user has been identified by online system.

Eric Zeng et al. [21] designed a control interface prototype of smart home based on principles of flexible access control, user agency, respect between users and smart home transparency. They started their research with aiming to answer following two questions, how to deal with security and privacy challenges for multi user in a smart home? What user requires and already following in smart home for security and privacy? Smart home mobile application was developed for multi users to control smart devices. To accomplish principle of user agency, an account is require to be created by user by user ID and password, more users can be added by simply QR code scan on the new user phone. To accomplish principles of flexible access control and respect between users, they designed access controls which includes Role based, Location based, Supervisory and Reactive access control. To accomplish “transparency of smart home behaviors” principle (for remotely control of smart home), they designed notifications which generates alert to users when home devices state is changed. They have deployed there system in seven smart homes for one month and observed the user logs. They concluded that prototype was not effective but they got basic understanding of users preferences and requirements which can be useful for improving access controls in smart home by making more usable configuration interfaces.

Shehzad Ashraf Chaudhry et al. [22] proposed secure certification based device to device anonymous access control scheme for IoMT. The IoMT helps to remotely access patients’ data and diagnose patients disease using various techniques of machine learning. Delay in communication among IoMT devices and server can cause serious issues for patients, therefore, it is very important to have secure communication between D2D for reducing delays. This scheme provides D2D access control using device specific certificates based on elliptic-curve and symmetric key cryptography. After registration of device with gateway and receipt of device specific certificate, a secure connection among devices can be established. Session key is shared among registered devices after mutual authentication. The proposed scheme has been formally verified and proved using RoR security model (real or random) that scheme is secure and resilient against device physical capture attack and different types of attacks. According to performance analysis, this scheme provides trade off between efficiency and security as compared to other schemes.

Fagen Li et al. [23] proposed signcryption based access control scheme for users to access sensor in IoT. They have formally verified security requirement using RoR model. User send message using certificateless cryptography environment to sensor in an identity-based cryptography. In this scheme, WSNs are accessed by authorized users only and user privacy is preserved by protecting query message. Certificates are not used in certificateless cryptography, however it does not have key escrow issue of identity-based cryptography. Certificateless cryptography requires third party which can be trusted and in this case called as key generation center. Partial private key has been generated by key generation center using identity and master key of user. Full private key is generated by combining secret value and partial private key, this user's full private key remains unknown to key generation center. They have compared their scheme with two other access control scheme based on signcryption, sensors computational cost and energy consumption of proposed scheme is largely reduced from other schemes.

Ming Luo et al. [24] proposed an efficient access control scheme based on certificateless and identity-based cryptography for WSN in IoT. In this scheme user using certificateless cryptography is allowed to communicate with sensors in identity-based cryptography with different parameters of systems to use it in cross domain context. Computation cost and bilinear pairings computations are less as compared to other scheme. Session specific temporary information security is achieved by this scheme which other schemes were unable to satisfy. Moreover, Performance analysis shows that this scheme is well-matched for WSNs in cross domain context of Internet of Things.

Weijia He et al. [25] presented rethinking requirement of access control policies for smart home in IoT environment. In smart homes multiple users interact with single device where access control is plays a vital role to protect the privacy and security of a system. They have started working on improving the policies for authentication and access control for smart home. Main focus of access control is on capabilities of device that action can be performed by device rather on focusing device granularity. They have started investigation keeping four research questions infront and studied in 425-participant. The four questions are actually based on the observations that many smart devices functions are combined in single device like hub can perform various task from controlling room locks to switching on lights etc. Most of the smart home are working on device centric model for authentication and access control where device to device access is denied or granted. They have moved to capability centric model for access control where capability is defined for a particular action like placing online order is performed by particular device like voice assistant. Four research questions are as follows; First question, access control policies varies in single smart home IoT devices or not. Second question, what all access are denied to child across participants of study. Third question, access control policy depends on what all factors. Last question, types of authentication methods that protects the smart home security and privacy. Keeping all these factors in mind, they have presented an access control and authentication policies for smart homes.

Amit Kumar Sikder et al. [26] proposed an access control system based on multiple user and multi device awareness for smart home. In smart home, multiple devices are installed and multiple user have right to access that devices through some interface like smartphone. In this paper, they have introduced access control mechanism for Multi user and multi device aware that allow user to select access controls flexibly as per user requirements. This scheme has three components which includes user interface, server and policy manager. Access control can be specified by user through user interface and server will translate access control into policies. These policies are analyzed by policy manager and then final policy will be generated after negotiation with users. They have implemented this system on real smart home and evaluated the effectiveness of system. The proposed system is robust against various types of access control related attacks and evolution shows that system has 100% success rate in detection of various types of attacks.

There are many issues and challenges during capturing and authentication process using fingerprint like fake biometrics (fingerprint copy, fingerprint picture, mold of a finger, "gummy"), wound, dirt or oil on scanner or on finger and voice recognition like use of voice recording, voice mismatching due to a surgery, cough; fever and background noise like traffic, televisions voice, music [27] [28].

2.1 Comparison Table – Authentication, Authorization and Sccess Control Mechanism used in Scheme with Strong Points/ Weakness

Scheme	Description	Mechanism	Biometric	Strong Points/ Weakness
Siswanto et al. [5]	Biometric Fingerprint Architecture for Home Security System	Authentication	Fingerprint	No threat model and security features defined
F. Afandi et al. [6]	Proposed android Application for smart home using Voice Recognition	Authentication	Voice Recognition	No threat model and security features defined
R. Dinar et al. [7]	Proposed Door automation system using voice command and PIN with android smartphone	Authentication	Speech command and PIN	No threat model and security features defined

Scheme	Description	Mechanism	Biometric	Strong Points/ Weakness
Yan Meng et al. [8]	Proposed Voice liveness detection system in Smart Home	Authentication	Voice liveness detection system	Secure and resilient against Spoofing Attacks
Lei Zhang et al. [9]	Proposed a voice attack in smart homes	Authentication	Voiceprint	**Strong Point:** Implemented Vmask attack on speaker verification system (Siri) and achieved 100% success rate in grey box scenarios and 70% in black box scenarios
Salahaldeen Duraibi et al. [10]	Presented Identity Authentication Model based on Voice Biometric for IoT Devices	Authentication	Voice Recognition	Scheme has not yet been implemented in intended environment, so this is only a conceptual model

Scheme	**Description**	**Mechanism**	**Biometric**	**Strong Points/ Weakness**
Changchun Yang et al. [11]	Proposed Control System Design for Smart Home Based on Wireless Voice Sensor	Authentication	Voice Recognition	System Cost will increased by increasing sensors because system will require large number of node to collect data
Sitalakshmi Venkatraman et al. [12]	Presented Use Cases for Smart Home Automation based on Voice-Control System	Authentication	Voice Recognition	**Strong Point:** Proposed model provides end to end security and all third party threats regarding privacy issues has been addressed and system is easy to configure with low cost
Ahmed Ismail et al. [13]	Proposed Speech Recognition based Smart Healthcare	Authentication	Voice Recognition	The system has limitation that if a user voice is affected due to illness then

Scheme	Description	Mechanism	Biometric	Strong Points/ Weakness
	System through DTW and SVM			system has difficulty to recognition of user voice **Strong Point:** Voice recognition accuracy is 97%
Boogdan et al. [14]	Proposed Security Framework for Smart Home applications	Authorization	-	Non-repudiation feature is missing
A. Munir et al. [15]	Proposed Smart Home security using Face and Speech Recognition	Offline automation system	Face and Speech Recognition	No threat model and security features defined
William Jang et al. [16]	Enabling Multi-user Controls in Smart Home Devices	Scenario based Authentication and Authorization	-	Scenario based explanation of requirement of users authorization for manufactures

Scheme	Description	Mechanism	Biometric	Strong Points/ Weakness
Maanak Gupta et al. [17]	Proposed an authorization framework for VIoT connected through cloud	Authorization	-	Framework for car authorization and requirement of vehicular clouds concept has been identified
Salah Zemmoudj et al. [18]	Proposed IoT based authorization model for smart hospitals	Authorization	-	Role based authorization controls implemented for access to the information and data
Mang Su et al. [19]	Proposed an authorization scheme based on encryption for IoT nodes in cloud platform	Authorization	-	Re-encryption based key generation are not possible for missing part of key which ensures authorization updation
Nor Syazwani	Proposed	No	Speech	Only improved

Scheme	Description	Mechanism	Biometric	Strong Points/ Weakness
Md Noh et al. [20]	Smart Home system using Biometric Recognition	mechanism	command	the efficiency of voice recognition
Eric Zeng et al. [21]	Proposed access control mechanism to Improve Security and Privacy in Smart Home	Access control	-	**Strong Point:** Prototype Mobile application implemented in seven homes which allows multiple users to control devices and got basic understanding of users preferences and requirements and useful for for improving access controls
Shehzad Ashraf Chaudhry et al. [22]	Proposed secure certification based device to device anonymous	Access control	-	Secure and resilient against device physical capture attack

Scheme	Description	Mechanism	Biometric	Strong Points/ Weakness
	access control scheme for IoMT			
Fagen Li et al. [23]	Proposed signcryption based access control scheme for users to access sensor in IoT	Access control	-	Sensors computational cost and energy consumption is largely reduced
Ming Luo et al. [24]	Proposed an efficient access control scheme based on certificateless and identity-based cryptography for WSN in IoT	Access control	-	Known session specific temporary information security has been satisfied
Weijia He et al. [25]	Presented rethinking requirement of access control	Access control	-	-

Scheme	**Description**	**Mechanism**	**Biometric**	**Strong Points/ Weakness**
	policies for smart home in IoT environment			
Amit Kumar Sikder et al. [26]	Proposed an access control system based on multiple user and multi device awareness for smart home	Access control	-	100% Success rate in detection of various types of attacks

Chapter 3

Threat Modeling

In this chapter, we will discuss threat modeling of smart homes. First of all, we will identify and characterize the system and define the kinds of threats in smart homes. Secondly, we will identify the assets and vulnerabilities in smart homes. Thirdly, threat agents and damages caused will be explained. Fourthly, attack vectors in relation to user authentication, authorization and access control will be discussed alongwith the characterizing the security controls to mitigate attack vectors. Lastly, threat model will be analyzed.

3.1 Identify and characterize the system

Smart homes are emerging technology in the field of IoT, so it is very important to plan, implement, maintain, and assess the security controls for smart home systems by performing a methodical analysis of risk involving system threat modeling [29] [30] [31]. The scope is limited to smart home system threat modeling, which involves focusing on the authentication and authorization of user in a smart home to protect unauthorized access to device and data [32]. Smart Homes architecture includes IoT devices (Air conditioner, Temperature sensor, microwave oven, lights and so on) installed in a smart homes, a server (for computation and storage of data) and a user as illustrated in Fig-2.1.

There are many kinds of threats in smart home environment [33] [34], we can divide them in three main categories as follows:-

1. Unintentional threats
2. Intentional threats
3. Malfunctions

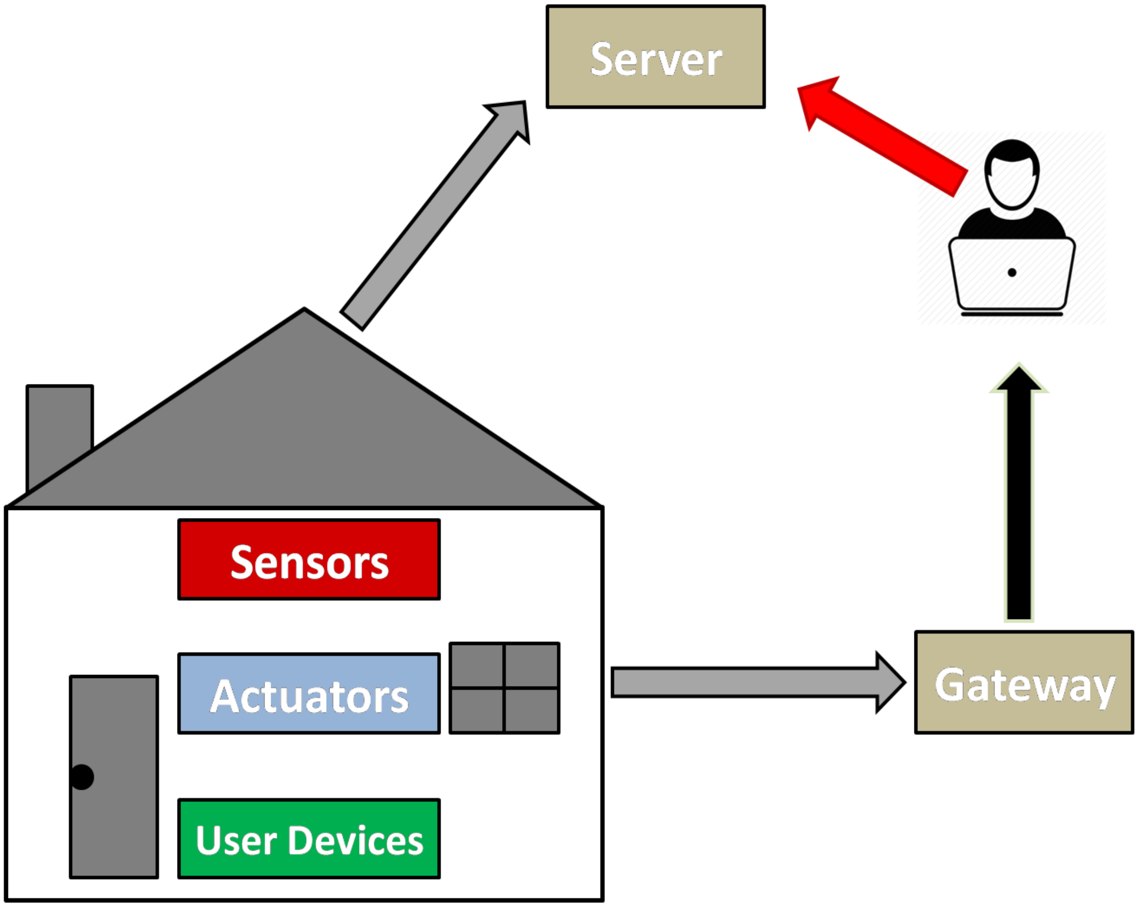

Fig-2.1: Smart Homes Architecture

1. Unintentional threats

a. Leakage of Information: Due to less computational power of IoT devices installed at smart homes and incorrect security polices implemented may results in information leakage over the network.

b. Data altered accidentally: If a data is changed or altered accidentally in the smart home applications it can cause certain errors and system may develop faults or malfunctioning in the smart home devices

c. Lack of planning: Planning is most important and key feature which can lead to serious security and privacy issues in smart homes. Failure of planning at any level (component, design, policy or installation) results in serious security issue.

d. Unreliable source: Unintentionally data has been accessed by smart device from unreliable source may leads to an attack. Simplest example is that Smart TV may accessed a website which has an injected malicious scripts by broadcaster may result in an attack.

2. Intentional threats

a Identity Theft: An adversary may obtain credentials of users / administrator and pose as an valid user of the home to exploit smart home services and can make changes in the policies.

b. Denial of service: Smart home devices are connected through network so denial of service or distributed denial of service may results in device unresponsive or behave abruptly.

c. Information Manipulation: Smart homes devices may be fed with wrong data by adversary helps in bypassing security features and exploiting the services of smart home.

3. System Malfunctions

a. Failure of communication channel: Communication channel failure may results non availability of smart home devices which may be due to hardware fault or software errors. It can also occur due to power failure or deliberate attack of adversary.

b. Smart Device Failure: Device failure sometimes may leads to serious consequences like doorlocks need to be broken for entry in house.

c. Power Failure or malfunction: Smart home devices may run on battery but for shorter time because some devices need more power for continuous working. So if power failure occurred it may lead to some serious consequences like no cooling system of home.

3.2 Assets

Smart homes have following type of assets [32] [35].

1. Personal Data
2. Video of Smart homes
3. Money & expansive items
4. Medical IoT devices
5. Furniture and Equipment

3.3 Vulnerabilities

A vulnerability is a weakness which can be exploited by a attacker to gain unauthorized access to or perform unauthorized actions on a system [36]. Smart homes may have vulnerabilities [37] [38] as shown in Fig-2.2.

a. Ineffective Authentication: authentication is main feature of proofing identity of valid user to a system. So if authentication mechanisms are not placed in a system adversary may exploit it and gets information of his interest.

b. Insecure web/ mobile interface: User need some kind of interface to operate smart home devices. So if interface is not secure adversary may exploit it and gets information of his interest.

c. Insecure network services: Smart homes may be connected to the Internet; if network is not secure adversary can attack it remotely or by downloading malware on equipment.

d. Insecure cloud interface: All data of smart homes are placed on server or cloud, if cloud interface is not secure it can be exploited by attacker.

e. Insecure software: Software vulnerabilities can be exploited by attacker to get control over smart home system.

f. Physical access to smart home system: If System is accessed physically, it is vulnerable to all kind of attacks by adversary.

g. No security updates: Due to use of fixed firmware system security is unable update which cause serious vulnerabilities that can be exploited by attackers.

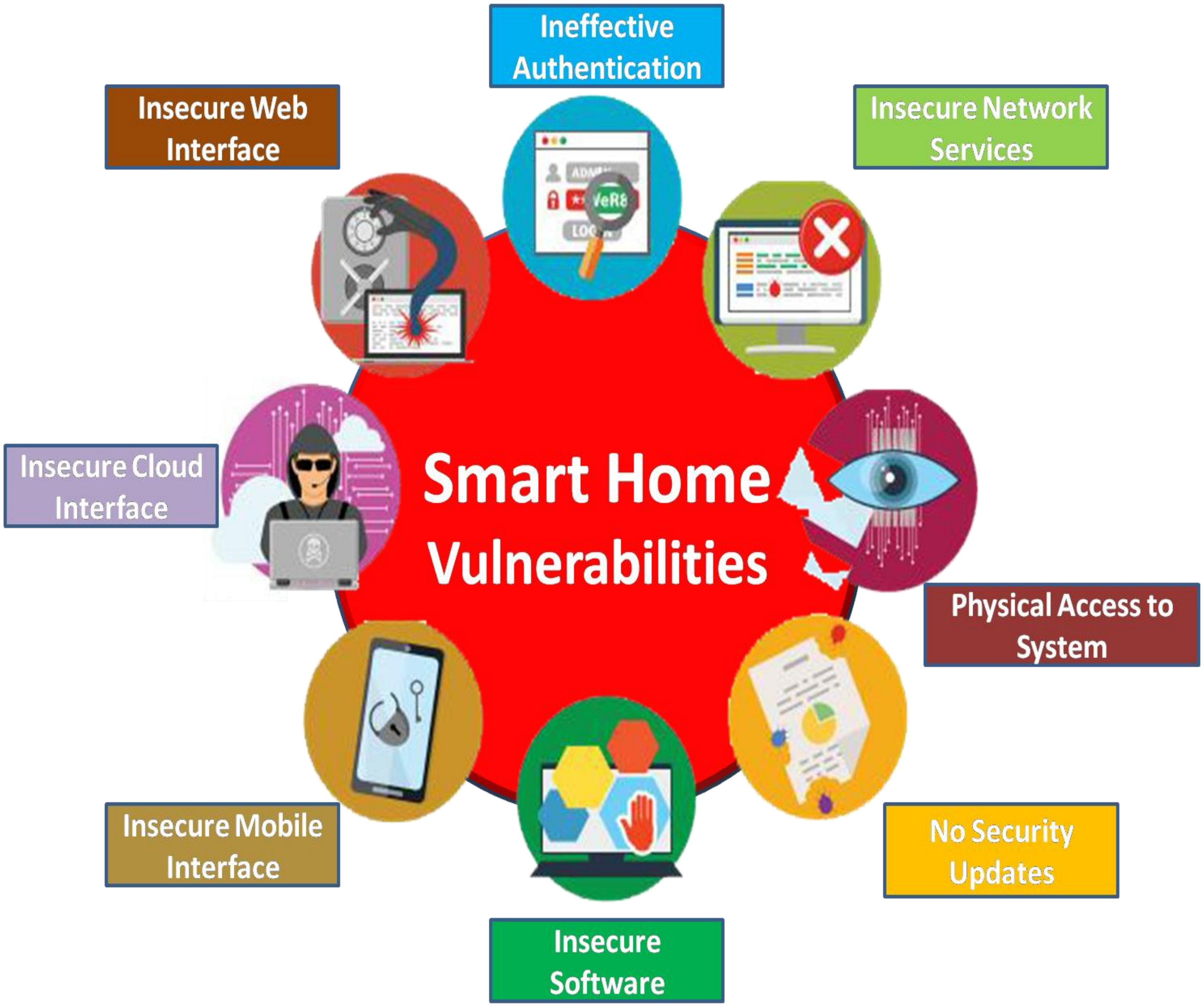
Ineffective Authentication
Insecure Web Interface
Insecure Network Services
Smart Home Vulnerabilities
Insecure Cloud Interface
Physical Access to System
Insecure Mobile Interface
No Security Updates
Insecure Software

Fig-2.2: Smart Home Vulnerabilities

3.4 Threat Agents

Possible attackers in smart homes can be [39]:

1. Cyber Attackers
2. Hackers-for-hire
3. Thieves
4. Criminal Gangs

These attackers can cause following losses to a smart homes and their users [40] (Fig-2.3).

a. They can steal the confidential information.
b. They can cause a financial loss.
c. They can make life threatening situation by controlling medical devices.
d. They can target customers for customer identity theft.
e. They can monitor smart homes.
f. They can use and sell data in black market.

Steal Confidential Information
Identity Theft
Financial Loss
Attack Agents Cause losses Smart Home
Monitor Smart Homes
Life Threatening
Sell Data on Dark Web

Fig-2.3: Attack agents can cause losses to a smart homes

3.5 Attack Vector's

Attack vector is a pathway an attacker uses to access vulnerability. Attack vectors in smart homes in relation to user authentication, authorization and access control are as shown in Fig-2.4 which are as follows [41] [42]:-

a. Masquerading Attack: Attacker claims to be authentic user in a system, may have access to all information

b. DOS Attack: Attacker Interrupts the services to legal users.

c. MitM Attack: Man-in-the-middle (MitM) attack is when an attacker intercepts communications between two parties and able to receive all communication.

d. Reply Attack: All valid information gathered by Attacker and used to exploit the system later on.

e. Spoofing Attack: when a person or program successfully identifies itself as another by falsifying data, to gain an illegitimate advantage.

f. Impersonation Attack: Attackers pose as a known or trusted person get sensitive information from system.

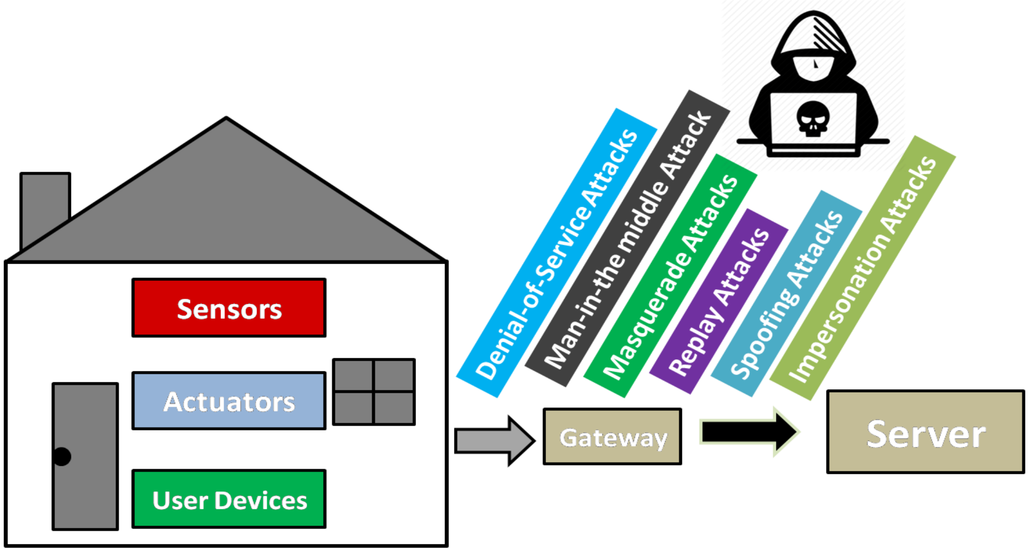

Fig-2.4: Attack Vectors in Smart Homes

3.6 Characterize the security controls for mitigating the attack vectors

Following security controls can be placed to mitigate attacks against each attack vectors [43] [44]:

a. Masquerading claims to be an authenticated user and steals authorized data, so authentication and authorization mechanism to be placed to mitigate this attack.

b. Replay attacker gathers all valid information and uses it to exploit the system later on, so authentication mechanism to be placed to mitigate this attack

c. Message modification construct the data/ information between authorized users and also a threat to data integrity, so authentication mechanism to be placed to mitigate this attack.

d. DoS suspend legal services to authorized users and a service availability threat by sending authentication requests, so authentication mechanism to be placed to mitigate this attack.

e. Spoofing attack is a situation in which a person or program successfully identifies as another by falsifying data to gain an illegitimate advantage or bypass access controls, so authentication and access control mechanism to be placed to mitigate this attack.

f. Impersonation attack attackers pose as a known or trusted person get sensitive information, so authentication and access control mechanism to be placed to mitigate this attack.

g. A man-in-the-middle (MitM) attack is when an attacker intercepts communications between two parties, so authentication mechanism to be placed to mitigate this attack.

3.7 Analyze the threat model

The security requirement in smart home includes Authentication, Authorization, Confidentiality, Integrity, Availability and Non-repudiation. We will be focusing on security requirements concerning to user i-e authentication, authorization and access control. Keeping in view security requirement following threats are perceived in smart home: Replay Attacks, DoS Attacks, Message Modification Attacks, Masquerade Attacks, Spoofing attacks, Man-in-the-middle attacks and Impersonation attacks. [45] [46] Therefore, a scheme is required to be formulated to mitigate the threats by authenticating and authorizing a user and implementing access control policy.

Chapter 4

Proposed Authentication, Authorization and Access Control Scheme using Voice Biometric in Smart Homes

In this chapter, firstly, we will discuss system model of our proposed scheme, work flow chart of our scheme alongwith security features in our scheme. Secondly, we will discuss each phase of our proposed scheme and at the end we will discuss security and performance analysis to formally proof that our scheme is secure against different types of attacks and also cost effective then other schemes.

In our scheme, we use fingerprint for authentication of user and voice recognition as 2nd factor of authentication. Moreover, voice is used for access control of smart home devices.

4.1 System Model

We have considered 4 entities in our proposed scheme: (Table 4.1)

1- Administrator → Registration Server.

2- IoT Devices → I_j.

3- User.

4- User device → Smart phone with biometric sensor.

Table 4.1: Entities in Proposed Scheme

Notation	**Description**	**Purpose**
A_d	Administrator	Will act as registration server and also responsible for device authentication.
U_r	User	User will be a person who will be using smat home devices.
M_d	User Device	User device will be used as a interface to use smart home devices by users
I_j	IoT Device	IoT devices will be end devices which will be operated and controlled by user in smart home

In our proposed scheme, administrator performs functionalities of registration server and also responsible for IoT device authentication. All IoT devices of network should be pre-installed by the administrator. Furthermore, to access IoT device or set of IoT devices, user must be valid user (registered with administrator) and login through user device using biometric. Administrator will define secret key material and stored on user device.

The security requirements in smart home in this scheme concerning to user are authentication, authorization and access control. Replay Attacks, DoS Attacks, Message Modification Attacks, Masquerade Attacks, Spoofing attacks, Man-in-the-middle attacks and Impersonation attacks [45] [46] are threats perceived in smart home as per above security requirement. To mitigate these threats we need to design and implement a user’s authenticating and authorizing scheme by enforcing implementation of access control policy.

We have designed distributed system in which authentication and access control are made at the sensor layer and lightweight system scheme using symmetric key cryptography, concatenations and hashing.

4.2 Work Flow Diagram

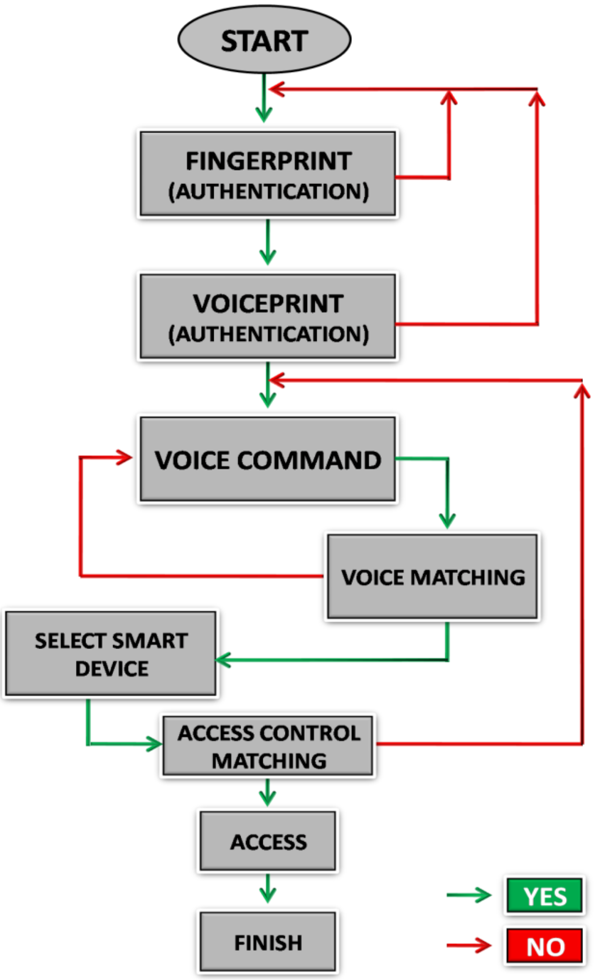

Fig-3.1: Proposed scheme work flow diagram

Security features in this proposed scheme are:

1. User authentication: Two factor authentication is used in this scheme, firstly fingerprint and secondly voice recognition along with time stamp to avoid replay attack.

2. User authorization and access control: Access control levels are implemented to ensure user authorization by using voice recognition with time stamp to avoid replay attack and unauthorized access.

4.3 Notation Table of Proposed Scheme

Notation	**Description**
A_d	Administrator
U_r	User
M_d	User Device
I_j	IoT Device identity
M_k	Master key
a, b	Two secrets of A_d
R_u	User real identity
F_{Bio}	H (Fingerprint biometric output (true or false) || M_dID)
V_{Bio}	H (Voice biometric output (true or false) || M_dID)
$U_{id} = H (R_u)$	Derived identity U_r
$SK_{au} = H (H (R_u) \|\| M_k)$	Secret shared key between A_d and M_d
$SK_{ai} = H (I_j \|\| M_k)$	Secret shared key between A_d and I_j

4.4 Proposed Scheme

Following are different phases used in our proposed scheme: (1) IoT devices installation phase, (2) registration phase, (3) Users installation phase, (4) login phase, (5) user request phase, (6) IoT device answer phase, (7) information retrieval phase, (8) User password updation phase. Fig 4.1 shows work flow of scheme and Fig 4.2 shows an overview of the scheme in different phases among each entity. In addition, summary of notations and abbreviations are given in Table 2.

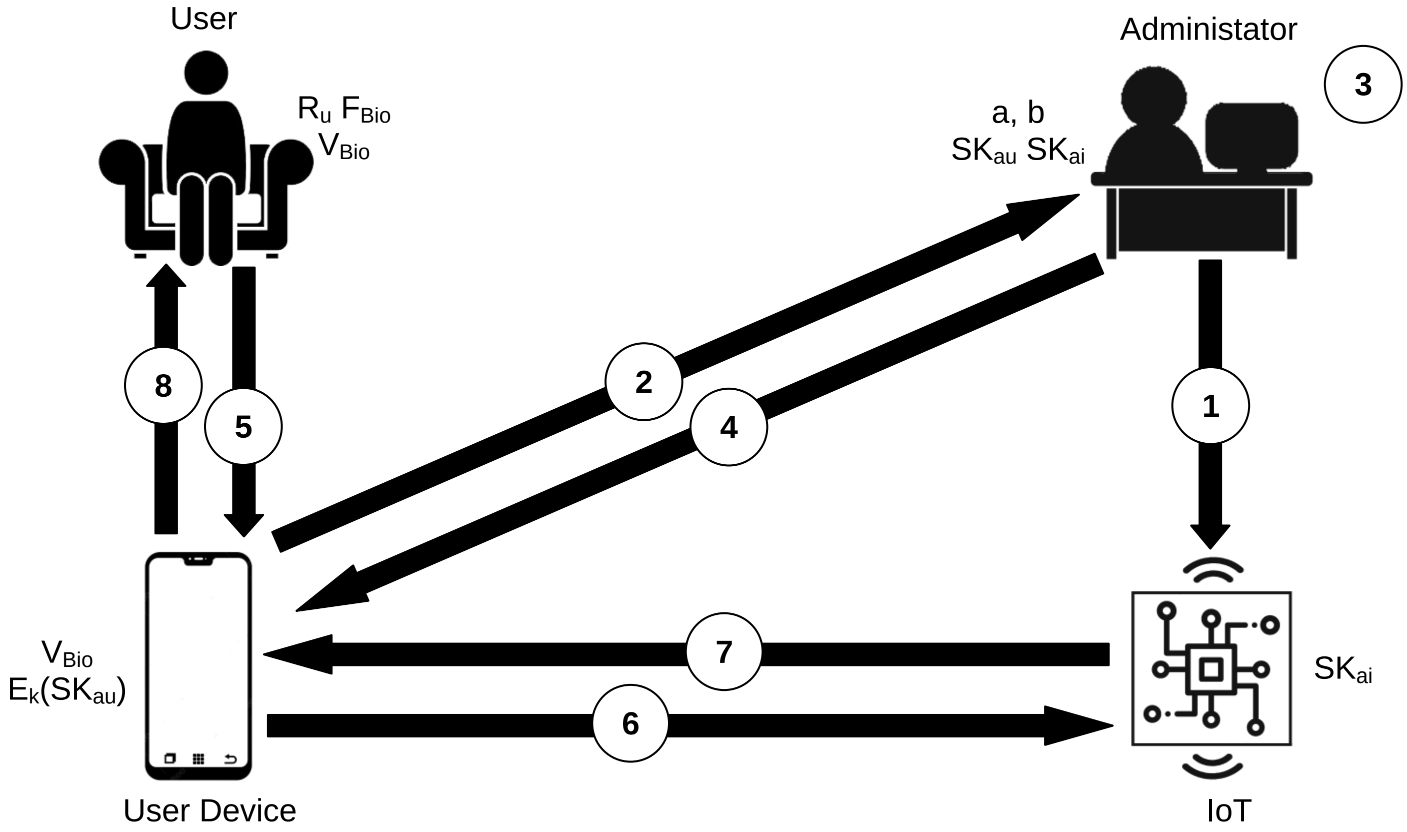

Fig-4.1 Proposed scheme overview

In phase-1, we have used (1) pre-shared key (SK_{au}) between A_d and U_r and pre-shared key (SK_{ai}) between I_j and A_d.

$$SK_{au} = H\ (H\ (R_u)\ ||\ M_k\ )\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots..(1)$$

$$\begin{cases} R_u \longrightarrow \text{User real identity like name, national ID number etc} \\ M_k \longrightarrow \text{Owner master key} \end{cases}$$

Pre-shared key as shown in (1) will be stored in user device in encrypted form $E_k(SK_{au})$ and adversary cannot access the information stored in user device even if it is lost or stolen.

User enters R_u, F_{Bio}, V_{Bio}, helps the user device to calculate information as shown in (2):

$$\left.\begin{cases} U_{RP} = H\ (F_{Bio} \oplus V_{Bio}) \\ U_{id} = H\ (R_u) \end{cases}\right\} \longrightarrow \quad K = H\ (U_{id}\ ||\ U_{RP})\ldots\ldots\ldots\ldots\ldots(2)$$

User password is combination of users fingerprint and voice biometric. Basically, when user enters voice, system will check the value of voice is within threshold level or not. System will take the value of voice (true or false) and concatenate it with the user device identification and then take the hash of this value to form user password which will be used for authentication and authorization.

Thus, we derive SK_{au} like (3):

$D_k(E_k(SK_{au}))$

$SK_{ai} = H(I_j \| M_k)$, I_j: IoT device identity…………………..(3)

4.3.1. IoT devices installation phase

Administrator will choose two secrets denoted by a, b. Identity of the IoT device j is denoted by I_j. The administrator shares parameters as shown in (4) with each IoT device using SK_{ai} between I_j and A_d. Parameter b remains unknown for U_r.

b, I_j, $H(a \| b)$, $H(I_j \| H(a))$ …………………………(4)

4.3.2. Registration phase

As we mentioned earlier, V_{Bio} and encrypted $E_k(SK_{au})$ are stored on M_d. Parameters at (5) will be calculated by M_d after U_r enter R_u and F_{Bio}:

$$\begin{cases} U_{RP} = H(F_{Bio} \oplus V_{Bio}) \\ U_{id} = H(R_u) \end{cases} \qquad \text{………….……………..(5)}$$

Now with above equations $K = H(U_{id} \| U_{RP})$ is derived. Request for registration include message registration with A_d to I_j. Time stamp is used to avoid replay attacks as shown in (6).

$U_{id} \| E_{SKau}(R_u \| U_{RP} \| reqAcc)$ ..………………………(6)

4.3.3. Users installation phase

In this phase, first computes key $SK_{au} = H\ (U_{id} \,||\, M_k\ )$ and received message will be decrypted by A_d. After decryption A_d verifies R_u identity using $U_{id} = H\ (R_u)$ and secret key material has been computed using $U_{RP} = H\ (U^R{}_{RP})$ with parameters a, b. In this scheme O_i, P_i, Q_i, S_i, T_i has particular function. After computing these parameters, encrypted message $E_{SKau}(P_i, Q_i, S_i, T_i, H(P_i, Q_i, S_i, T_i))$ will be sent from A_d to M_d to store these parameters on M_d. Fig-4.2 gives overview of 1st two phases (1. Registration and 2. Installation).

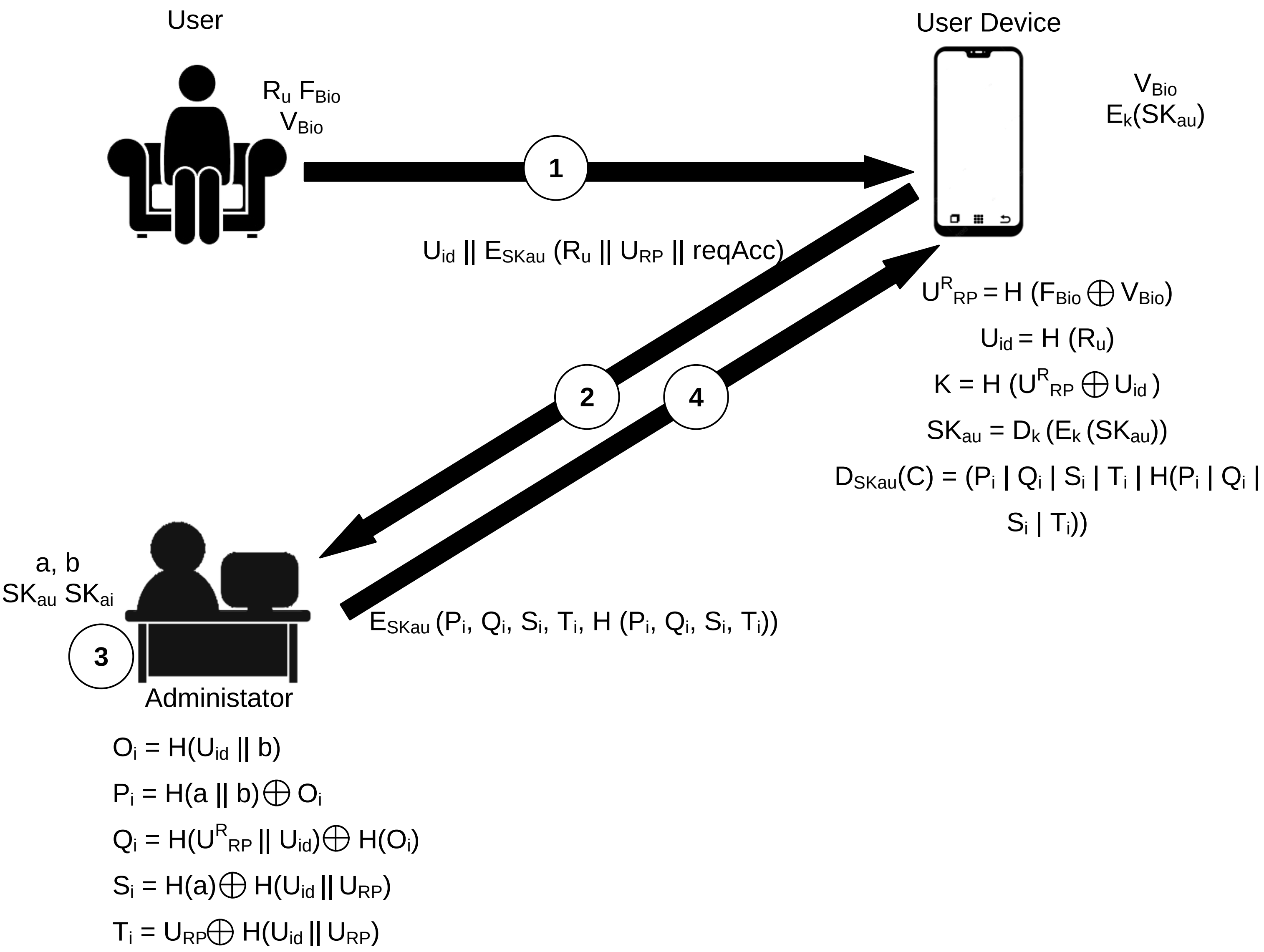
User
User Device
$R_u\ F_{Bio}$
V_{Bio}
V_{Bio}
$E_k(SK_{au})$
1
$U_{id} \,||\, E_{SKau}\ (R_u \,||\, U_{RP} \,||\, reqAcc)$
$U^R{}_{RP} = H\ (F_{Bio} \oplus V_{Bio})$
$U_{id} = H\ (R_u)$
$K = H\ (U^R{}_{RP} \oplus U_{id}\ )$
$SK_{au} = D_k\ (E_k\ (SK_{au}))$
$D_{SKau}(C) = (P_i \mid Q_i \mid S_i \mid T_i \mid H(P_i \mid Q_i \mid S_i \mid T_i))$
2
4
a, b
$SK_{au}\ SK_{ai}$
3
Administator
$E_{SKau}\ (P_i, Q_i, S_i, T_i, H\ (P_i, Q_i, S_i, T_i))$
$O_i = H(U_{id} \,||\, b)$
$P_i = H(a \,||\, b) \oplus O_i$
$Q_i = H(U^R{}_{RP} \,||\, U_{id}) \oplus H(O_i)$
$S_i = H(a) \oplus H(U_{id} \,||\, U_{RP})$
$T_i = U_{RP} \oplus H(U_{id} \,||\, U_{RP})$

Fig-4.2 Overview of 1st two phases (1. Registration and 2. Installation)

4.3.4. Login phase

In this phase, U_r enters R_u and fingerprint F_{Bio} with voiceprint V_{Bio}, then device can compute following parameters as shown (7).

$$\left\{ \begin{array}{l} U_{id} = H\ (R_u) \\ U_{RP} = H\ (U^{R}_{RP}) \end{array} \right. \longrightarrow \quad T_i = H\ (U_{id} \mid\mid U_{RP}) \oplus U_{RP} \text{ ……(7)}$$

If computed value of T_i is equals with the stored value of T_i then user login is successful.

4.3.5. Request phase

On successful login, in this phase U_r give voice command to selects I_j. Device performs computations as shown (8) and (9).

$$H(a) = S_i \oplus H\ (U_{id} \mid\mid U_{RP}) \text{ …………………………………..(8)}$$

$$H(O_i) = Q_i \oplus H\ (U_{RP} \mid\mid U_{id}) \text{ ………………………………….(9)}$$

User can construct H (I_j || H(a)) using H(a) and store on IoT device. Since H (a || b) is stored in IoT device, it can construct P_i and find O_i using P_i. As a result, to create secret shared key and cypher text, following operations are carried out as shown in equations (10)-(15). A random nonce R_N and time stamp (Req) has been added to avoid replay attacks.

$$Q_1 = H\ (I_j \mid\mid H(a)) \oplus H\ (U_{id} \mid\mid R_N) \text{ …………………………..(10)}$$

$$Q_2 = H\ (O_i) \oplus R_N \text{ ………………….……………………..(11)}$$

$$V_1 = H\ (R_N \oplus P_i) \text{ ……………………………………………(12)}$$

$$CU_i = P_i \oplus H\ (Q_1) \text{ ……………….……………………..(13)}$$

$K = H\ (R_N \parallel I_j \parallel H(O_i))$ ……………………………………….(14)

$E_k = (U_{id} \parallel Q_2 \parallel Req)$ ……………………………………….(15)

Message as shown in equation (16) is sent to gateway for further transfer of message to the corresponding I_j.

$CU_i \parallel Q_1 \parallel Q_2 \parallel V_1 \parallel E_k\ (U_{id} \parallel Q_2 \parallel Req_1)$ ………………….(16)

4.3.6. Answer phase

After receipt of request message, using stored parameters following computations as shown in equation (17) - (21) is performed by I_j.

$H\ (U_{id} \parallel R_N) = H\ (I_j \parallel H(a)) \oplus Q_1$ …..……………………..(17)

$P_i = CU_i \oplus H\ (H\ (I_j \parallel H\ (a)) \parallel H\ (U_{id} \parallel R_N))$…….…………..(18)

$O_i = P_i \oplus H\ (a \parallel b)$ …………………………………………..(19)

$R_N = H\ (O_i) \oplus Q_2$ ……………….……………………….(20)

$V_1^* = H\ (R_N \oplus P_i)$ …………………………………………...(21)

If value of V1* is equal to V1 value, then it means U_r is authenticated and authorized. To execute decryption $D_k = (U_{id} \parallel Q_2 \parallel Req)$, key $K = H\ (R_N \parallel I_j \parallel H(O_i))$ is derived. Following computations as shown in equations (22)-(24) are executed with random value R_v.

$Q_3 = R_v \oplus H\ (U_{id} \parallel R_N)$ …………………………………………(22)

$V_2 = R_N \oplus H\ (I_j \parallel P_i \parallel R_v)$…...……………….……………………(23)

$SK_{NV} = H\ (R_N \parallel R_v)$ ……………………………………....(24)

After all computations, $Q_3 \,||\, V_2 \,||\, E_{SK_{NV}}$ (CM) is sent to U_r in which CM is a confirmation. Fig-4.3 gives overview of 3 phases (1. User login, 2. Request and 3. Answer).

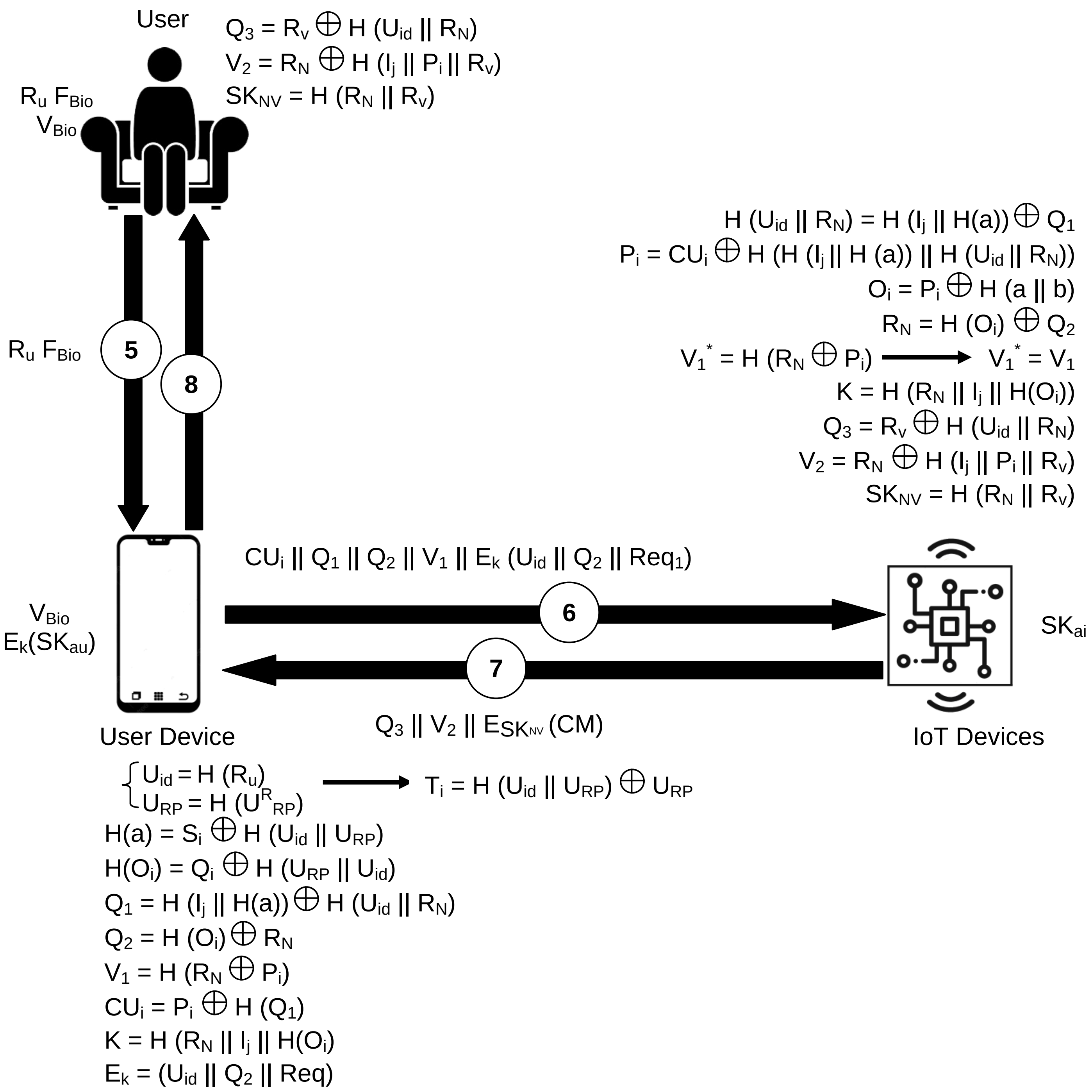
User
$Q_3 = R_v \oplus H(U_{id} \,||\, R_N)$
$V_2 = R_N \oplus H(I_j \,||\, P_i \,||\, R_v)$
$SK_{NV} = H(R_N \,||\, R_v)$
R_u F_{Bio}
V_{Bio}
$H(U_{id} \,||\, R_N) = H(I_j \,||\, H(a)) \oplus Q_1$
$P_i = CU_i \oplus H(H(I_j \,||\, H(a)) \,||\, H(U_{id} \,||\, R_N))$
$O_i = P_i \oplus H(a \,||\, b)$
$R_N = H(O_i) \oplus Q_2$
$V_1^* = H(R_N \oplus P_i) \longrightarrow V_1^* = V_1$
$K = H(R_N \,||\, I_j \,||\, H(O_i))$
$Q_3 = R_v \oplus H(U_{id} \,||\, R_N)$
$V_2 = R_N \oplus H(I_j \,||\, P_i \,||\, R_v)$
$SK_{NV} = H(R_N \,||\, R_v)$
R_u F_{Bio}
5
8
$CU_i \,||\, Q_1 \,||\, Q_2 \,||\, V_1 \,||\, E_k(U_{id} \,||\, Q_2 \,||\, Req_1)$
6
7
V_{Bio}
$E_k(SK_{au})$
SK_{ai}
$Q_3 \,||\, V_2 \,||\, E_{SK_{NV}}$(CM)
User Device
IoT Devices
$\left\{ \begin{array}{l} U_{id} = H(R_u) \\ U_{RP} = H(U^R{}_{RP}) \end{array} \right. \longrightarrow T_i = H(U_{id} \,||\, U_{RP}) \oplus U_{RP}$
$H(a) = S_i \oplus H(U_{id} \,||\, U_{RP})$
$H(O_i) = Q_i \oplus H(U_{RP} \,||\, U_{id})$
$Q_1 = H(I_j \,||\, H(a)) \oplus H(U_{id} \,||\, R_N)$
$Q_2 = H(O_i) \oplus R_N$
$V_1 = H(R_N \oplus P_i)$
$CU_i = P_i \oplus H(Q_1)$
$K = H(R_N \,||\, I_j \,||\, H(O_i))$
$E_k = (U_{id} \,||\, Q_2 \,||\, Req)$

Fig-4.3 Overview of 3 phases (1. User login, 2. Request and 3. Answer)

4.3.7. Information retrieval phase

Equation (25) is derived by user and Equation (26) is computed.

$R_v = Q_3 \oplus H\ (U_{id} \,||\, R_N)$ ……………………………………..(25)

$N_u \oplus H\ (I_j \,||\, P_i \,||\, R_v)$ …………………………………………(26)

Computed result from above equations and transmitted value of V_2 are compared to obtain mutual authentication and to decrypt last message, shared symmetric key can be derived if results of above equation and transmitted V_2 are equal.

4.3.8. User password updation phase

In this phase, new password value needs to be entered by user which results in updating the value of U_{RP}. Q_i and T_i values are again computed and stored on M_d. Encryption key of Sk_{au} will also need to be updated which results in updatation of $E_k(Sk_{au})$.

Chapter 5

Security and Performance Analysis

In this chapter, we will do security analysis using different techniques and performance analysis of proposed scheme.

5.1 Security Analysis

The system entities are protected by our proposed scheme from a variety of attacks. We have utilized informal analysis and formal analysis using BAN logic model to prove proposed scheme is resilient against all attacks which were described in threat model.

5.1.1 Informal Security Analysis

We will provide informally analysis in this part to prove that this scheme protects smart home devices from all known attacks.

a. Replay attack

Replay attack is not possible at registration phase due to the addition of a time stamp. An adversary cannot modify anything since they cannot decrypt registration request or response. Furthermore, attack on IoT device through user request message is not possible due to inclusion of time stamp in it.

b. Masquerade Attacks

It is an attack in which a fake identity is used to obtain unauthorized access to personal computer data using valid access identification. This attack is not possible due to biometric password during login phase and also biometric authentication and authorization at request phase to operate any IoT device.

c. Message Modification Attacks

An attacker modifies the destination address to redirect a message to a new destination or modify data on a target computer in a message modification attack. Attacker cannot obtain valuable information from H (U_{id} || R_N), H (I_j || H(a)).

d. Illegitimate data access or control

An adversary or attacker cannot obtain a token due to integrated of token with computation of A_i. Value of B_i is computed using A_i. Attacker cannot construct valid A_i and B_i because he is unaware of the secrets a, b. Even if he has the user's device, an adversary will not be able to access an IoT device in smart home due to two-factor authentication, which requires both identity and biometric passwords (fingerprint and voice) to continue the procedure. Moreover, due to authorization and access control implementation, attacker will not be able to access an IoT device.

e. Spoofing attacks

A spoofing attack occurs when a program or person effectively impersonates another by falsifying data in order to obtain authorized access to legal information. This attack is not possible due to biometric password during login phase and also biometric authentication and authorization at request phase to operate any IoT device.

f. Man-in-the-Middle attack

In MITM attack, adversary listens, modifies and transmits message between user to server or user to IoT device. In our scheme MITM attack is not possible due to reason that adversary cannot obtain valuable information from H (U_{id} || R_N), H (I_j || H(a)).

5.1.2 Formal Authentication Analysis Using BAN logic

We have used well-known BAN-logic to do a formal analysis (e.g., authentication, session-key establishment, and freshness) of the proposed scheme. The reader can get further information [47] for BAN logic notations and rules. To validate the proposed scheme, we have used notations and symbols of BAN-logic as shown in table 5.1. Thereafter, goals, assumptions and idealized forms have been defined and BAN logic proof is conducted.

Table 5.1: Notations of BAN Logic

Notations	**Definition**
$B_{1,} B_2$	Two Principals
$C_{1,} C_2$	Two Statements
$B_1 \mid\equiv C_1$	B_1 believes C_1
$B_1 \lhd C_1$	B_1 receives C_1
$B_1 \mid\sim C_1$	B_1 sends C_1
$B_1 \mid\Rightarrow C_1$	B_1 controls C_1
$\#(B_1)$	B_1 is fresh
$B_1 \overset{K}{\Leftrightarrow} B_1'$	K is a secret known only to B_1 and B_1'
(B_1, B_2)	B_1 or B_2 is a part of formula (B_1, B_2)
$\{ B_1 \}_K$	B_1 is encrypted with K
$(B_1)_K$	B_1 is hashed with K
$B_1 \overset{K}{\leftrightarrow} B_2$	B_1 and B_2 have shared key K
B_1/ B_2	If B_1 then B_2
SK_{au}	Shared Key

5.1.2.1 Ban Logic Rules

The Basic Ban logic rules are as follows.

a. **Message meaning rule (MMR):**

$$\frac{B_1 \mid\equiv B_1 \overset{K}{\longleftrightarrow} B_2,\ B_1 \triangleleft (C_1)_K}{B_1 \mid\equiv B_2 \mid\sim C_1} \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(28)$$

b. **Nonce verification rule (NVR):**

$$\frac{B_1 \mid\equiv \#(C_1),\ B_1 \mid\equiv B_2 \mid\sim C_1}{B_1 \mid\equiv B_2 \mid\equiv C_1} \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(29)$$

c. **Jurisdiction rule (JR):**

$$\frac{B_1 \mid\equiv B_2 \mid\Longrightarrow C_1,\ B_1 \mid\equiv B_2 \mid\equiv C_1}{B_1 \mid\equiv C_1} \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(30)$$

d. **Belief rule (BR):**

$$\frac{B_1 \mid\equiv (C_1, C_2)}{B_1 \mid\equiv C_1} \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(31)$$

e. **Freshness rule (FR):**

$$\frac{B_1 \mid\equiv \#(C_1)}{B_1 \mid\equiv \#(C_1, C_2)} \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(32)$$

5.1.2.2 Goals

The following goals should be achieved by proposed scheme to show that U_r and A_d securely authenticate each other.

G_1: $U_r \mid\equiv V_2$

G_2: $A_d \mid\equiv V_1$

5.1.2.3 Idealized Forms

The idealized forms of the communicated messages during authentication in our scheme can be described as follows:-

$M_1 = U_r \longrightarrow A_d$: $(CU_i, Q_1, Q_2, V_1, E_k(R_u, Q_2, Req_1))$

$M_2 = A_d \longrightarrow U_r$: $(Q_3, V_2, E_{SK}(CM))$

5.1.2.4 Assumptions

Following are intuitive proof assumptions of proposed scheme for the BAN logic:

A_1: $U_r \mid\equiv \#(Q_2)$

A_2: $A_d \mid\equiv \#(Q_3)$

A_3: $U_r \mid\equiv A_d \mid\Longrightarrow R_N$

A_4: $A_d \mid\equiv U_r \mid\Longrightarrow R_V$

A_5: $U_r \mid\equiv U_r \overset{SK_{au}}{\longleftrightarrow} A_d$

A_6: $A_d \mid\equiv U_r \overset{SK_{au}}{\longleftrightarrow} A_d$

5.1.2.5 Ban Logic Proof

Following steps are performed for BAN logic proof:

Step 1: A_d receives M_1.

S_1: $A_d \triangleleft CU_i, Q_1, Q_2, V_1, E_k (R_u, Q_2, Req_1)$

Step 2: S_1 and A_6 is added in equation (28) to get S_2.

S_2: $A_d \mid\equiv U_r \mid\sim CU_i, Q_1, Q_2, V_1, E_k (R_u, Q_2, Req_1)$

Step 3: S_2 and A_1 is added in equation (32) to get S_3.

S_3: $A_d \mid\equiv \# CU_i, Q_1, Q_2, V_1, E_k (R_u, Q_2, Req_1)$

Step 4: S_2 and S_3 is added in equation (29) to get S_4.

S_4: $A_d \mid\equiv U_r \mid\equiv CU_i, Q_1, Q_2, V_1, E_k (R_u, Q_2, Req_1)$

Step 5: S_4 is added in equation (31) to get S_5.

S_5: $A_d \mid\equiv U_r \mid\equiv (V_1)$

Step 6: U_r receives M_2.

S_6: $U_r \triangleleft Q_3, V_2, E_{SK} (CM)$

Step 7: S_6 and A_5 is added in equation (28) to get S_7.

S_7: $A_d \mid\equiv U_r \mid\sim Q_3, V_2, E_{SK} (CM)$

Step 8: S_7 and A_2 is added in equation (32) to get S_8.

S_8: $A_d \mid\equiv \# Q_3, V_2, E_{SK} (CM)$

Step 9: S_7 and S_8 is added in equation (29) to get S_9.

S_9: $A_d \mid\equiv U_r \mid\equiv Q_3, V_2, E_{SK}$ (CM)

Step 10: S_9 is added in equation (31) to get S_{10}.

S_{10}: $A_d \mid\equiv U_r \mid\equiv (V_2)$

Step 11: From S_5 and S_{10}.

S_{11}: $U_r \mid\equiv A_d \mid\equiv U_r \xleftrightarrow{SK_{au}} A_d$

S_{12}: $A_d \mid\equiv U_r \mid\equiv A_d \xleftrightarrow{SK_{au}} U_r$

Step 12: Equation (30) is applied to S_{11} using A_3 and S_{12} using A_4 to get S_{13}.and S_{14}.

S_{13}: G_1: $U_r \mid\equiv V_2$ (Goal 1)

S_{14}: G_2: $A_d \mid\equiv V_!$ (Goal 2)

Finally, U_r is authenticated and authorized.

5.1.3 Comparison of Security Features

In this part, we shall compare the security features of our proposed model to those of other relevant schemes. Table 5.2 shows the outcomes of the comparison, our proposed scheme is compared with [8] [9] [10] [11] [12] schemes. Different scheme shows resilience against various types of attacks, however, no scheme shows resilience to all attacks listed in table 5.2. The attack listed in table are related to authentication of user, authorization of user and access control provision to user for operating different IoT devices. Our proposed scheme is resilient against all attacks listed in below table which means that scheme provides desired security characteristics that were highlighted as one of the research objectives. As a result, our system is more secure than the previously mentioned schemes.

Table 5.2: Comparison of Security Features

Scheme	[8]	[9]	[10]	[11]	[12]	Proposed
Replay attack	×	×	×	×	×	✓
Masquerade Attacks	x	×	✓	✓	×	✓
Message Modification Attacks	×	✓	✓	×	✓	✓
Illegitimate data access or control	×	×	×	✓	✓	✓
Spoofing attacks	✓	✓	×	✓	×	✓
Man-in-the-Middle attack	×	×	✓	×	✓	✓

5.2 Performance Analysis

IoT devices have limited and less resources which effects performance of a particular device. Performance of a system or device can be evaluated by using two methods: computation cost and communication overhead of system:

5.2.1 Computational Cost

Computation cost of proposed scheme has been evaluated according to encryption/ decryption and hash functions time cost. Efficiency of scheme is analyzed by comparing computation costs of our proposed scheme with other previous related schemes. Following notations have been used to calculate computation costs:

a. T_{H}: Time complexity of hash function.

b. $T_{Ek/Dk}$: Time complexity of encryption/decryption.

The time cost of symmetric-key encryption/ decryption and one-way hash function operations are 0.0056 sec and 0.00032 sec respectively. The values are as under:-

a. $T_H \approx 0.00032$ sec

b. $T_{Ek/Dk} \approx 0.0056$ sec

Table 5.3 shows the summary of Computation cost comparison of our proposed scheme with other previous related schemes. Comparison shows that efficiency of our proposed scheme is more than other schemes.

Table 5.3: Comparison of Computational Cost

Scheme	User	IoT Device	Administrator	Total
[8]	$8T_H \approx 0.00224$ *sec*	$6T_H \approx 0.0016$ *sec*	$9T_H \approx 0.00256$ *sec*	$23T_H \approx 0.0064$ *sec*
[9]	$12T_H \approx 0.00352$ *sec*	$8T_H \approx 0.00224$ *sec*	$15T_H \approx 0.00448$ *sec*	$35T_H \approx 0.01024$ *sec*
[10]	$9T_H + 2T_{EK/DK} \approx 0.01344$ *sec*	$5T_H + 2T_{EK/DK} \approx 0.01248$ *sec*	$9T_H + 4T_{EK/DK} \approx 0.02496$ *sec*	$23T_H + 8T_{EK/DK} \approx 0.05088$ *sec*
[11]	$6T_H + 2T_{EK/DK} \approx 0.01344$ *sec*	$5T_H + 2T_{EK/DK} \approx 0.01248$ *sec*	$6T_H + 2T_{EK/DK} \approx 0.01344$ *sec*	$17T_H + 6T_{EK/DK} \approx 0.02688$ *sec*
[12]	$9T_H \approx 0.00256$ *sec*	$6T_H \approx 0.0016$ *sec*	$9T_H \approx 0.00256$ *sec*	$24T_H \approx 0.00672$ *sec*
Proposed	$4T_H + 2T_{EK/DK} \approx 0.01344$ *sec*	$5T_H + 2T_{EK/DK} \approx 0.01344$ *sec*	$6T_H + 1T_{EK/DK} \approx 0.01344$ *sec*	$15T_H + 5T_{EK/DK} \approx 0.03248$ *sec*

5.2.2 Communication Overhead

Communication overhead is calculated by considering number of transmitted messages during authentication phases among entities. Efficiency of scheme is analyzed by comparing computation costs of our proposed scheme with other previous related schemes. Following notations have been used to calculate Communication overhead:-

a. Hash (SHA-1 hashing algorithm), Random nonce and identity: 128 bits

b. Block size of ciphertext (AES-128 is applied): 128 bits.

Three messages have been exchanged in our proposed protocol:

M_1= (U^R_{RP}, V_{Bio}, F_{Bio})

M_2= ($CU_i \| Q_1 \| Q_2 \| V_1 \| E_k (U_{id} \| Q_2 \| Req_1)$)

M_3= ($Q_3 \| V_2 \| E_{SK_{NV}} (CM)$)

Above messages requires 1408 bits during login phase and authentication phase. Table 5.4 shows the summary of communication cost and the number of messages exchanged of our proposed scheme with other previous related schemes. The message length (bits) transmitted or received by an entity is shown in below table e.g. (512/ 384) means that 512 bits message is transmitted by user and 384 bits received.

Table 5.4: Comparison of Communication Overhead

Scheme	**No. of messages to entity**		
	User	***IoT Device***	***Gateway***
[8]	*768/ 512*	*1152/ 768*	*768/ 512*
[9]	*640/ 384*	*1664/ 1152*	*1024/ 768*
[10]	*512/ 512*	*768/ 384*	*384/ 256*
[11]	*384/ 128*	*512/ 384*	*768/ 640*
[12]	*1024/ 768*	*1152/ 768*	*1024/ 640*
Proposed	*512/ 512*	*1024/ 768*	*384/ 640*

Chapter 6

Conclusion and Future Work

Scheme discussed is a distributed authentication and access control mechanism for accessing IoT devices in smart home to users allowed by owner or administrator. Additional advantages like anonymity and user unlinkability with smart devices for any outsider are acquired due to unique structure of the keying materials. Furthermore, the authentication technique may be integrated with various mechanisms of access control with ease. Use of user biometrics in our system, this scheme also avoids smart card theft and password guessing attacks. We have used BAN logic analysis to validate the scheme’s correctness. This scheme prevents system from replay attack by adding time stamp in request message. The performance analysis i-e computation cost and communication cost comparisons of our scheme with other schemes shows that efficiency of proposed scheme is more than other schemes. In the future work, we plan to implement the proposed scheme in practice.

References

[1] Prosanta Gope, Tzonelih Hwang, “BSN-Care: A Secure IoT-based Modern Healthcare System Using Body Sensor Network” IEEE Sensors Journal, Volume: 16, Issue: 5, March1, 2016.

[2] W. Iqbal, H. Abbas, P. Deng; J. Wan; B. Rauf; Y. Abbas; I. Rashid, "ALAM: Anonymous Lightweight Authentication Mechanism for SDN Enabled Smart Homes," in IEEE Internet of Things Journal, Volume: 8, Issue: 12, June 2021, doi: 10.1109/JIOT.2020.3024058.

[3] S. Kavianpour, B. Shanmugam, S. Azam , M. Zamani , G. Narayana Samy, F. De Boer "A Systematic Literature Review of Authentication in Internet of Things for Heterogeneous Devices", Journal of Computer Networks and Communications, vol. 2019, Article ID 5747136, 14 pages, 2019.

[4] Mohammed El-hajj, Ahmad Fadlallah, Maroun Chamoun and Ahmed Serhrouchni, “A Survey of Internet of Things (IoT) Authentication Schemes”, 2019 Sensors. 10.3390/s19051141.

[5] A. Siswanto, N. Katuka, K. Ruhana, “Biometric Fingerprint Architecture for Home Security System” The 3rd Innovation and Analytics Conference & Exhibition (IACE) 2016, Sintok, Kedah, Malaysia.

[6] F. Afandi and R. Sarno, "Android Application for Advanced Security System based on Voice Recognition, Biometric Authentication, and Internet of Things,"

2020 International Conference on Smart Technology and Applications (ICoSTA), Surabaya, Indonesia, 2020, pp. 1-6, doi: 10.1109/ICoSTA48221.2020.1570615292.

[7] R. Dinar Hayu Arifin and R. Sarno, "Door automation system based on speech command and PIN using Android smartphone," 2018 International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, 2018, pp. 667-672, doi: 10.1109/ICOIACT.2018.8350715.

[8] Yan Meng, Wei Zhang, Haojin Zhu, and Xuemin Sherman Shen. "Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures." IEEE Wireless Communications 25, no. 6 (2018): 53-59.

[9] Lei Zhang, Yan Meng, Jiahao Yu, Chong Xiang, Brandon Falk, and Haojin Zhu. "Voiceprint mimicry attack towards speaker verification system in smart home." In IEEE INFOCOM 2020-IEEE Conference on Computer Communications, pp. 377-386. IEEE, 2020.

[10] Salahaldeen Duraibi, Frederick T. Sheldon and Wasim Alhamdani “Voice Biometric Identity Authentication Model for IoT Devices” in International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 9, No 1/2, May 2020.

[11] Changchun Yang, "Design of Smart Home Control System Based on Wireless Voice Sensor", Journal of Sensors, vol. 2021, Article ID 8254478, 11 pages, 2021. https://doi.org/10.1155/2021/8254478.

[12] Sitalakshmi Venkatraman, Anthony Overmars, and Minh Thong. "Smart Home Automation—Use Cases of a Secure and Integrated Voice-Control System" Systems 2021, 9, no. 4: 77. https://doi.org/10.3390/systems9040077.

[13] Ahmed Ismail, Samir Abdlerazek, and Ibrahim M. El-Henawy. "Development of Smart Healthcare System Based on Speech Recognition Using Support Vector Machine and Dynamic Time Warping" Sustainability 2020, 12, no. 6: 2403. https://doi.org/10.3390/su12062403

[14] B. Chifor, S. Arseni, I. Matei and I. Bica, "Security-Oriented Framework for Internet of Things Smart-Home Applications," 2019 22nd International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 2019, pp. 146-153, doi: 10.1109/CSCS.2019.00033.

[15] A. Munir, S. Kashif Ehsan, S. M. Mohsin Raza and M. Mudassir, "Face and Speech Recognition Based Smart Home," 2019 International Conference on Engineering and Emerging Technologies (ICEET), Lahore, Pakistan, 2019, pp. 1-5, doi: 10.1109/CEET1.2019.8711849.

[16] William Jang, Adil Chhabra, and Aarathi Prasad. "Enabling multi-user controls in smart home devices." In Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, pp. 49-54. 2017.

[17] Maanak Gupta and Ravi Sandhu, ”Authorization Framework for Secure Cloud Assisted Connected Cars and Vehicular Internet of Things”. In Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies

(SACMAT '18). Association for Computing Machinery, New York, NY, USA, 193–204, 2018. https://doi.org/10.1145/3205977.3205994.

[18] Salah Zemmoudj, Nabila Bermad and Mawloud Omar, “Context-aware pseudonymization and authorization model for IoT-based smart hospitals”. Journal of Ambient Intelligence and Humanized Computing, Springer, 2019.

[19] Mang Su, Bo Zhou, Anmin Fu, Yan Yu and Gongxuan Zhang, "PRTA: A Proxy Re-encryption based Trusted Authorization scheme for nodes on CloudIoT", Information Sciences, Volume 527, 2020, Pages 533-547, https://doi.org/10.1016/j.ins.2019.01.051.

[20] Nor Syazwani Md Noh, Haryati Jaafar, Wan Azani Mustafa, Syed Zulkarnain Syed Idrus, A. H. Mazelan, “Smart Home with Biometric System Recognition,” 2020 J. Phys.: Conf. Ser. 1529 042020.

[21] Eric Zeng and Franziska Roesner. "Understanding and improving security and privacy in multi-user smart homes: a design exploration and in-home user study." In 28th {USENIX} Security Symposium ({USENIX} Security 19), pp. 159-176. 2019.

[22] Shehzad Ashraf Chaudhry, Azeem Irshad, Jamel Nebhen, Ali Kashif Bashir, Nour Moustafa, Yasser D. Al-Otaibi and Yousaf Bin Zikria “An Anonymous Device to Device Access Control based on Secure Certificate for Internet of Medical Things Systems”. Sustainable Cities and Society. 75. (2021). 103322. 10.1016/j.scs.2021.103322.

[23] Fagen Li, Yanan Han and Chunhua Jin, "Practical access control for sensor networks in the context of the Internet of Things". Computer Communications, Volumes 89-90, 2016, Pages 154-164, https://doi.org/10.1016/j.comcom.2016.03.007.

[24] Ming Luo, Yi Luo, Yuwei Wan and Ze Wang, "Secure and Efficient Access Control Scheme for Wireless Sensor Networks in the Cross-Domain Context of the IoT", *Security and Communication Networks*, vol. 2018, Article ID 6140978, 10 pages, 2018. https://doi.org/10.1155/2018/6140978

[25] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Durmuth, Earlence Fernandes and Blase Ur, “Rethinking Access Control and Authentication for the Home Internet of Things (IoT)”. 27th USENIX Security Symposium (USENIX Security 18), 2018, pages 255-272.

[26] Amit Kumar Sikder, Leonardo Babun, Z. Berkay Celik, Abbas Acar, Hidayet Aksu, Patrick McDaniel, Engin Kirda and A. Selcuk Uluagac, "Kratos: Multi-user multi-device-aware access control system for the smart home." *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 2020.

[27] Taqiyah Ghazali, Zakaria, Nur Haryani, “Security, comfort, healthcare, and energy saving: A review on biometric factors for smart home environment”, 2018 Journal of Computers Vol. 29 No. 1, 2018, pp. 189-208, doi: 10.3966/199115992018012901017.

[28] I. Vorobyeva, D. Guriel, M. Ferguson and H. Oladapo, "Benefits and issues of biometric technologies. Are biometrics worth using?," IEEE SOUTHEASTCON 2014, Lexington, KY, 2014, pp. 1-8, doi: 10.1109/SECON.2014.6950706.

[29] Kavallieratos, Georgios, Nabin Chowdhury, Sokratis Katsikas, Vasileios Gkioulos, and Stephen Wolthusen. "Threat Analysis for Smart Homes" Future Internet 11, no. 10: 207. (2019) https://doi.org/10.3390/fi11100207

[30] Ali, Bako, and Ali I. Awad. "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes" Sensors 18, no. 3: 817. (2018), https://doi.org/10.3390/s18030817

[31] A. Collen, N. A. Nijdam, J. Augusto-Gonzalez, S. K. Katsikas, K. M. Giannoutakis, G. Spathoulas, E. Gelenbe, K. Votis, D. Tzovaras, N. Ghavami, M. Volkamer, P. Haller, A. Sánchez and M. Dimas. “GHOST - Safe-Guarding Home IoT Environments with Personalised Real-Time Risk Control”. Security in Computer and Information Sciences. Euro-CYBERSEC 2018. Communications in Computer and Information Science, vol 821. Springer, Cham. https://doi.org/10.1007/978-3-319-95189-8_7

[32] G. Kavallieratos, V. Gkioulos and S. K. Katsikas, "Threat Analysis in Dynamic Environments: The Case of the Smart Home," 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), 2019, pp. 234-240, doi: 10.1109/DCOSS.2019.00060.

[33] Amar Seeam, Ochanya S. Ogbeh, Shivanand Guness and Xavier Bellekens, "Threat Modeling and Security Issues for the Internet of Things," 2019 Conference on Next Generation Computing Applications (NextComp), 2019, pp. 1-8, doi: 10.1109/NEXTCOMP.2019.8883642.

[34] S. Karthick, N. Gomathi, R. P. Mahapatra, Anitha Rajakumari and Pritee Parwekar, “Various Security Problems and Its Solving for Future Dynamic IoT-Based Smart Home Automation”. In Proceedings of International Conference on Recent Trends in Computing . Lecture Notes in Networks and Systems, vol 341, (2022), Springer, Singapore. https://doi.org/10.1007/978-981-16-7118-0_63

[35] Ivan Cvitić, Dragan Peraković, Marko Periša and Mirjana D. Stojanović, "Novel Classification of IoT Devices Based on Traffic Flow Features," Journal of Organizational and End User Computing (JOEUC) 33, no.6: 1-20. http://doi.org/10.4018/JOEUC.20211101.oa12

[36] Haseeb Touqeer, Shakir Zaman, Rashid Amin, Mudassar Hussain, Fadi Al-Turjman and Muhammad Bilal, “Smart home security: challenges, issues and solutions at different IoT layers”. J Supercomput 77, 14053–14089 (2021). https://doi.org/10.1007/s11227-021-03825-1

[37] Oludare Isaac Abiodun, Esther Omolara Abiodun, Moatsum Alawida, Rami S. Alkhawaldeh and Humaira Arshad, “A Review on the Security of the Internet of Things: Challenges and Solutions”. Wireless Pers Commun 119, 2603–2637 (2021). https://doi.org/10.1007/s11277-021-08348-9

[38] Mohamed Abdel-Basset, Nour Moustafa, Hossam Hawash and Weiping Ding, “Internet of Things Security Requirements, Threats, Attacks, and Countermeasures”. In: Deep Learning Techniques for IoT Security and Privacy. Studies in Computational Intelligence, vol 997, (2022). Springer, Cham. https://doi.org/10.1007/978-3-030-89025-4_3

[39] Aram Kim, Junhyoung Oh, Jinho Ryu and Kyungho Lee, "A Review of Insider Threat Detection Approaches With IoT Perspective," in IEEE Access, vol. 8, pp. 78847-78867, 2020, doi: 10.1109/ACCESS.2020.2990195.

[40] Raveendranadh Bokka and Tamilselvan Sadasivam, “Deep Learning Model for Detection of Attacks in the Internet of Things Based Smart Home Environment”. In Proceedings of International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications. Advances in Intelligent Systems and Computing, vol 1245. (2021). Springer, Singapore. https://doi.org/10.1007/978-981-15-7234-0_69

[41] Ryan Heartfield, George Loukas, Sanja Budimir, Anatolij Bezemskij, Johnny R.J,.Fontaine, Avgoustinos Filippoupolitis and Etienne Roesch, “A taxonomy of cyber-physical threats and impact in the smart home”. Computers & Security, Volume 78, 2018, Pages 398-428, https://doi.org/10.1016/j.cose.2018.07.011.

[42] Vincent Omollo Nyangaresi, "ECC Based Authentication Scheme for Smart Homes," 2021 International Symposium ELMAR, 2021, pp. 5-10, doi: 10.1109/ELMAR52657.2021.9550911.

[43] Ruqaiya Khan, Vinod Kumar Shukla, Bhopendra Singh and Sonali Vyas, “Mitigating Security Challenges in Smart Home Management Through Smart Lock”. In: Data Driven Approach Towards Disruptive Technologies. Studies in Autonomic, Data-driven and Industrial Computing. Springer, Singapore. (2021). https://doi.org/10.1007/978-981-15-9873-9_7

[44] Tarek Gaber, Amir El-Ghamry and Aboul Ella Hassanien, “Injection attack detection using machine learning for smart IoT applications”. Physical Communication, Volume 52, 2022, 101685, https://doi.org/10.1016/j.phycom.2022.101685.

[45] Ziarmal Nazar Mohammad, Fadi Farha, Adnan O. M. Abuassba, Shunkun Yang and Fang Zhou, "Access control and authorization in smart homes: A survey," in Tsinghua Science and Technology, vol. 26, no. 6, pp. 906-917, Dec. 2021, doi: 10.26599/TST.2021.9010001.

[46] Talal A.A Abdullah, Waleed Ali, Sharaf Malebary and Adel Ali Ahmed, “A Review of Cyber Security Challenges, Attacks and Solutions for Internet of Things Based Smart Home”. IJCSNS International Journal of Computer Science and Network Security, VOL.19 No.9, September 2019

[47] Michael Burrows, Martin Abadi and Roger Needham, "A logic of authentication," Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, vol. 426, no. The Royal Society London, pp. 233--271, 1989.