

Enhancing QoS and Security in IP Multimedia Subsystem (IMS) Using Virtual Machines



Ph.D (Computer Science)

By

Mahmood ul Hassan
Reg# 68-FBAS/PHDCS/F11

Supervisor

Dr. Qaisar Javaid, Assistant Professor
Department of CS&SE, IIU, Islamabad

**Department of Computer Science & Software Engineering
Faculty of Basic & Applied Sciences
International Islamic University, Islamabad
2022**

TH-28015th

PHD

2015

MAE

Virtual reality
Multimedia (subsystem)
Virtual Machines

A dissertation submitted to the
Department of Computer Science & Software Engineering,
International Islamic University, Islamabad
as a partial fulfillment of the requirements
for the award of the degree of
Doctor of Philosophy in Computer Science

Final Approval

It is certified that we have read this thesis, entitled “**Enhancing QoS and Security in IP Multimedia Subsystem (IMS) Using Virtual Machines**” submitted by **Mr. Mahmood ul Hassan Reg No. 68-FBAS/PHDCS/F11**. It is our judgment that this thesis is of sufficient standard to warrant its acceptance by the International Islamic University Islamabad for the award of the PhD degree in Computer Science

Committee

External Examiner

Prof. Dr. Muhammad Zubair
Dean, Faculty of Computing,
Riphah University, Islamabad



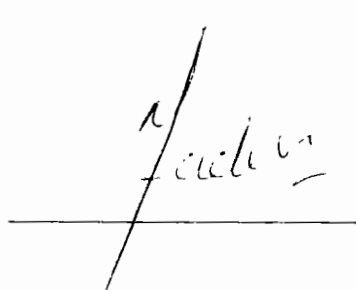
External Examiner

Dr. Muhammad Muzammil
Assistant Professor, DCS,
Bahria University, Islamabad



Internal Examiner

Dr. Muhammad Nadeem
Assistant Professor,
Department of Computer Science & Software Engineering,
FBAS, IIUI



Supervisor

Dr. Qaisar Javaid
Assistant Professor,
Department of Computer Science & Software Engineering,
FBAS, IIUI



Declaration

I hereby declare that this thesis, neither as a whole nor as a part thereof has been copied out from any source. It is further declared that no portion of the work presented in this report has been submitted in support of any application for any other degree or qualification of this or any other university or institute of learning.



Mahmood ul Hassan

Dedication

This thesis is dedicated to my family, especially to my father, my mother, wife and my sons.



Mahmood ul Hassan

Acknowledgments

This thesis and all my efforts are fruitful only due to Allah Almighty, the Most Merciful and Beneficent, Who gave me strength to complete this task to the best of abilities and knowledge. I would like to thank my supervisor **Dr. Qaisar Javaid**, who gave all their knowledge, guidance and support to boost my confidence and learning. I would also like to thank my wife who has supported patiently and firmly during completion of my task.

I would also like to acknowledge my friends, students and all of them encouraged and provided technical support to me. I must admit without their sincere support, I was not able to complete this task. I would like to admit that I owe all my achievements to my truly, sincere and most loving parents, sister, brothers and friends who mean the most to me, and whose prayers have always been a source of determination for me.

Abstract

One of the important goals in the design of next generation networks is to provide quality of service and security to the users. With the rapid increase in number of telecommunication users, the security objective as well as providing heterogeneous type of services at differentiated quality of service (QoS) levels underscores the need for deployment of advanced network solutions. Both of the defined objectives have emerged as a wide research area during the last few years. In connection with the above mentioned goals, we have investigated the Policy and Charging Control (PCC) architecture concepts in this research and propose a corresponding framework ensuring secure QoS levels with the use of virtual machines, a crucial need for next generation networks.

In the last few years, the Virtualization technique has proved as a crucial requirement of cloud computing. This technique is used for efficient computing as well as optimal utilization of hardware resources. In the proposed system we employed the same virtualization technique in the form of virtualized IMS machines. Different devices having IP-based connectivity such as mobile device, laptop, PC, IP phone etc. can be used for establishing a connection with such virtual machines or servers. With the use of virtual machines in the proposed architecture, we have managed to reduce the session setup delay, increase the scalability of the system, make the user equipment lightweight, and enhance the resource utilization.

Moreover, to further enhance the security and efficiency of the IP Multimedia Subsystem (IMS) framework we investigated and analyzed the state-of-the-art Session Initiation Protocol (SIP) protocols. SIP, being an underlying constituent protocol for IMS framework, is used to establish, maintain and terminate the communicative sessions. In the last decade, many SIP based authentication protocols have been introduced; however security limitations render those protocols unfeasible for practical deployments. One of the recent works related to SIP based authentication protocols was presented by Lu et al., Chaudhary et al, and Dongqing et al. We discovered few limitations in Dongqing et al. including the susceptibility to privileged insider attack, Denial of Service (DOS) attack and session specific temporary information attack. Then

we proposed an enhanced SIP authentication protocol bearing secure and efficient features. Besides, the Dongqing et al. assumes a strictly time synchronized system, which limits the practical effectiveness of the protocol for a real environment. To counter the discussed limitations and threats as posed to Dongqing et al., we proposed an improved SIP authentication scheme. This is evident from the results that our proposed scheme supports 50% more security features than Dongqing et al. The strong security features of our work are proved under formal security analysis such BAN logic and validated using automated PROVERIF tool.

Contents

1. Introduction	1
1.1 IP Multimedia Subsystem	1
1.1.1 Quality of Service (QoS) in 3G Access	5
1.2 Problem Statement	7
1.3 Research Objectives	7
1.4 Research Contribution	8
1.5 Summary	9
2. IP Multimedia Subsystem	10
2.1 Architectural requirements of IP Multimedia Subsystem	10
2.1.1 IP Multimedia Sessions	10
2.1.2 IP Connectivity	10
2.1.3 Requirements of QoS in IP Multimedia services	13
2.1.4 IP policy control for ensuring correct usage of media resources	13
2.1.5 Communication Security	13
2.1.6 Support of roaming	14
2.1.7 Interworking with other networks	15
2.1.8 Service Control Model	15
2.1.9 Service development	15
2.2 IMS entities and their functionalities	16
2.2.1 Call Session Control Functions	16
2.2.1.1 Proxy Call Session Control Function	16
2.2.1.2 Interrogating Call Session Control Function	18
2.2.1.3 Serving Call Session Control Function	18
2.3 Databases	19
2.4 Service Functions	20
2.5 Registration	21
2.6 Identification of Users	23
2.6.1 Private User Identity	23
2.6.2 Public User Identity	23

2.6.3 Derived Public User Identity and Private User Identity	24
2.7 Identification of Services (Public Service Identities)	24
2.8 Identification of Network Entities	25
2.9 IP Multimedia Services Identity Module	25
2.10 Universal Subscriber Identity Module	25
2.11 Discovering the IMS Entry Point.....	25
2.11.1 S-CSCF Assignment	26
2.12 Quality Mechanism	26
2.12.1 Quality of Service Protocols	27
2.12.2 Policy-based QoS Architectures	29
2.12.3 Quality of Service Management	29
2.12.3.1 Traffic Policing	29
2.12.3.2 Peak Information Rate	30
2.12.3.3 Committed Information Rate	30
2.12.3.4 Committed Burst Size	30
2.12.3.5 PBS	30
2.12.3.6 Traffic Shaping	30
2.13 Quality of Service Attributes related to Policy Decision Point	30
2.13.1 QoS Parameters Related to Policy Control.....	31
2.13.2 QoS Class Identifier (QCI)	31
2.13.3 Allocation and Retention Priority (ARP)	31
2.13.4 Guaranteed Bit Rate (GBR)/Non-Guaranteed Bit Rate (Non-GBR).....	31
2.14 Summary	31
3. Cloud Computing.....	33
3.1 Introduction	33
3.2 Characteristics of Cloud Computing.....	33
3.3 Service Models	34
3.3.1 Software as a Service (SaaS)	34
3.3.2 Platform as a Service (PaaS).....	35

3.3.3 Infrastructure as a Service (IaaS)	35
3.4 Types of cloud.....	35
3.4.1 Private Cloud	35
3.4.2 Community Cloud	35
3.4.3 Public Cloud	36
3.4.4 Hybrid Cloud	36
3.5 Scalability	36
3.5.1 Vertical Scaling.....	36
3.5.2 Horizontal Scaling	37
3.6 Cloud Elastically	37
3.7 Virtualization	38
3.7.1 Virtual Machine Manager (VMM)	38
3.8. Virtualization in IP Multimedia Subsystem& Literature Review.....	39
3.8.1 Virtualization of IP Multimedia Subsystem Client.....	39
3.8.2 Integration of IMS-PCC Architecture with Virtualization IMS Client Model	41
3.8.3 Roaming.....	41
3.8.4 Virtual IMS Client Architecture	41
3.8.4.1 Details of QoS and Virtual IMS Client.....	42
3.8.4.2 Quality of Service (QoS) in 3G Access	42
3.8.5. Literature Review.....	43
3.9. Summary	49
4. Proposed System Virtualization.....	50
4.1 Introduction.....	50
4.2 Provision of Quality of Service.....	50
4.3 Support of Equipment.....	52
4.4 System evaluation	53
4.4.1 Process Delay in OpenIMS	53
4.4.2 CPU utilization Measurement	54
4.6 Advantages of the Proposed Model	57

4.7 Summary	57
5. Security Fundamentals	58
5. 1 Introduction.....	58
5.1.1 Password Guessing Attacks	58
5.1.2 Replay Attacks	58
5.1.3 Man-in-the-middle Attacks	58
5.1.4 Stolen-verifier Attacks	59
5.1.5 Denning-Sacco Attacks.....	59
5.1.6 Registration Attacks.....	59
5.1.7 Known-key Security	59
5.1.8 Session key Security	59
5.1.9 Perfect Forward Secrecy	60
5.1.10 Mutual Authentication	60
5.2 Review of HTTP Digest Authentication Scheme for SIP.....	60
5.3. SIP Authentication Mechanisms.....	61
5.3.1 Authentication Methods Based on Diffie Hellman:	62
5.3.2Authentication Methods Based on Elliptic Curve cryptography.....	62
5.3.3 Authentication Methods Based on Nonces	63
5.4 Authentication Methods Based on Identity Based Encryption	63
5.5 Authentication Using Smart Card	64
5.5.1 A Single Round-Trip SIP Authentication Scheme for Voice over Internet ProtocolUsing Smart Card	65
5.5.2 Comparison and Cost Analysis.....	66
5.6 Summary	68
6. Proposed System Security	69
6.1 Introduction.....	69
6. 2. Preliminaries	70
6.2.1 Hash Function	70

6.2.2 Elliptic Curve essentials.....	70
6.2.3 Bio-hashing.....	71
6.3. Working and Crypanalysis of Dongqing et al Scheme.....	71
6.3.1 Working of Dongqing et al. protocol.....	71
6.3.1.1 Server Registration Phase.....	72
6.3.1.2 User Registration Phase.....	73
6.3.1.3 Mutual Authentication Procedure.....	73
6.3.2 Weaknesses in Dongqing et al. protocol.....	73
6.3.2.1 Privileged Insider threat.....	73
6.3.2.2 Session Specific Temporary Information threat.....	74
6.3.2.3 Denial of Service (DoS) Attack.....	74
6.3.2.4 Time-synchronization Problem.....	75
6.4. Proposed Model.....	75
6.4.1 Initialization Phase.....	75
6.4.2 Registration Procedure.....	75
6.4.3 Mutual Authentication Procedure.....	76
6.4.4 Password Modification Phase.....	78
6.5 Security Analysis.....	78
6.5.1 Security Discussion.....	78
6.5.1.1 Replay Attacks.....	78
6.5.1.2 Offline-Password Guessing Threat.....	79
6.5.1.3 Stolen Verifier Attacks.....	79
6.5.1.4 Stolen Smart Card Threat.....	79
6.5.1.5 Session Key Security.....	80
6.5.1.6 Known-Key Security.....	80
6.5.1.7 Perfect Forward Secrecy.....	80
6.5.1.8 Mutual Authentication.....	81
6.5.1.9 Anonymous Authentication.....	81
6.5.1.10 Privileged Insider Attack.....	81
6.5.1.11 Session-Specific Temporary Information Threat.....	82

6.5.2 Automated Security Verification	82
6.5.3 Formal Security Analysis (BAN Logic)	87
6. 6 Performance Evaluation Analysis.....	90
6.7. Summary	92
7. Conclusion and Future Work	93
References.....	95

List of Figures

Figure 1.1 Policy and charging control architecture in IMS.....	4
Figure 1.2 3G access message sequence for QoS provisioning.....	6
Figure 2.1 Users roaming and connectivity options	12
Figure 2.2 IMS/CS roaming cases	14
Figure 2.3 Role of S-CSCF in routing	19
Figure 2.4 HSS.....	20
Figure 2.5 IMS registration.....	22
Figure 3.1. IMS client virtualization.....	40
Figure 3.2. Virtual IMS client PCC architecture	42
Figure 3.3 QoS provisioning in 3 G access.....	43
Figure 4.1 Proposed model	51
Figure 4.2 Message standard and processed model process delay	53
Figure 4.3 :Comparison between standard and proposed P-CSCF CPU utilization.....	54
Figure 4.4 :Comparison between standard and proposed I-CSCF CPU utilization	54
Figure 4.5 :Comparison between standard and proposed S-CSCF CPU utilization.....	55
Figure 4.6:Comparison between standard and proposed HSS CPU utilization.....	55
Figure 5.1. HTTP digest authentication scheme.....	61
Figure 5.2. Proposed authentication model.....	65
Figure 6.1. Flow of registration, login and authentication phase of Dongqing et al. model.....	72
Figure 6.2. Proposed authentication protocol	77
Figure 6.3. Channels, constructor, destructor, events and equations.....	84
Figure 6.4: UserUi process	85
Figure 6.5. ServerSj process	86

List of Tables

Table 5.1. Comparison between Zhang et al, and Azeen et al. protocol	67
Table 5.2: Attacks on protocols under different conditions.....	68
Table 6.1. Notations	72
Table 6.2: Comparison for multi-server schemes	91
Table 6.3: Computational comparison	92

List of Abbreviations

3GPP	3rd Generation Partnership Project
AAA	Authentication, Access and Accounting
AUC	Authentication Centre
BAN	Burrows-Abadi-Needham Logic
BGCF	Breakout Gateway Control Function
CAMEL	Customized Applications for Mobile Network Enhanced Logic
CBS	Committed Burst Size
CDHP	Computational Diffie–Hellman Problem
CIR	Committed Information Rate
CN	Core Network
CSCF	Call Session Control Functions
CSE	CAMEL Service Environment
DLP	Discrete Logarithm Problem
DoS	Denial of Service
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithm Problem
ESM	Elliptic Scalar Multiplication
ETSI	European Telecommunications Standards Institute
GBR	Guaranteed Bit Rate
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
H-PCRF	Home PCRF
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem

IMS-MGW	IMS Media Gateway
IP CAN	IP-Connectivity Access Network
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITU	International Telecommunication Union
MCC	Mobile Country Code
MGCF	Media Gateway Control Function
MNC	Mobile Network Code
MRFC	Multimedia Resource Function Controller
OCS	Online Charging System
OSA	Open Services Architecture
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy Call Session Control Function
PDF	Policy Decision Function
PDP	Packet Data Protocol
PEP	Policy Enforcement Point
PIR	Peak Information Rate
PS	Packet Switched
PSTN	Public Switched Telephone Network
QCI	QoS Class Identifier
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
ROM	Random Oracle Model
RTP	Real-time Transport Protocol
SA	Security Associations
S-CSCF	Serving Call Session Control Function
SGSN	Serving GPRS Support Node

SGW	Signaling Gateway
SIP	Session Initiation Protocol
SIP ECC	Session Initiation Protocol Elliptic Curve Cryptography
SLF	Subscription Location Function
SSH	Secure Shell
SSL	Secure Socket Layer
THIG	Topology Hiding Inter-network Gateway
TISPAN	Telecoms & Internet Converged Services & Protocols for Advanced Networks
TCP	Transmission Control Protocol
UMTS	Universal Mobile Telecommunications System
VoD	Video on Demand
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network

List of Publications

1. Hassan, M. U., Chaudhry, S. A., & Irshad, A, "An Improved SIP Authenticated Key Agreement Based on Dongqing et al," *Wireless Personal Communications*, pp. 110(4), 2087-2107., 2020.
2. Irshad, A., Sher, M., Rehman, E., Ch, S. A., Hassan, M. U., & Ghani, A, "A single round-trip sip authentication scheme for voice over internet protocol using smart card," *Multimedia Tools and Applications*, pp. 74(11), 3967–3984, 2015.
3. Irshad, A., Sher, M., Faisal, M. S., Ghani, A., Hassan, M. U, & Ashraf Ch, S, "A secure authentication scheme for session initiation protocol by using ECC on the basis of the Tang and Liu scheme," *Security and Communication Networks*, pp. 7(8), 1210–1218, 2014.

1. Introduction

With the rapid increase in the number of telecommunication users, the heterogeneous type of services at differentiated quality of service levels underlines the requirements of the deployment of advanced network solutions. The simultaneous handling of traffic flows, web browsing, grid computing, Video on Demand (VoD) needs requires special network capabilities. The IP Multimedia Subsystem (IMS) which is given in 3rd Generation Partnership Project and accepted by other standardization bodies including European Telecommunications Standards Institute (ETSI)/ Telecoms & Internet converged Services & Protocols for Advanced Networks (TISPAN), is the foundation of the next generation networks (NGN) [1].

The IP Multimedia Subsystem uses SIP and is based on generic architectural framework. SIP is used for communication including various types of media e.g. voice, video and data communication services to mobile networks as well as fixed networks [2][3]. The IP multimedia subsystem provides access independent and frequent mechanisms for authentication, security, charging and Quality of Service etc. In release [4] policy enforcement and charging policy of IMS have been described in detail. Policy and charging control architecture fulfill this requirement. Policy enforcement is used for QoS in PCC architecture e.g. a user uses limited bandwidth during certain hours. In [5] IP Multimedia Subsystem/ Policy and Charging Control (IMS/PCC) architecture has been implemented in combination with virtualized IMS client.

1.1 IP Multimedia Subsystem

Different functional elements are implemented by the IMS core [2] for the sake of call control. The proxy CSCF, the interrogating Call Session Control Function and the Serving CSCF are the three functional elements [5]. IMS is based on Session Initiation Protocol and its major entities consist of Session Initiation Protocol proxies.

These Session Initiation Protocol servers are referred to as Call Service Control Functions. To communicate with these proxies, the user device has to apply the functionality of Session Initiation Protocol user agent. For registration and session establishment all call session control functions have to play a vital role. Each Call Session Control Function

performs specific task. All functions also send data to a function that handles offline charging. Details are depicted in Figure 1.1

Proxy-CSCF is the first point where user communicate with the IMS. SIP signaling coming from the user equipment is forwarded to the Proxy CSCF. The terminating SIP signals are directed from the Proxy Call Session Control Function to User Equipment(UE). The specific tasks associated with the Proxy CSCF consisted of SIP compression and interaction with Policy Decision Function(PDF). IPsec security association as well as emergency session detection tasks are also associated with the Proxy CSCF [6].

The Proxy CSCF can compress SIP messages if the User Equipment (UE) wants to receive signaling messages in compressed form. The Proxy CSCF can also uncompress SIP messages. For SIP signalling, Proxy CSCF keeps the Security Associations and applies confidential safeguard and integrity. This prevents any sort of spoofing attacks and replay attacks. When an operator is keen to apply Service-Based Local Policy, the Proxy CSCF establishes a session and media oriented information to the PDF. Proxy CSCF is also responsible for emergency session detection.

The Interrogating- CSCF which is a type of Session Initiation Protocol proxy is situated at the administrative functional domain of the IMS [7]. It finds the location of a particular UE from the Home Subscriber Server (HSS) and directs the UE's messages to its assigned S-CSCF [7]. The I-CSCF obtains the name of S-CSCF from the Home Subscriber Server. It forwards any SIP request or response to the Session-CSCF. To hide functionality of gateway between networks[6].

The functions of the Serving Call Session Control Function include registration procedures, routing related decisions and maintains session states and also stores profiles of various services, which need to be implemented. When a user has to make a registration request, the request is sent to the S-CSCF.

A challenge is generated to the user equipment upon obtaining the authenticated data from the Home Subscriber Server by the S-CSCF. After getting and verifying the response, the Serving-

CSCF gets the registration and initiates monitoring the registration level. During the registration process, the S-CSCF downloads a service profile which is stored in the Home Subscriber Server. S-CSCFs are always located in the home domain of the users, they serve [1]. The HSS stores master data depository services and provides the IMS network components for handling different calls and all types of service sessions. User-to-user services or user-to-network services are made possible by the applications servers.

Figure 1.1 shows the Policy and charging control architecture in IMS. The existing Policy and Charging Control (PCC) architecture is result of succession of 3GPP Releases. The Release 8 introduced two key entities. One is termed as the policy and charging rules function, and the other is known as Policy and Charging Enforcement Point. To ensure synchronization and implementation of QoS policy rules between the signaling and the transport layer, the Policy and Charging Rules Function (PCRF) enforces these rules [9]. Policy decisions made by policy and charging rules functions are enforced by the Policy and Charging Enforcement Point. Policy and Charging Enforcement Point is present in the Packet Data Network Gateway that establishes a connection between UE and external Packet Data Networks (PDNs). In WLAN access Packet Data Network Gateway is the router at edge in the home domain that makes link to the external networks. Two types of charging system are used in IMS as described in [9] one is Online Charging System which is used for prepaid type charging and other is offline type charging meant for Postpaid charging. Different access technologies have the ability to have access to IMS in different approaches. To add a device a proper interface with IMS core is required. e.g in 3GPP access S-GPRS Support Node present in the Serving gateway is used. For recovery of the user profile and implementations of its preferences, a kind of access control as well as a bridge to IMS access is employed. For the achievement of these objectives these entities should have a support of number of functions. These are Authentication functions, Access functions and Accounting functions. The QoS and enforcement of different policies i.e limits of bandwidth, time limitation etc. In case of WLAN, the AAA Peer and WLAN Access Gateway is used.

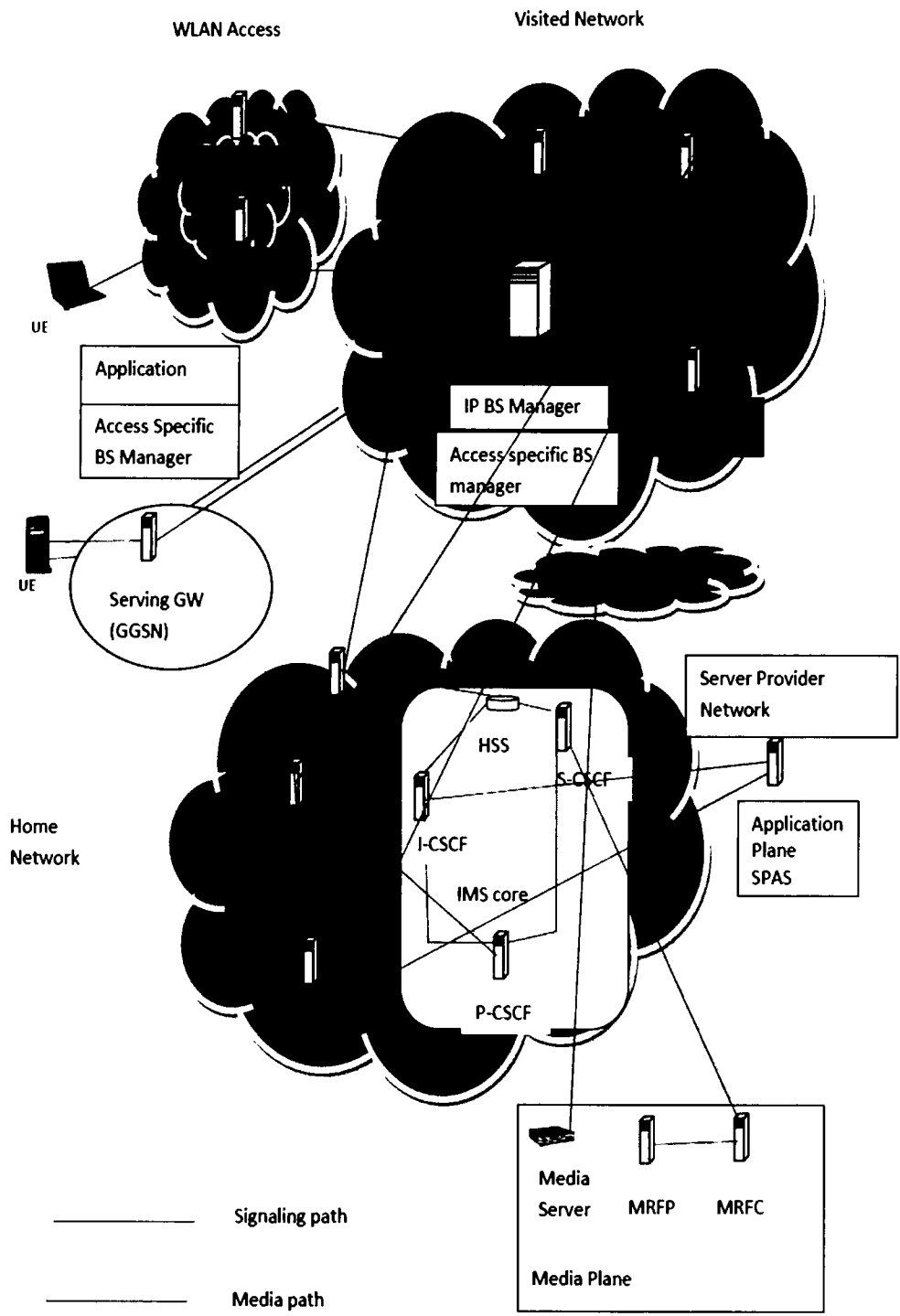


Figure 1.1 Policy and charging control architecture in IMS [5]

1.1.1 Quality of Service in 3G Access

The standards of Quality of Service(QoS) in IP Multimedia Subsystem reveal the service that has been deployed in such networks[1]. The PCC architecture applies PCC and Quality of Service rules for QoS provisioning.

The PCC rules were used to derived QoS rules [11]. There are two ways in which H-PCRF can provide PCC rules to PCEF i.e push mode and pull mode. In Push mode the PCC rules are shoved towards the available PCEF by the H-PCRF. While in pull mode the PCEF put a request for the desired rules whenever it gets a request regarding PDP context activation from the terminal user. The QoS provisioning in 3 GPP is given in Figure 1.2. The mode of QoS provisioning is considered a pull mode in this figure. The figure is explained as following:

(Step 1 to 5) The IMS client requests an initiation of session by sending SDP offer message to the Proxy CSCF. The Proxy CSCF gets SDP request and moves this information to H-PCRF, for this needful, it has to sends an AAR message to H-PCRF.

(Step 6-8) In sixth step the H-PCRF identifies the IP Connectivity Access Newtork (IP CAN) session information and stores the service information. H-PCRF uses session description to select a collection of distinct PCC rules for session establishment. In step seven the Home PCRF forwards an AAA message to Proxy CSCF. In step eight ultimate SDP answer message is forwarded to the IMS end user for further action.

(Step 9) Once SDP messages are retrieved the IP Multimedia client connects the SDP information in order to retrieve a particular QoS parameters.

(Steps 10–12)The IMS client sends the PDP context to the PCEF. The PCEF sends the CCR message for requesting the IP QoS parameter authorization from the V-PCRF. In next step, the visiting PCRF sends the CCR message to the home PCRF.

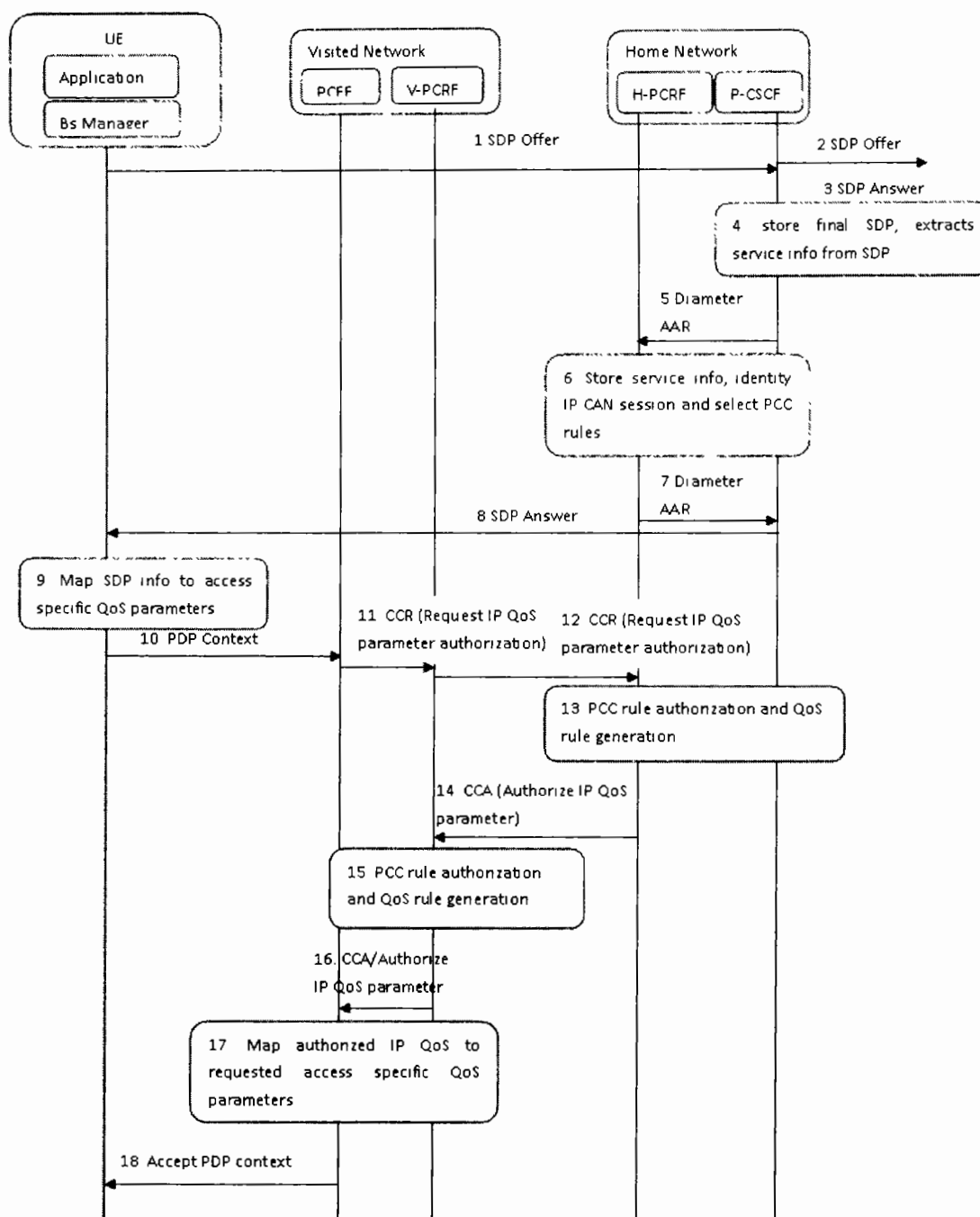


Figure 1.2 3G Access Message Sequence for QoS provisioning [5]

(Steps 13 to 16) PCC rules, which have been selected earlier, are installed in the PCEF. For this purpose the PCC rules are authorized and QoS rules are generated. The Home PCRF sends an answer for credit control which carries legitimate IP QoS associated parameters. The visiting

PCRF receives the QoS rules and validates them before forwarding the PCC rules to the PCEF via a CCA message.

(Steps 17 to 18) The mapping of legitimate IP QoS in order to get QoS parameter. After that it sends the PDP context to the related IMS client.

1.2 Problem Statement

The Next Generation Network provides network architecture for the provision of services which are independent of access technology. For scalable and a better utilization of resources and light weight user equipment, virtual machines need to be used to ensure the uninterrupted provision of Quality of Service enabled Services. The process delay, improvement in utilization of Session Call Service Control Functions needs to be addressed. These IP-based multimedia services rely on SIP for establishing, maintaining and terminating the communicative sessions, which underscores the efficiency and security of SIP protocol.

Various SIP based authentication schemes have been presented during the last decade. However these previous schemes have many limitations. Recently Dongqing et al. proposed an improved SIP authentication protocol. Nonetheless, we ascertain that Dongqing et al.'s authentication scheme is susceptible to privileged insider attack, Denial of Service (DoS) attack, and session specific temporary information attack. Besides, this protocol assumes a strictly time synchronized system, which limits the practical effectiveness of the protocol for a real environment.

1.3 Research Objectives

The statement of the problem formulates the basis for this research work. From extensive study of related work and the problem statement following objectives can be achieved from this research work.

1. To understand the QoS and requirements of the IP Multimedia Sub Systems using virtual machines. How the virtual machines are used in the IP Multimedia Subsystem and how SIP works in virtualized IMS environment to ensure Quality of Service?

2. To propose an architecture which ensures the QoS levels in IP Multimedia Subsystem using virtual machines. How the performance Call Session Control Functions can be increased with increasing number of users. Our research work also has the aim of evaluating the proposed system.
3. To find vulnerabilities in Dongqing et al.'s authentication scheme and to propose an improved SIP authentication protocol that covers the limitations of Dongqing scheme.

1.4 Research Contribution

- We have studied in details the QoS in IP Multimedia in detail using virtual machines.
- We have proposed an architecture. Results shows that it performs better and manages load management in a better way.
- The result shows that it ensures the uninterrupted provision of services to the user.
- Session setup delay has been decrease as shown in the graphs.
- The system scalability has been increased in the proposed architecture.
- Implementation of light weight user equipment
- Better utilization of resources.
- Privileged insider attack has been avoided in the proposed scheme.
- To prevent Denial of Service (DoS) attack.
- The issue of session specific temporary information attack has been removed
- To tackle the issue of strictly time synchronized system, which limits the practical effectiveness

The thesis is organised as follows:

Chapter 1 is about Introduction. Chapter 2 shows the brief overview of IP Multimedia This chapter elaborate IP Multimedia Subsystem Session, IP connectivity, need of QoS in IP Multimedia Services, IP policy control etc. Various entities and their roles in IMS, Call Session Control functions, databases are explored in detail.

In chapter number 3, cloud computing, Software as a Service, Platform as a Service and Infrastructure as a Service has been addressed. Various types of community cloud, public cloud, private cloud, and hybrid cloud are part of this chapter. the concept of virtualization and various virtualization tools are discussed. At the end of this chapter detailed literature review related to Quality of Service and virtualization has been given. The proposed model has been described in chapter number 4. Simulation result of OpenIMS are given. Performance different Call Session Control Functions are shown. Operating System Ubuntu 14.04 LTS (OpenIMS), DNS Server (BIND-9.3.2), Web Server (Apache2) MySQL Server, Wireshark Network Protocol Analyzer, SIPp Traffic Generator Tool software are used for generation of results. Chapter 5 consists of definitions and brief descriptions of various types of security attacks e.g password guessing attacks, replay attacks, Man-in-the-middle attacks, Stolen-verifier attacks and other various important attacks. Authentication schemes for example authentication methods based on Diffie Hellman, Authentication methods based on Elliptic curve cryptography, Authentication methods based on nonces and Authentication methods based on identity based encryption are explained in detail in this chapter. The chapter 6 is about proposed system. Dongqing et al. scheme has been discussed in detail. In this work, we elaborated that Dongqing et al.'s scheme is susceptible to privileged insider attack, Denial of Service (DoS) attack, and session specific temporary information attacks, other than a limitation of time synchronization. Thus, to counter the limitations in Dongqing et al., we propose an improved SIP authentication scheme.. The comparative analysis of proposed and contemporary schemes shows that proposed system perform better in in terms of security and efficiency.

1.5 Summary

In this chapter, basics of IP Multimedia Subsystem have been described. The PCC architecture enforces PCC and QoS rules in order to ensure the uninterrupted provision of QoS. The Quality of service in 3G Access has been described in detail. Finally the chapter concludes with the statement of the problem describing the use of virtual machine in IP Multimedia Subsystem and various limitations in the Dongqing et al.'s authentication scheme, research objectives, research contribution and the organization of the thesis.

2 . IP Multimedia Subsystem

This chapter describes the various important elements of 3GPP IP Multimedia Subsystem.

2.1 Architectural requirements of IP Multimedia Subsystem

The IMS architecture has been designed on some basic parameters and its design has capacity for development for improvement in future. The requirements of 3rd Generation Partnership Project (3GPP) IP Multimedia Subsystem are specified in [12].

2.1.1 IP Multimedia Subsystem Sessions

For audio, video and messaging services in the communication networks, circuit switched bearers are used. Offering end users service continues as end users shift to the packet switched domain and initiate to gain services of the IP Multimedia Subsystem. Number of entities have been added and vast communication resources has been included in the IMS infrastructure to take the communication to the next level. During a single session, IP Multimedia Subsystem users can use a variety of IP based services. User is able to integrate, add or drop various services like video, voice and text during the communication.

2.1.2 IP Connectivity

In IMS, a device has a unique IP address for connectivity. The applications which needs end to end connectivity can be easily achievable with IPv6 as IPv6 has sufficient address storage. Therefore 3rd Generation Partnership Project has exclusive support for IPv6. However early implementations and deployment of IP Multimedia Subsystem used IPv4. The details are documented in IMS [3GPP TR 23.981].

End users may connect to home network or visited network using IP connectivity. On the left side of the Figure 2.1 an IP address is shown which user equipment gets from the visited network. In case if a user is present(roaming) in visited Universal Mobile Telecommunications

System(UMTS) network, the Radio Access Network, Gateway GPRS and the Serving GPRS support node are situated in the home network. The IP address obtained by a terminal device is shown in the Figure 2.1. In case of UMTS network, if the user is moving, both Radio Access Network (RAN) and Serving GPRS Support Node (SGSN) exists in the visited network.

In this case the user is present in the home network all the entities required for communication entities required for communication are present in the home network. The connectivity of IP address is accessed in that network. It is vital to notice that a user can be in the roaming mode and can get IP connectivity from the home network. This is depicted in the figure 2.1. An IP Multimedia Subsystem network can be setup in a specific single area and can access e.g General Packet Radio Service (GPRS) roaming in order for the connection of the users to the home network. From practical point of view this is not the case as routing mechanism would not be high enough efficient.

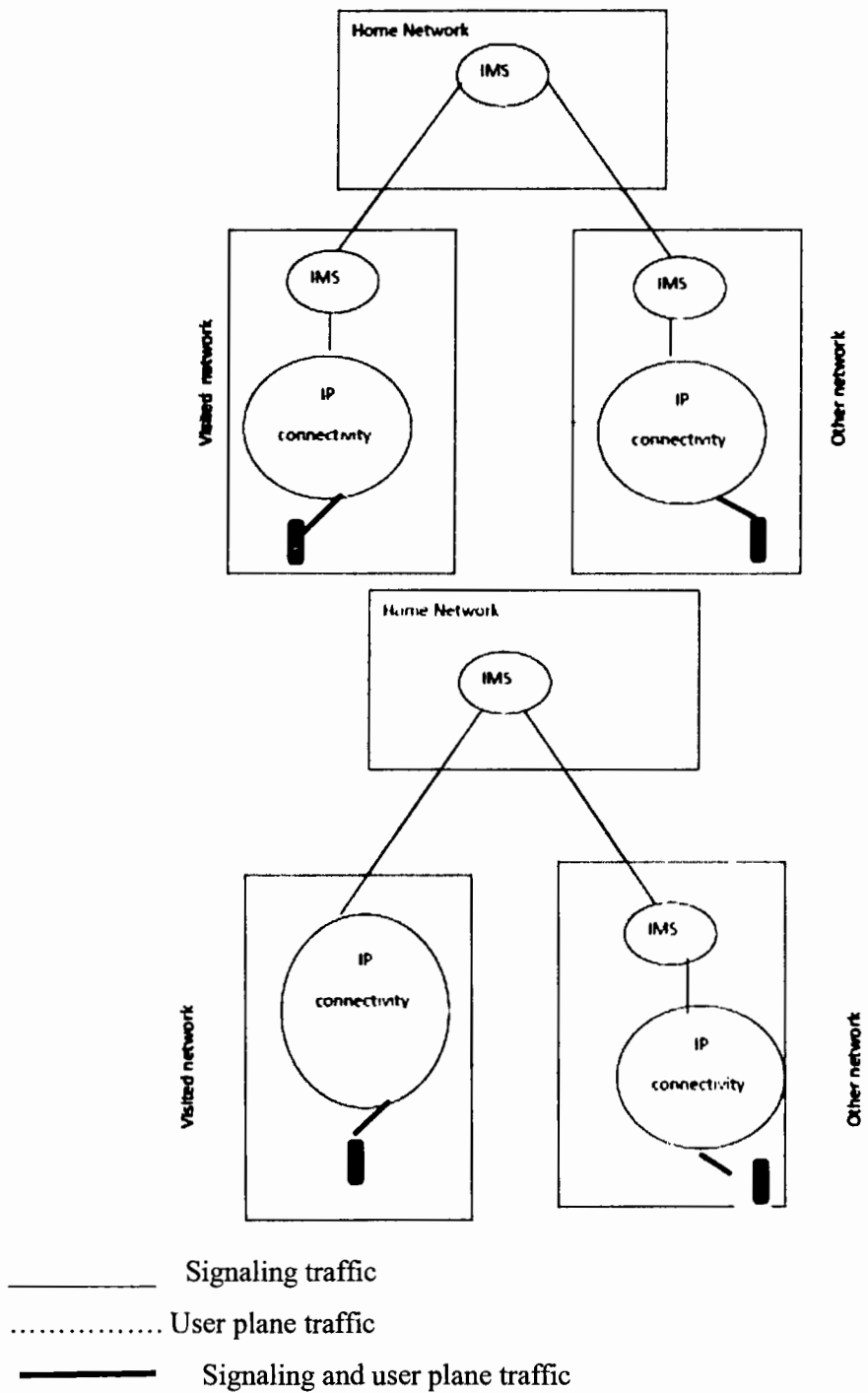


Figure 2.1 User roaming connectivity options[13]

2.1.3 Requirements of QoS in IP Multimedia Services

Quality of Services is important in public networks. Increase and variable of delay, out of order arrival of packet, loss or discard of packet are common problems in public internet. These problem will no longer in case of IP Multimedia Subsystem. The IP Multimedia Subsystem would not face such problem no longer. The underlying access and transport network are designed in a way to ensure Quality of Service from end to end.

During the SIP session the end user express its Quality of Service requirements like type of packet size, packet frequency, bit rate, usage of RP payload for media types as well as bandwidth adaptation. The network users reserve the correct resources from the access network after conferring the requirement at the application level. Once QoS parameters are created, with a suitable protocol e.g RTP the individual media types are encoded and packetized. These packets are sent to the access and transport network by use of protocols such as TCP or UDP on the particular Internet Protocol.

2.1.4 IP Policy Control

It is potential to authenticate and to have control of the bearer traffic use projected for IP multimedia subsystem media. It is based on the signaling parameters at the IMS session. Communication between the IP connectivity access network and the IP Multimedia Subsystem is needed for this reason. The policy control element verifies that values conferred in SIP signaling and is needed for activating bearers for media traffic. This helps an operator to ensure that its bearer resources are not being misappropriated. When SIP session between end points is initiated or halted, the policy control element is enabled to be implemented.

2.1.5 Communication Security

Security is a important needs in every sort of communication networks. Besides the access network procedures, the IP Multimedia Subsystem has specific mechanisms for authentication and authorization. In addition, the integrity and confidentiality which are important features for the Session Initiation Protocol messages is applied between the IMS network and the end user.

The security provided in IMS is of the same level as provided in the GPRS and circuit switched networks.

2.1.6 Support of Roaming

Roaming is one of the basic feature which enables the end user to have uninterrupted communication regardless of his location. It means that a user can avail network services even not present in the geographical area away from the home network. In case of GPRS roaming IMS is accessible when the visited network provide the RAN and SGSN and the home network offers the GGSN and IMS functionalities.

The primary advantage of the discussed model is the comparison of roaming model with the GPRS for optimum utilization of the resources. Inter domain roaming between the IP Multimedia Subsystem and the CS is referred to as IP Multimedia Subsystem and CS CN domain roaming.

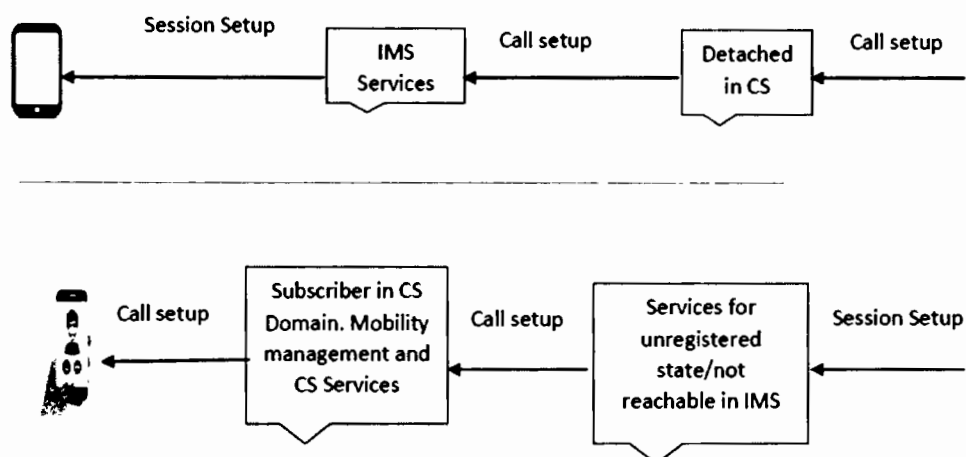


Figure 2.2 IMS/CS roaming cases[13]

In case a user is unregistered or unreachable in some particular domain then he session can be forwarded to the other domain. Besides the services which are common and present in both

domains, the CS CN domain and the IP Multimedia Subsystem domain have their own distinct services.

2.1.7 Interworking with other Networks

It is obvious that the IP Multimedia System is not installed around the globe, rather various types of the communication networks exist. The users have various types of terminals and have different subscriptions. To cope the challenge to ensure the QoS enabled communication between different terminals having different geographical location and having different network, needs to be ensured. Besides other network requirement the IP Multimedia Subsystem must be able to connect large number of terminals as possible. So interworking feature has been included in IMS to keep up communication with mobile, PSTN, internet users and ISDN users. The internet applications which exists out the 3GPP community are accessible from IMS.

2.1.8 Service Control Model

Visited service control is being used in the 2nd generation mobile network. The traffic is controlled and services are offered by the visited network in case the user is roaming. This entity is called visited control model in the second generation. Internet Engineering Task Force protocols will need additional extensions to support these protocols. Due to complexity the visited service solution was dropped and it could not offer visible added value as compared to home service control. On the other hand, the visited service control implies some restrictions. As the visited and home network has to offer same kind of services, the service development is slow. As the inter operator reference points increase in number, the need of complex solution also increases.

2.1.9 Service Development

The need for scalability in a service platform, as well as the ability to rapidly introduce new services, suggests that traditional approaches are no longer adequate. The IMS framework must support to offer QoS ensured support to multimedia, speech, messaging file sharing, video, gaming, transfer of data and necessary supplementary services within the IP Multimedia Subsystem.

2.2 IMS entities and their functionalities

In this section various entities of IP Multimedia Subsystem and their prime functions are described. Following are main entities of the IMS

- Call Session Control Functions
- Services i.e application server, Multimedia Resource Function Processor(MRFP), Multimedia Resource Function Controller (MRFC)
- Databases i.e Home Subscriber Server (HSS), Subscription Location Function (SLF)
- Support functions i.e Packet Data Protocol (PDF), (Topology Hiding Inter-network Gateway) THIG ,SEG

Interworking functions including Breakout Gateway Control Function (BGCF), Media Gateway Control Function (MGCF), Signaling Gateway (SGW), IMS Media Gateway (IMS-MGW)

- Charging.

2.2.1 Call Session Control Functions

Call Session Control Functions are divided into three categories. Proxy Call Session Control, Serving Call Session Control, and Interrogating Call Session Control P-CSCF, S-CSCF, and I-CSCF are the abbreviations for these Call Session Control Functions respectively. Particular functions are assigned to each CSCF. Every CSCF has its own specific functions. All CSCFs are involved during the registration process and session establishment process and complete the SIP routing mechanism.

2.2.1.1 Proxy- Call Session Control Function

Proxy Call Session Control Function abbreviated as P-CSCF is the point of interaction for UE and IMS network i.e the requests sent by the IP Multimedia Subsystem terminal device are forwarded to Proxy Call Session Control Function. All SIP terminating SIP signaling coming from the network is also forwarded from the P-CSCF to the terminal device. This node offers

several functions concerned with the security. There are four specific functions performed by the P-CSCF namely SIP compression, IPSec security association, emergency session detection and interaction with Policy Decision Function. SIP protocol is larger than binary encoded protocols, 3GPP has the facility of SIP compression between the user and P-CSCF in order to speed up to establish the session. The Proxy Call Session Control Function requires to compress messages if the terminal device needs messages in compressed form. One of the responsibility of P-CSCF is to keep Security Associations as well as implementing integrity and confidentiality security for SIP signaling. This is obtained during SIP registration as user equipment and P-CSCF negotiate IP Sec SAs. If an operator needs to apply SBLP the P-CSCF performs the relay session and the information related to media to PDF.

Depending on the obtained information, the PDF gets the authenticated IP QoS information. The IP QoS information is forwarded to the GGSN before accepting a secondary PDP context action while implementing the Service Based Local Policy. Further through PDF the IP Multimedia Subsystem is capable to carry IP Multimedia Subsystem charging correlation information to the GPRS network. In the same way the PDF the IP Multimedia Subsystem is capable to perform IMS charging correlation information to the General Packet Radio Services network. This results in merging in the billing system of the charging data records coming from the IP Multimedia Subsystem and General Packet Radio Services.

2.2.1.2 Interrogating-Call Session Control Function

The I-CSCF interacts with the Subscriber Location Function as well as Home Subscriber Server and performs the role of a SIP proxy server. There are four specific functions carried out by the I-CSCF are given below:

- To know the next S-CSCF/application server from the HSS
- Allocating an S-CSCF depending on information obtained from the HSS.
- Forwarding the requests further to a specific S-CSCF or the application server
- It provides the functionality of topology hiding Inter-network Gateway.

2.2.1.3 Serving Call Session Control Function

S-CSCF is the IP Multimedia Subsystem's central point, as it is responsible for handling the registration process, routing decisions, session states, and service profile storage. Any registration from a user is forwarded to the S-CSCF which access and obtains the data required for authentication from Home Subscriber Server. A challenge is generated depending on the authentication data to the terminal device. The S-CSCF accepts and supervise the registration process upon receiving and verifying the response.

Then a user can avail IP Multimedia System services. In the registration process the service profile which is a set of user information, is downloaded from the Home Subscriber Server. The service profile consists of instructions depending on the required media policy by the Serving-CSCF. Important routing decisions are made by the S-CSCF. The UE originates a request through P-CSCF to S-CSCF. S-CSCF decides whether application servers needs to be contacted before further sending the request.

After finding the suitable application server, the S-CSCF either maintains a session in IP Multimedia Subsystem or breaks to other domain. If the user equipment is looking for a called user using the Mobile Station ISDN number, the S-CSCF converts the MSISDN number to SIP Universal Resource Identifier format before forwarding the message. The IP Multimedia Subsystem does not route request based on MSISDN number. The requests which are terminated at the user equipment are also received by the S-CSCF. Although the S-CSCF has the information of the IP address of the user equipment from the registration it forwards all requests through the Proxy-CSCF, as the Proxy-CSCF takes the responsibility of the SIP compression and security related functions.

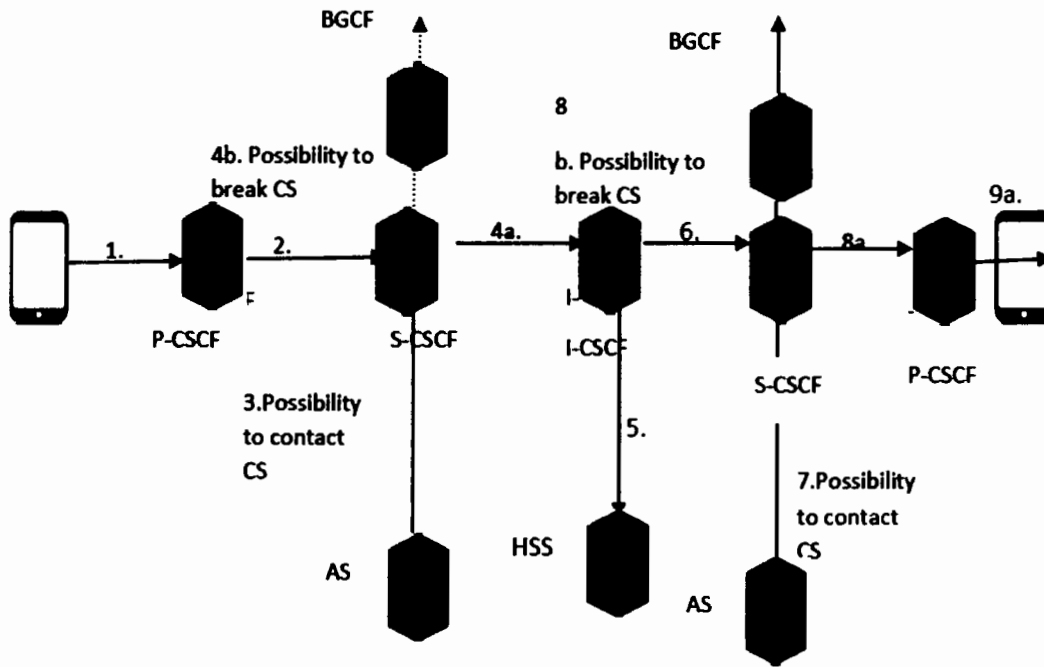


Figure 2.3 Role of S-CSCF in routing[13]

2.3 Databases

Basically two types of databases exist in the IP Multimedia Subsystem. One is Home Subscriber Server abbreviated as HSS and the other is Subscription Location Function abbreviated as SLF. Information related to the subscriber of IP Multimedia Subsystem resides in the Home Subscriber Server. The Home Subscriber Server also hold service related data. The HSS contains user identities, access parameters, service triggering information and registration information. The user identities can be classified into two types. The home network operator allocates the user private identity. It is used during registration and authorization of users.

With the help of public user identity users can communicate with each other. IP Multimedia System access parameters are used to establish sessions. These parameters may be like roaming

authorization, user authentication and allocated Serving-CSCF names. Service triggering information makes the SIP service to execute.

The Home Subscriber Service determines and offers the user specific parameters for the processing of S-CSCF. This information helps the I-CSCF in the selection of appropriate S-CSCF for a user. In case of Packet Switched Domain and the Circuit Switched domain, the Home Subscriber Service contains the Local Register and the Authentication Centre.

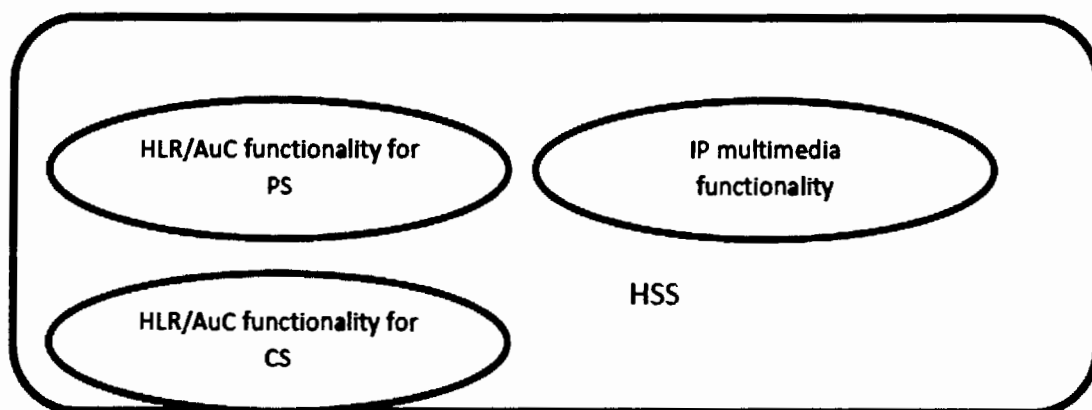


Figure 2.4 HSS[13]

Home Location Register provides support to the PS domain entities. In the same way Home Location Register provides this facility to CS domain entities. By using this facility a subscriber can access services of the CS domain as well as provide the facility of roaming to the Global System for Mobile Communication or UMTS CS domain networks. There is a unique secret key in AUC for each user. This key is utilized in the generation of dynamic security data which is used by each mobile subscriber. When mutual authentication of the International Mobile Subscriber Identity and the network is performed, this data is used for this purpose. As the number of the mobile subscriber increases the HSS may be more than one in the home network.

2.4 Service Functions

The service related functions can be categorized into the following types

- Multimedia Resource Function Controller abbreviated as MRFC

- Multimedia Resource Function Processor abbreviated as MRFP
- Application Server abbreviated as AS

Application servers are the functions at the top of the IP Multimedia Subsystem and are not real IMS entities. However we consider the Application Servers as a part of IP Multimedia System functions because these entities offer value added multimedia services in the IP Multimedia Subsystem e.g presence and push to talk over cellular. An Application Server exists in the home network or may be in some other network known as third party. The third party may be a standalone Application Server or network. The important responsibilities of the AS are: It processes the incoming SIP request messages coming from the IP Multimedia Subsystem. AS has the capability to initiate SIP requests. It sends the accounting information to the charging functions after accepting the SIP request. The Application Server does not only offer the SIP based services because the operators may also offer services like CAMEL, CSE and OSA for its IMS subscriber.

2.5 Registration

Before the registration it is necessary that the UE must get an IP connectivity bearer and also find out the P-CSCF which is the entry point of IP Multimedia Subsystem. The User Equipment gets an IP connectivity bearer and looks for an IP Multimedia Subsystem entry point which is the P-CSCF before initiating the registration process. IP Multimedia Subsystem registration consists of two stages. The leftmost part of Fig 2.5 projects the first phase i.e how UE is challenged by the network. The rightmost portion in Fig 2.5 indicates the second phase- it shows the way user equipment reply the challenge and finishes the registration. First ,the User Equipment send a request SIP REGISTER to the find out the Proxy-CSCF. This request consists of the registration of identity and home domain name which is the address of the I-CSCF. After obtaining the REGISTER request, the P-CSCF processes and resolve the IP address of I-CSCF via home domain name. The I-CSCF contacts the HSS to determine the capabilities are needed to select S-CSCF. The I-CSCF passes the REGISTER request to the Serving-CSCF until the S-CSCF has made its decision. When the Serving-CSCF find an unauthorized user it retrieves the authentication data from the Home Subscriber Server. After obtaining the authenticated data the S-CSCF sends a 401 unauthorized response. The user equipment evaluates a response in order

to challenge and then forward another Register request to the Proxy-CSCF. Again the Proxy-CSCF interacts with the Interrogating-CSCF and the Interrogating-CSCF further finds the Serving-CSCF.

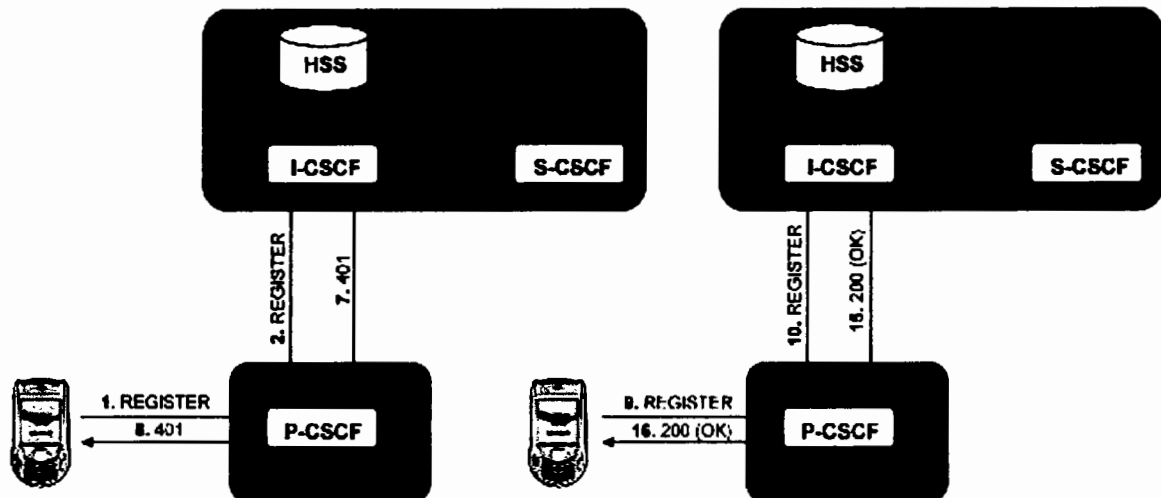


Figure 2.5 IMS registration[13]

The S-CSCF downloads the user profile from the HSS once the user response is authenticated. Then the S-CSCF acknowledges the registration request and responds with a 200 OK message. Upon the successful authorization of the user equipment it is enabled to establish sessions. The user equipment and the P-CSCF find out the S-CSCF in the network during the registration process to provide the necessary service.

The UE periodically refreshes its registration in order to keep the registration active. Upon the lapse of the registration time, then the S-CSCF removes the registration if the UE fails to refresh its registration. When the user equipment needs to de-register from the IP Multimedia Subsystem it sets a registration timer to 0 and further forwards a REGISTER request.

Session Initiation Protocol has the capability to register one public user identity at a particular time. There are chances that a user may have more than one public user identity then the user has to manage registration of each public user identity on individual basis. At the user end, this process can be annoying and time consuming. For this reason, a solution has been introduced by

the 3GPP to handle the registration of many public user identities simultaneously. This mechanism is known as implicit registration.

A single registration request is used to register a set of public user identity in this concept. In the implicit registration if any of the public user identities in a set is registered then every public user identities in the set are registered simultaneously. In the same way if any of the public user identities gets de-registered, the rest of the public user identities in the set also de-registered at the same time. In this process public user identities may access distinct service profile but some public user identities may access the same service profile[12].For implicit registration the public user identities has to send the SUBSCRIBE to the Serving-CSCF which reply with NOTIFY request.

2.6 Identification of Users

Following are the types of the identification of users.

2.6.1 Private User Identity

To identify a user within the home network, private user identity is used. This identity is global identity and is defined by the home network.

2.6.2 Public User Identity

User identities in IP Multimedia Subsystems networks are known as public user identities. These are normally named as IP Multimedia Public Identity in IP Multimedia Subsystem. A public identity is used for communicating with the other users and IMS users are able to establish a session with different networks e.g Global System for Mobile communication (GSM). The IP Multimedia Subsystem architecture force the following needs for public user identity [14, 15]:

SIP Uniform Resource Identifier or a telephone Uniform Resource Locator format are the format are followed by the public user identity . It is vital than an ISIM application must have not less than one user identity. It is also impossible for the user equipment to make changes in the public user identity. A pubic user identity needs to be registered in order to initiate IMS

sessions and IP Multimedia Subsystem session which not related e.g NOTIFY, SUBSCRIBE, MESSAGE etc. It is necessary that a public user identity should register prior to terminating the IMS sessions.

2.6.3 Derived Public User Identity and Private User Identity

As it is stated in earlier sections, a private user identity and public user identity are present in an ISIM application. It is not necessary that all equipment in the market support ISIM application therefore IMS has incorporated accessibility method without the use of ISIM. Private and public user identity as well as home domain name are extracted from the International Mobile Subscriber Identifier in this model.

This procedure is fit for user equipment that has a Universal Subscriber Identity Module application. Below are the steps involved in the derivation of the private user identity from the Universal Subscriber Identity Module. In the first step user part consisting of digits is swapped with the string from International Mobile Subscriber Identity(IMSI). Every private user identity domain part which have Mobile Country Code and Mobile Network Code values International Mobile Subscriber Identity and domain name which is pre-defined. All these parts are combined separated by dots in the order given below Mobile Network Code(MNC), Mobile Country Code (MCC),Pre-defined domain name.

2.7 Identification of Services (Public Service Identities)

It is vital to understand that some identities are necessary to identify services and groups which the application servers host specially when variety of services like presence, messages and group services capabilities. These identities are created as per requirement by the user in the application server and are not registered before usage. Public service identity was introduced as the ordinary public user identities were simple[13]. Public service identities are in the format of SIP URI or may be in tel URL format.

2.8 Identification of Network Entities

The network nodes which are part of the SIP routing mechanism should be identifiable by using a suitable SIP URI in addition to the identification of the users. The header fields of SIP messages use these URIs in order to identify these nodes.

2.9 IP Multimedia Services Identity Module

On the Universal Integrated Circuit Card, there is an application called IP Multimedia Services Identity Module. It is a safe and removable device that in UE in to identify and authenticate the user to the IMS. The ISIM has the capability of co existence with the SIM and the USIM on the same UICC. It allows users to use the same smartcard in both GSM and earlier UMTS releases.. More than one application may exists in the UICC. IP Multimedia Services Identity Module contains IMS specific subscriber data. During the registration of IMS[13] most of the data is required. Security keys includes the integrity keys, ciphering keys and key set identifiers. Integrity keys perform the duty of the verification of integrity and protection of Session Initiation Protocol Signaling. To ensure the confidential protection of Session Initiation Protocol signaling, cipher keys are used. Release 5 had lacking of confidential protection however it is included in Release 6[13].

2.10 Universal Subscriber Identity Module

The Universal Subscriber Identity Module stores the subscriber related information and specific identifies a particular subscriber. It is vital for accessing the PS domain. Like ISIM, the USIM application is located on the UICC. The USIM consists of the security parameters for communicating with the PS domain, access point names which are allowed and Multimedia Message Services [16, 17, 18].

2.11 Discovery of the IMS entry point

It is the process in which the UE communicates with the IP Multimedia Subsystem and finds in any case one IP address of the P-CSCF. In 3GPP two dynamics procedures are used for the P-CSCF discovery. One is Dynamic Host Configuration Protocol- Domain Name System DHCP-

DNS method and the other is GPRS method. In the GPRS mechanism the end user add the P-CSCF address request flag in the PDP context activation request and obtains the IP address of the P-CSCF in turn. The procedure for the Gateway GPRS Support Node for obtaining the IP address is not standardized.

2.11.1 S-CSCF assignment

After discovering of the P-CSCF the next step is the assignment of the specific S-CSCF. When a user wants to register with the network, or when an unregistered user receives a Session Initiation Protocol request, the S-S-CSCF is assigned. The S-CSCF does not respond if S-CSCF is already assigned.

2.12. Quality Mechanism

One of the important standards to asses a system is the measurement of network performance which involves the deployment, operation and customer satisfaction. Quality of Experience abbreviated as QoE and QoS[19] are the two approaches the quality of the network is assessed. QoE, less frequently QoX or QX is the measurement of pleasure or displeasure of the user's experiences with a service e.g web browsing, phone call, TV broadcast. QoE deals with the whole service experience, it is a way to assess the human feelings, cognition and satisfaction. The similar concept is also being used in social sciences and engineering science. It concentrates on perceptive overall human quality necessities. It focuses on the user expectations and their effect on the QoS[20].

These constraints are converged on human experience and are of wide area of research. QoS defines a set of metrics that depending on the functioning of the network is then assessed using appropriate metrics and evaluated depending on the factors that define QoE[19][21]. As per the definition of the ITU Recommendation E.800[22], Quality of Service is described totality of characteristics of a telecommunications service that let on its ability to meet the service demand of the users. Quality of service plays a vital role by using different indicators to assess the

performance of the network e.g delay variation, bandwidth, end to end delay, bit error rate and data rate etc[23]

Within the perspective of an IP network, a service means how traffic is handled overall with in a specific domain. If a service fulfill the requirements of the client it means the service maintains a level of the QoS[24]. Four Quality of Service categories are defined by the 3GPP and Telecoms & Internet Converged Services & Protocols for Advance Networks (TISPAN). These QoS categories include streaming class, conversational class ,interactive class and background class. Conversational class reacts quickly to delay variation and has tolerance level which is low for packet loss. The most time-sensitive traffic is the conversational class and is used in the VoIP and audio/video conversation. Streaming class is responsive to but shows tolerance to delay variation, and have limited tolerance to packet loss.

Delay and jitter constraints are less strict as compared with conversational traffic class and is used in video streaming e.g video on demand. Interactive class is used to prioritize the packet data protocol (PDP) contexts. The interactive class is related with the traffic handling priority(THP). Its value ranges between 1 and 3. It transfers transparently with the low error bit rate. It is used in web browsing, telnet and video on demand. Background class is least sensitive to delay having tolerance with low bit error rate. It is used in email, Instant messaging and chatting connected with network functioning and service responsiveness. A user can communicates with an operator or two operators can mutually communicate with each others. One party performs the role of customer to purchase services and other acts as a service provider[25].

2.12.1 Quality of Service Protocols

To ensure and appropriate Quality of Service of the network, the Internet Engineering Task Force (IETF) has introduced Integrated Services model for resources based on reserve model and traffic prioritization based on Differential Services[26][27]. In DiffServ traffic is distributed in various classes when congestion occurs the prioritization of these aggregates with a code in the datagram to control the situation [9].

Every node in the communication network should recognize the code to prioritize packets[28]. Nodes in the network utilizing the Resource Reservation Protocol a channel and admission control of packet is reserved by the IntServ. The implementation is done through following three types of services.

Guaranteed service

- The guaranteed service is used in hard real-time applications.
- Provision of service requirement and traffic characteristics as per user specifications.
- At all routers admission control policy is implemented.
- Calculates guaranteed bandwidth, jitter and bandwidth

Controlled load

- Used in the applications that have capability to adapt to the network conditions.
- Provision of service requirement and traffic characteristics as per user specifications as in case of Guaranteed service.
- Admission control policy is implemented at routers level.
- As compared with the guarantee service the guarantee is not strong.

Best effort

- Before starting the session the Quality of Service requirement and characteristics of the traffic must be declared.
- There are problems related to the scalability and complexity which can be tackled by the implementation of the DiffServ. The operation between different operators are based on SLAs which is the main element of DiffServ[29].

2.12.2 Policy-based QoS Architectures

Various architecture models for the control of data flows have been presented by the organizations like ETSI TISPAN in order to ensure the QoS in Next Generation Network.. The IETF documented the policy framework in RFC 2753[30] which specifies standard policy rules. These rules are expressed as a model for the configurations of the network or devices. Special repositories are used to store these rules known as Policy Decision Points and Policy Decision Functions abbreviated as PDPs and PDFs respectively. As per the Quality of Service requirements these repositories pick up the rules of suitable policies as per the received requests for policy[40]. The Policy Enforcement Point is a type of server for the implementation policy for admission control and making decision when a user wants to use network resources. For this a user has to forward a transaction request to the Policy Enforcement Point(PEP). The ETSI TISPAN architecture is known as the Resource and Admission Control Subsystem for Quality of Service. This subsystem manages the control element policy, admission control and resource reservation in the next generation Network. It is the important component that prioritizes the packets by the use of DiffServ protocol and Resource Reservation Protocol (RSVP protocol) is used for the resource reservation. It communicates with the access and the core network as well. The PCC framework has flexibility and appropriate to different services, load models as well as access network.

2.12.3 Quality of Service Management

In order to enforce different policies for management of the QoS framework, it is vital to understand the various parameters involved in the provision of selected service. These services are well explained in [32][33].

2.12.3.1 Traffic Policing

Traffic policy determines which packets are removed by the limits or operating policies, dropping packages with lowest priority when forwarding. This method is implemented in routers and on input and output interfaces it is applied on IP packets depending on the variables given in RFC 2698.

2.12.3.2 Peak Information Rate

Peak information rate (PIR) is the maximum transmission rate a user can receive in bits depending upon the service level agreement or any sort of contract between the user and the service operator. The PIR is always smaller or equals to the maximum capacity provided by the operator.

2.12.3.3 Committed Information Rate

It is the average rate of long term traffic that the service operator assumes to offer a user with service level agreement or contract. This parameter is less than Peak Information Rate and is measured in bits. The CIR is always lower than the PIR

2.12.3.4 Committed Burst Size

The number of reserve bytes for bursts of service that can be communicated to the PIR and still complying the SLA provided at the CIR.

2.12.3.5 PBS

It is like CBS but specified with respect of PIR rather than CIR parameter.

2.12.3.6 Traffic Shaping

Traffic shaping employs a policy depending on queueing and than extraction of packets to retain the rate of the traffic. To ensure the contracted bandwidth, it is generally used by the service providers and the customers.

2.13 QoS Attributes related to Policy Decision Point

Quality of Service attributes are defined in Release 99 of 3rd Generation Partnership Project. These attributes include Traffic class, SDU format information, Traffic-handling priority, Maximum bit rate for uplink, Residual bit error ratio, Maximum bit rate for downlink, Transfer

delay, Guaranteed bit rate for uplink, Delivery order, SDU error ratio, Allocation/retention priority, Guaranteed bit rate for downlink , Maximum SDU size.

2.13.1 QoS parameters related to policy control

The PCRF manages the QoS policy Control[54] in order to guarantee the traffic over Long Term Evaluation and Long Term Evaluation Advanced networks.

2.13.2 QoS Class Identifier (QCI)

It is a procedure used in 3GPP in order to guarantee a bearer traffic is allocated a suitable Quality of Service (QoS). The parameters may include scheduling weights, queue management thresholds, admission thresholds, link layer protocol configuration and so on

2.13.3 Allocation and Retention Priority

It finds out the priority settings for the allocation and retention of an EPS bearer service which enables the network in making the decision for accepting these processes having a maximum bit rate abbreviated as MBR specifies within a specific period of time the maximum number of bits transmitted or received by the network.

2.13.4 Guaranteed Bit Rate /Non-Guaranteed Bit Rate

This parameter shows the bit rate resources reservation status means whether bits are reserved or not. With in a specific period of time, the number of bits transmitted or received by the network.

2.15 Summary

In this chapter architectural requirements of IMS have been explained in detail. This includes IP Multimedia Subsystem Session, IP connectivity, need of QoS in IP Multimedia Services, IP policy control etc. Next section describes the IP Multimedia Subsystem entities and their functionalities. The IMS entities comprised of Call Session Control Functions, application

Servers, databases, support functions, and interworking functions. Functions of various types of Call Session Control Functions e.g Proxy-Call Session Control Function, Interrogating –Call Session Control Function and Serving –Call Session Control Function has been discussed. Others type of IP Multimedia Subsystem entities have also been elaborated in detail. It is very vital that the performance of the system may be accessed i.e the overall deployment, operation and also analyse the satisfaction level of the end user. For this, various parameters involved related to the Quality of Service has been described in this chapter. The chapter elaborates the provision of Quality mechanism including different definitions and descriptions given by various standard bodies has been explained. Further QoS protocols has been described. The policy based QoS architecture, QoS management has also been described .

3. Cloud Computing

This chapter deals with the basics of cloud computing, its characteristics, service models, Virtualization, Virtual client and literature review in detail.

3.1 Introduction

As the services demand of users changes the computing is also being adapted according to the service model that meets the needs of the user. A user is concerned with the availability of the service as per their demands without having concern of the way or location where the services are provided. A number of computing paradigms are presented to reorganize the computing vision such as cluster computing, grid computing and now cloud computing.

Cloud computing is the result of various computing paradigms which include grid computing internet delivery, storage elasticity, pay per use on demand, content out sourcing and distributed computing[34,35,36]. The infrastructure which is known as “cloud” provides on demand services provision all over the world cloud computing has many definitions. Definition available in the U.S. National Institute of Standards and Technology “ It is a computing model for enabling the convenient, ubiquitous and on demand access to a pool of configurable computing resources that can be quickly allocated and de allocated with minimum administrative effort and interaction with the service providers”

Cloud computing has enabled a large number of organizations to create a variety of opportunities in the market [37]. To meet the requirements of the customer, a cloud provider has to consider specific key performance indicators known as KPIs.

3.2 Characteristics of Cloud Computing

On-demand self-service:

The consumer is able to perform all the actions automatically without requesting resources from the cloud service providers. For this purpose the cloud providers ensure infrastructure to meet the consumer demands automatically. There is a need of high level planning to meet the current demand, usage of resources and to see the future needs.

Resource pooling:

In resource pooling the physical and virtual resources of the service providers are pooled to offer services to multiple users. The assignment and reassignment of resources are dynamically managed to meet the user demand. Figure 4.1 highlights the concept of resource pooling.

Rapid elasticity:

Depending upon the services demanded by the consumer, the cloud computing resources automatically scale up and scale down. These results in the provision of QoS ensured services without degradation at any time.

Measured service:

Cloud systems are quite capable to automatically control and optimize the user required services such as storage, processing, number of active user account and bandwidth. The utilization of provided services is properly managed i.e monitored, controlled and reported.

3.3 Service Models

Cloud computing has following three service models.

3.3.1 Software as a Service

SaaS provides the accessibility of an application from any device using web browser or an application. The consumers are independent of resources and cannot directly manage the cloud infrastructure; the management of such type of service is the responsibility of the cloud infrastructure host. SaaS is also named as Application as AaaS. Some of the examples of such types of service providers are Google Office Productivity application, NetSuite, and Salesforce Customer Relationships Management system [38,36,39].

3.3.2 Platform as a Service

PaaS model that provides a development model which is deployed in a cloud infrastructure. In PaaS applications are developed and available at the cloud platform as a service for the consumer. The programming languages, libraries, services and tools are existed in the PaaS for their application development. The underlying cloud provider's infrastructure is inaccessible to the consumer. Facebook, App Exchange, Salesforce, Google App Engine, Windows Azure, Bunzee connect, IBM Websphere Cloudburst, Amazon EC2 and Force.com provide PaaS services [38, 35, 39, 40].

3.3.3 Infrastructure as a Service

In IaaS, the cloud provider guarantees that the user has access to processing, networks, storage, and other basic computing services. The user has option to select operating system, applications, storage. The user also has limited access to the networking components. Hardware as a Service is another name for IaaS. [30,33,2]. The user has no privileges to control and manage the cloud provider's infrastructure. Mosso Rackspace, Amazon Web Services, GoGrid, MSP On-Demand are few examples of the IaaS. Computing as a Service, Storage as a Service, and Database as a Service are the three categories of IaaS.

3.4 Types of cloud

Following are the types of clouds

3.4.1 Private cloud

Private cloud refers to a model in which the available resources of the cloud for organization for dedicated use. A private cloud is controlled by an organization by using internal resources. Combination of organization and third party offerings is also possible in private cloud. Firewalls ensure the protection of the cloud from illegitimate access.

3.4.2 Community cloud

Organizations having some mission e.g security, policy etc of specific community may collaborate to manage the community cloud. One or more organization or third party having common objectives, needs may manage, control and own this type of cloud.

3.4.3 Public cloud

General Public can access the cloud computing resources through standard Application Programming Interfaces (APIs) using the Internet. The public cloud can be owned by the autonomous organizations, private organization or government organization or may be owned by these organization in partnership and these organizations manage the cloud [38,40,41].

3.4.4 Hybrid cloud

In hybrid cloud two or more deployment models are combined to work as a new cloud infrastructure. The hybrid cloud also has to follow the standard technologies in order to make sure the portability of the data and applications e.g cloud bursting for load balancing within the cloud [38,40].

3.5 Scalability

The major objective of the cloud computing is to provide maximum level of scalability. For this purpose two different approaches are used in the cloud architecture i.e vertical scaling and horizontal scaling.

3.5.1 Vertical Scaling

Computing resources having more power are used in order to meet the demand of the customer in this approach. Although this scale up technique performs very well but requires significant amount of capital expenditure which may sometimes results in exceeding of the capacity before the deployment of the resources.

3.5.2 Horizontal Scaling

Horizontal scaling provides reliable and fully automated service. In order to satisfy customer demand, cloud services are scaled up in small groups. This form of service is preferred by large-scale businesses. The demand of the user is monitored on regular basis and then using scale out method the infrastructure is scaled to meet the user demand.

3.6 Cloud Elasticity

Elasticity is one of the vital features of the cloud computing which is the measure of degree of system adaptability to the load situation by automatic management of provision and de-provision of resources. By using this characteristic finest utilization of the computing resources can be utilized and making possible to meet the actual demand of the user by dynamic scale up and scale down of available resources. When elasticity is enabled in an application service, following two situations may occur.

Over-provisioning:

In this scenario, guaranteed QoS are provided to the end users even during the peak hours. If the service once determine the maximum actual demand then the capacity is wasted during the non peak hours [42].

Under-provisioning:

In case of under provisioning, the service operator does not care of failing in provivison of the services to the end users as per their requirements and even does not take care about the revenue reduction. In this type of service provision, the service providers offer poor quality of service when the demand exceeds the actual capacity during the peak hours. Further if the service providers are enable to meet the user demand at peak time, the some of users leave the site permanently[42].

3.7 Virtualization

The virtualization concept is used in the cloud computing in which one or more virtual machines can be run on a computer. Through virtualization hardware i.e memory, processors and storage resources can be utilized in optimal manner. This technique has also resulted in the evolution of the energy efficient computing also.

A virtual machine monitor abbreviate as VMM is also named as hypervisor is a type of software which provides the abstraction of the virtual machine and giving the user the ability to create and run virtual machines on the physical device. The hypervisor runs virtual machines on physical machine known as host. The Virtual Machine Manager abbreviated as VMM, Vritual Box VMware etc are examples of virtualization tools.

3.7.1 Virtual Machine Manager (VMM)

The VMM provides a Graphical User Interface(GUI) where virtual machines can be created as well as managed. Through VMM the performance of an resource utilization of all running machines can be viewed[39]. Similarly VMM ensures the availability of the system if any of the guest operating system domain fails to provide the services.VMM manage to load multiple operating system at the same time. The shared resources between the operating systems are managed by the VMM also helps in keeping of incoming interrupt request.

A VMM is preferred due to the the reason that different operating systems may run on a hardware platform without any alteration. It is not necessary that all processors support virtualization because of unprivileged instructions. The VMM manages these instructions the technique of dynamic recompilation to find unprivileged instructions on runtime and traps them into VMM. This technique is known as full virtualization. There is no need to change the source code o the operating system in full virtualization. When the VMM routine modifies the source code of the guest operating system then it is known as para virtualization. Some important relevant tools are described below.

Virt-Install:

This tool is used for the installation of the operating systems into virtual machines. GUI based interface is available for the creation of virtual machine.

Virt-Clone:

This tool is used to clone an existing virtual machine which is inactive. It creates a new configuration by copying the images on the disk. Use of GUI may be an option while cloning of virtual machine.

Virt-Image:

This tool is helpful in the installation of an operating system by using the pre defined image.

Virt-Viewer:

Virt Viewer is a GUI based display of the virtualized guest operating system.

3.8 Virtualization in IP Multimedia Subsystem and related Literature Review

In this section virtualization of IP Multimedia Subsystem and an endeavor has been done to describe various research work carried out in virtualization and Quality of Service in IP Multimedia Subsystem.

3.8.1 Virtualization of IP Multimedia Subsystem Client

The concept of Virtual IMS client was introduced and a virtual IMS client was developed in [43]. Figure 3.1 shows various components of virtual IMS client. In this architecture it was decided to shift almost signaling load to a specially designed server. This server is collocated with a P-CSCF and is named as Surrogate [5].

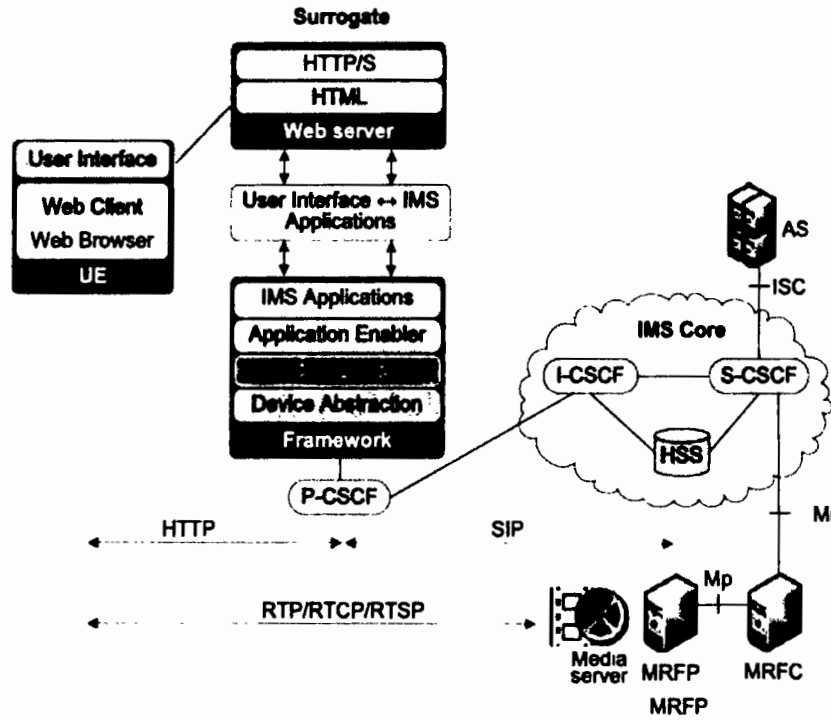


Figure 3.1. IMS client Virtualization [5]

This server performs the role of virtual server so that users can access, organize and monitor their services which are based on SIP. There is a Web server located in the surrogate. The user communicates with web server using an interface which graphical and runs on the Web client. Any type of device which is capable of IP connectivity can be termed as UE. In order to transfer the graphical user interface input to the IMS client application and IMS session status to the web server, a layer is required between the Server hosting the web and the IP Multimedia Subsystem UE. As the user interface layer lies in the IP Multimedia Subsystem application layer already, it is implemented in the UE via graphical user interface which is baed on web. There is a need must to implement to explore variety of IMS applications to the web server [15]. The UE uses HTTP for communicating with the surrogate and communication of the surrogate with the IMS core SIP is used. UE must be authenticated by the IMS core network in order to access IP Multimedia Subsystem services.

Application is also a challenge it is met by using UICC smartcard in the IMS application SIM. Universal Subscriber Identity Module (UICC) is a type of smartcard that keeps the identification of the subscriber and other information safely. It cannot be deployed within the surrogate. For instantiating of virtual ISIM application IMS soft client is required.

3.8.2 Integration of IMS-PCC Architecture with Virtualization IMS Client Model

In this section, integration of virtualization of IMS client with IP Multimedia Subsystem Policy and Charging Control (PCC) architecture model is explained. The IMS client virtualization model was integrated with the IMS PCC architecture in[5]. By the virtualization of the IMS client, the intricacy of the interaction with the IMS network is kept far from the access network. Third users can be used to implement the surrogate or the visited network may provide this facility. But in this model it is assumed to be implemented in the home network. This solution is useful for signaling path as IMS client often communicates with home network instead of visiting network. When surrogate is present in the home network, the propagation time of control messages will be reduced.

3.8.3 Roaming

The virtual client has the ability to completely virtualize the client using IMS Session Initiation Protocol. By examining the IMS (SIP) signaling plane it can simply stated that roaming has vanished. The IMS service session is accessed just like the terminal user is present in the home network in case of 3 / 4 G networks or WLAN/ broadband. However if media access plan is considered both roaming and non roaming scenarios may occur depending on the physical location of the end user.

3.8.4 Virtual IMS Client Architecture

This section delves into the PCC Architecture, which is the architecture used by virtual IMS clients. IP Multimedia Subsystem service deals the control plane and the media plane separately. The reason is due to the lack of the capability of the media plane for virtualization as media has to provide to the terminal devices. The two main elements present within the UE are simply

applications in the control plane and Access Unique BS Manager in the media plane. The applications constituted of the UCIC, IMS SIP and IMS SDP client. It may include other types of IMS application enablers.

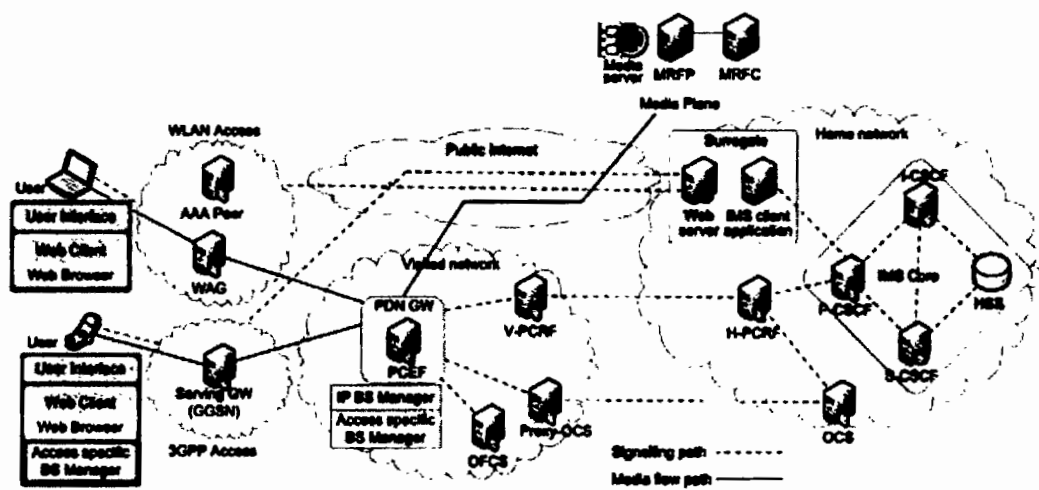


Figure 3.2. Virtual IMS client PCC Architecture [5]

The Access Specific BS manager once successful in mapping the PDP context parameters mapped from Quality of Service specifications in the application layer. A serving gateway reserve the resources according to the needs of the PDP Context. The serving gateway must be enrich of resource reservation which will results to gain the acceptable class of Quality of Service. Hence the Access specific BS Manager is vital element of which terminal device and therefore it is not recommended to pass it through virtualization process [5].

3.8.4.1 Details of QoS and Virtual IMS Client

In this section QoS provisioning for 3GPP Access Network and WLAN access using virtual IMS client is described.

3.8.4.2 Quality of Service in 3G Access

The sequence of messages is as follows:

Step 1: The end user initiates a service request and sends this request to the IMS client using web based interface.

Step 2-: IMS client sends SDP offer to P-CSCF. The Proxy CSCF extracts and keep save SDP information and directs the information to Home PCRF, for this it needs to send AA Request.

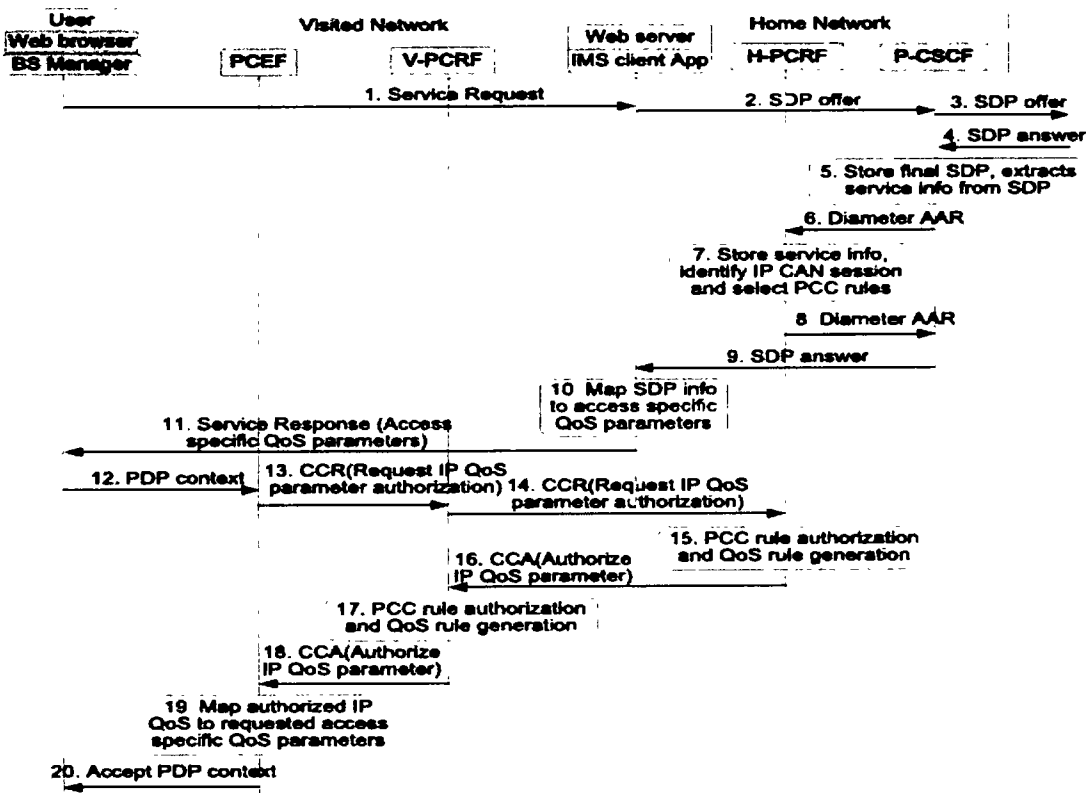


Figure 3.3 QoS provisioning in 3 G Access[5]

Steps 7:9: In this step the Home PCRF selects PCC rules for the session establishment and send back AAA message to Proxy CSCF. In next step the Proxy CSCF sends SDP answer to the specific IMS client.

Steps 10:11 The IMS client binds the Session Description Protocol information to access specific Quality of Service parameters.

3.9 Literature Review

In this section various researches carried out on QoS, policy control, charging architecture and other IMS issues have been discussed.

The next generation wireless communication systems will be based on still emerging heterogeneous concepts and technologies and it is hoped that these systems will move towards anytime anywhere communication [44]. In the article [45] IP level signaling techniques have been proposed to provide Quality of Services to the different applications. The next generation mobile networks may support many radio access technologies. Besides mobile phones, laptops and personal digital assistants personal area moving and sensor networks are also part of this generation networks. In this research article, a variety of user terminals are discussed to use seamless communication sessions. To enable an access and transport technology, independent Quality of Service information methods which have Quality of Service signaling at IP level techniques needs to be introduced. For this goal, information set of information entities for this type IP level Quality of Service signaling Protocol was introduced. After evaluating the application program, session level signaling and IP QoS, these information elements are comparatively trouble free to find for the IP Quality of Service controller. Through the use of technology specific translation functions, these elements can also provide useful QoS information of different wireless technologies. With the passage of time various features and architectures have been included in the Third Generation Partnership Project. In [46] the application of PCC to the EPS has been described. This research article shows an overview of the release 8 policy and charging control based architecture [47] which are applicable to the evolved packet system [48][49].

In [50] the issue of several interpretations in the PCC architecture has been studied and its various implementations have been analyzed. The PCRF, the key element of the PCC architecture uses PCC rules as the primary information element. The PCC Rules are defined in the form of a structure. It consists of information that enables the QoS control and charging, user plane detection and policy for a service data flow. Two different PCRF prototypes have been designed in this research work and their advantages and disadvantages are explored. The first prototype is based on the PCC rule in the Media Sub Component structure while the second works on Media Components Description. The findings of the second prototype implementation are superior to the first prototype implementation. In research endeavor in [48] to explore a policy based QoS techniques and architecture in the current domain of UMTS PS has been made. Policy-based architecture has been proposed for QoS mechanisms in WLAN, as well as an

aggregation of various policy-based QoS architectures for UMTS and WLAN. The policy architecture deployed ranges through three scenarios. The first scenario is the pure hierarchical architecture while the second scenario is a mixed peering/hierarchical architecture and the third scenario is pure peering architecture [48]. The implementation of this architecture reduces session setup time and also reduces policy exchange load. The scalability feature for these interworking scenarios can be maximized. In [48] the functionality needed for integration between WiMAX networks with current IMS/PCC architecture defined has been presented.

The objective of this proposed architecture has been to just minimum changes to the standard 3GPP interface and its components [50]. New Interfaces have been added only where only essential in the WiMAX architecture in order to meet the access specific requirements.

Self organization of IP Multimedia Subsystem networks is an area which has not been explored in very much detail. The concept of self organizing IP Multimedia Subsystem is dissimilar than the concept of P2P-SIP [51]. The performance and advantages of having numerous SIP servers on the host are deeply analyzed in [52]. In that research paper, the design requirements which results to reduce IP Multimedia Subsystem server co-location and the various sorts of Session Initiation Protocol calls which can advantage from co-location of IMS servers has been described.

Various problems associated to (QoS) and architecture which requires minimal optimal IMS configuration has been described by Fabini et al. [53]. On one physical machine different domains were setup using a virtual test bed. The concept of distributed IMS architecture was presented by Matus et al.[6]. This architecture consisted of functional elements of network in the form of Distributed Hash Tables overlay networks. In [54] a self organization and adaptive IMS architecture was introduced, using a prototype test-bed results were retrieved. That paper discussed the possibility of merging and splitting of IMS functional elements at different nodes according to the network requirements.

Dutta et al in [55] introduced the concept of adaptive IMS architecture capable of self organizing. The merging and splitting of various functional components of IMS at various nodes without disrupting the ongoing session has been analyzed. To implement 3G WLAN

interworking, Hasswa et al.[56] proposed a model which gets benefits of the application layer of IP Multimedia Subsystem to modification in the IMS core components and WLAN. To achieve this objective WLAN application server was set up in the application layer of IP Multimedia Subsystem and a SIP server was implemented in the WLAN.

In [57] a tight coupling architecture was proposed in which WLAN was coupled to the UMTS through an SGSN emulator. Results of simulation showed that there is a service continuity during handoff from UMTS to WLAN. In handoff from WLAN to UMTS, there was a small disruption in the service.

Interworking solutions which are required in UMTS and in WLAN networks has been proposed in [58]. The architecture of IMS as proposed by the 3GPP was used for coupling of network and session management in real time scenarios. It provides many solution to deficiencies in the existing interworking architectures. Few ways to avoid the data duplication have been recommended.

In [59] the authors proposed two different approaches for deployment of 4G network. For session handling 3GPP IMS architecture was used. In the research endeavor in [59] LCSCW2 and TCSCW2 architectures for 4G heterogeneous wireless networks. The cost model to find the cost of IMS signalling and data traffic in the LCSCW2 architecture has been presented. The authors provided the direction for hybrid approach.

In [60] an interesting technique known as Networking Context Aware Policy Environment was introduced. This solution is established on a policy engine installed on a terminal device. This engine collects information provided by the user, the network operator and as well as the protocols. Dutta et al. investigates the mobility management schemes in Multi Media Domain (MMD) networks[61]. The proposed scheme used the distributed signaling servers around the edges of the network. A test-bed for this architecture was developed which analyzed three different types of handoff. In [62] a solution has been proposed for the issues raised during connecting the IMS when using conventional internet. The proposed technique was used on UMTS domain, DiffServ core, an IMS core and an internet domain. When the packets of the

internet users are marked as best effort, it causes a problem. For this IP FIX solution was introduced. This technique has minimum packet overhead.

An effort in [63] was made to propose a signaling architecture for QoS provisioning in IMS networks. In this architecture a QoS broker was introduced which monitors the network bandwidth and also responsible for dealing with policy exchange between domains. Mani & Crespi investigates in [64] the problem of Quality of Service provisioning between various inter domains and different technologies. For each access network a separate policy decision function was introduced with the central PDF which is present in the IMS network.

Another framework that deals with the mobility as well as Quality of Service in an IP Multimedia Subsystem networks was proposed in [65]. The Domain Policy Manager is one and the policy enforcement point is the second major parts of this solution. The inter domain vertical handoff management has been analyzed to highlight the performance of the architecture.

In [67] the author proposed an architecture for harmonizing IMS with Multiprotocol Label Switching (MPLS). In this solution IMS function is used to get the session profile for LSP selection. The concept of dual phase capacity assignment has also been proposed in this work to maximize the utilization of resources. In [68] a mechanism was proposed for the management of QoS in the NGN with plan of IMS session and the advantages of this architecture in MPLS has been explored. In [69] a method used to preserve the QoS values as well as charging data of users communicating through IMS networks has been proposed. In this method with the data call, original descriptions of user sessions are migrated. The charging records are also allowed to move. This helps in restoration of the service quality.

End to End QoS for Inter-Domain IMS has been investigated in [70]. The authors in [71] investigated the QoS estimation in real time. Fuzzy logic is used to evaluate the IMS networks in connection with efficiency and also reliability. It was concluded in this research paper that there is a need of autonomous system based on eTOM process and fuzzy logic for real time correlation of deterioration in effective mechanism of Quality of system for watching real-time services in IP Multimedia Subsystem networks.

In [72] for real time streaming services which is the main objective of IMS a streaming service architecture having a cross layer playback rate been proposed. In [73] the NSIS (Next Steps in Signaling) solution has been proposed that combines the DiffServ and IntServ with other properties of control traffic. The purpose is to show the integration with IMS. NSIS permits session binding which can be used for local optimization.

This technique adds detection rerouting to enable the system to identify route changes and find a new route automatically. Detailed analysis of SIP performance has been explained in [46]. With the help of measurements it is shown that parsing, memory allocation, string handling, and thread architecture have effect on the performance of SIP.

In [47] message prioritization mechanism in SIP server architecture has been implemented. Several facts with respect to the design and the corresponding prioritization of message and strategies for message rejection have been explained. In [48] negotiation of QoS in SIP has been investigated. The processing of parameters necessary for Quality of Service, based on local policy of the network as well as SIP negotiation by the policy decision point has been evaluated. The approach proposed in [49] was build on major concepts of QoS in order to support to SIP calls carrying them in DiffServ IP trunks.

Huang *et al* in [50] demonstrated a scheme of dual stack in order to minimize the SIP tunneling overhead and to reduce the transmission delay in 3G IMS. In [51] a scheme for mobility management which is cost efficient has been proposed by integration of MIP with SIP. In [52] the author proposed a technique that combines the mobility management in Mobile IP and SIP. The previous method uses independent registration for Mobile IP and SIP. From the analysis of the numerical results, it is shown that the number of signaling messages and delay duration was minimized.

SIP mobility management have QoS parameters has been explored in [46-52]. All these techniques have investigated data transfer using post session set up.

3.10 Summary

We've spoken about cloud computing in this chapter. Various aspects of cloud computing have been elaborated. Service models i.e SaaS, PaaS and IaaS has been explained in detail. The next section describes the various types of private cloud, community cloud, public cloud and hybrid cloud. One of the key objective of the cloud computing is ensure that the system is scalable. The scalability issues has been described in detail. At the end of the chapter concept of virtualization and various virtualization tools has been explained. Further virtualization in IP Multimedia subsystem and the concept of virtual client and virtual server has been described in details. Various entities in the virtual server and their working has been described. How integration of IMS PCC architecture with virtualization IMS client model has been explained in detail. Provision of QoS in virtualized environment has been discussed in detail. At the end the detailed literature review related to Quality of Service and virtualization has been given.

4. Proposed System Virtualization

4.1 Introduction

In the proposed system a server known as surrogate is used. The concept of surrogate was introduced in [5] and has been explained in detail in previous chapter. The surrogate provides the SIP based accessibility to the users and acts as a virtual server. In the previous model a web server was used, for better work load balancing and to ensure communication we have introduced number of servers with shared memory. Any device having the capability of IP connectivity such as mobile device, laptop, PC, IP phone etc can be used as a UE and connect with the surrogate.

The UE communicates with the surrogate via HTTP, while the surrogate communicates with the IMS core network via SIP. In proposed model, the virtualized IMS consists of three virtualized IMS machines having shared memory. Shared DB is a shared database among the various IP Multimedia virtual machines instances. To assign specific IMS VM to the subscriber, IMSLocator is used during the registration process. It is also used in localizing the IMS VM instance during the phase of discovery. IMSLocator is just a simple proxy without changing the message content. The IMS locator works as a manager for shifting communication to any of these machines depending on the workload. The proposed model is shown in the figure 4.1. The intention in proposed model was to implement scalable system without markable increase in the end to end session setup delay within the acceptable bounds.

4.2 Provision of Quality of Service

Following the 3GPP access rules, in our proposed model the QoS provisioning is as follows.

1. The IMS client initiates the session using SIP and SDP messages. The Proxy-CSCF extracts the SDP information and sends to the Home-PCRF via AA-Request.

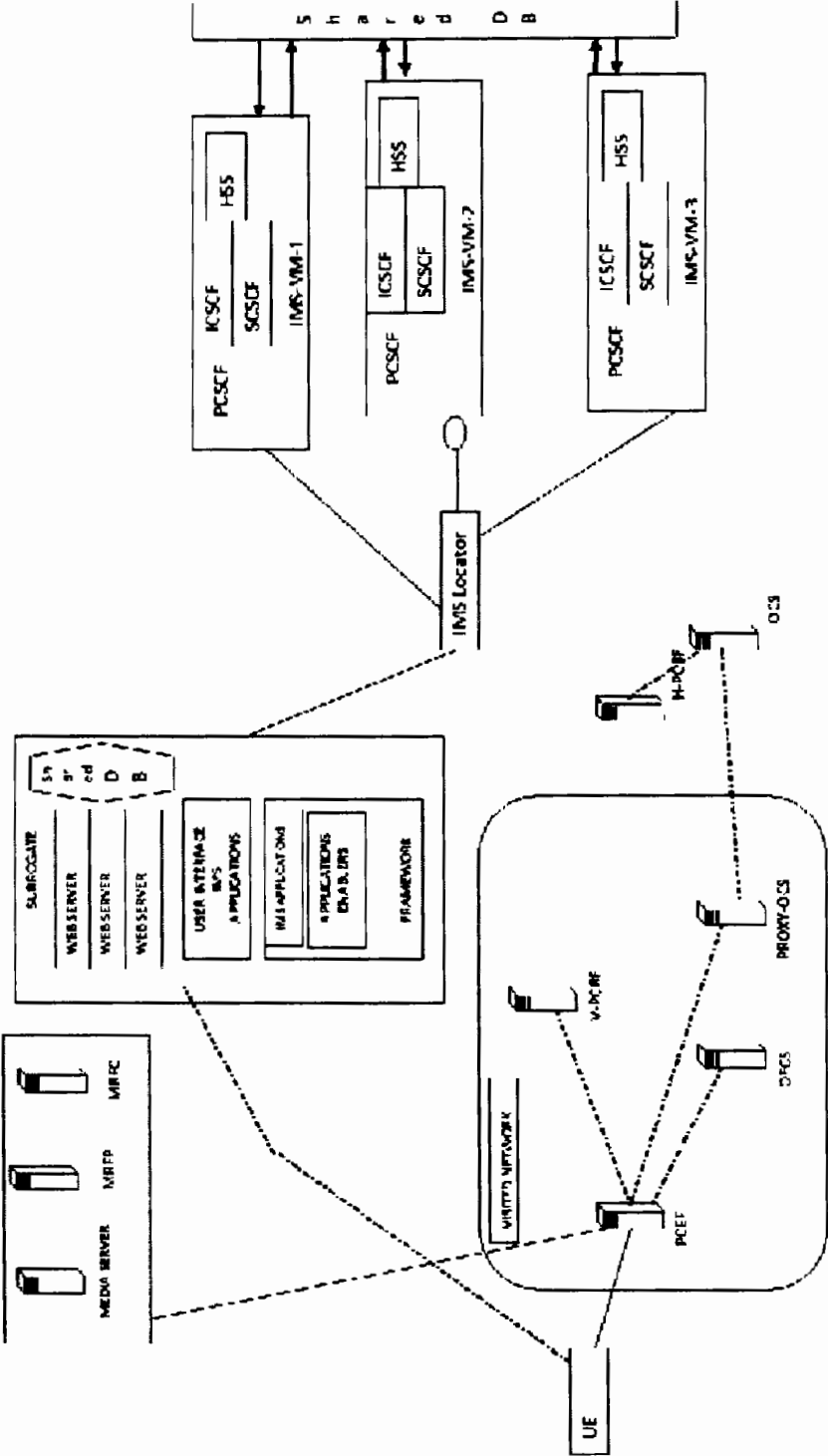


Figure 4.1 proposed model

2. The Home-PCRF selects a set of PCC rules for this session based on the session description.
3. The PCRF replies with AAA message to the corresponding Proxy-CSCF.
4. In the next step the P-CSCF forwards the final SDP answer to the client
5. When the IMS client receives the final SDP responses, it sends a service response message with access specific parameters.
6. In next step the PCEF request V-PCRF via CCR message for the IP QoS parameters. The visiting V-PCRF sends the CCR message further to home-PCRF.
7. The PCEF generates the QoS rules. The Home-PCRF reply with CCA message.
8. The Visiting-PCRF gets the QoS rules from the Home-PCRF.
9. Upon successful validation of the QoS rules, the visiting-PCRF provide PCC rules to the PCEF.
10. The PCEF accepts the PDP context action request for the provision of QoS parameters.

4.3 Support of Equipment

Hardware

- Laptop HP corei5 (OpenIMS Server)
- Client System
- Switch Ethernet
- Speaker
- Microphone

Software

- Operating System Ubuntu 14.04 LTS (OpenIMS)
- DNS Server (BIND-9.3.2)
- Web Server (Apache2) MySql Server
- Wireshark Network Protocol Analyzer
- SIPp Traffic Generator Tool

4.4 System Evaluation

After successful installation and configurations of the system, we need to evaluate the implementation results. The objective of the evaluation is to measure the performance of the proposed model.

4.4.1 Process Delay in OpenIMS

It is the time taken by the SIP signal inside the OpenIMS server before it is forwarded to the destination. When the server receives the INVITE signal, it checks the user registration status to find the called user IP address and user port. After finding the user port it will then pass INVITE signal to the destination on that IP address and user port . Simple checking is done for other signals only perform the role of proxy only to forward the calls. The other signals only need short time for the processing of server. Figure 4.2 shows the standard and proposed model of delay. The graph shows remarkable low time of connectivity.

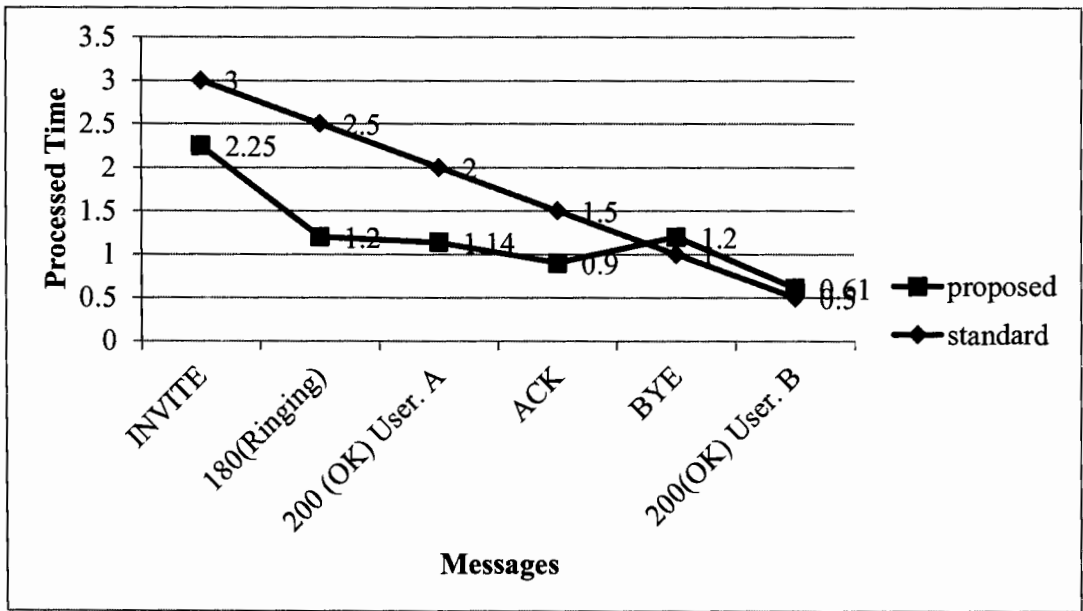


Figure 4.2 Message standard and proposed model process delay

4.4.2 CPU utilization Measurement

Figure 4.3 to Figure 4.6 shows the percentage utilization of CPU. There are five steps each consists of 5 minutes and total 25 minutes. This test was repeated with or without the proposed architecture in place.

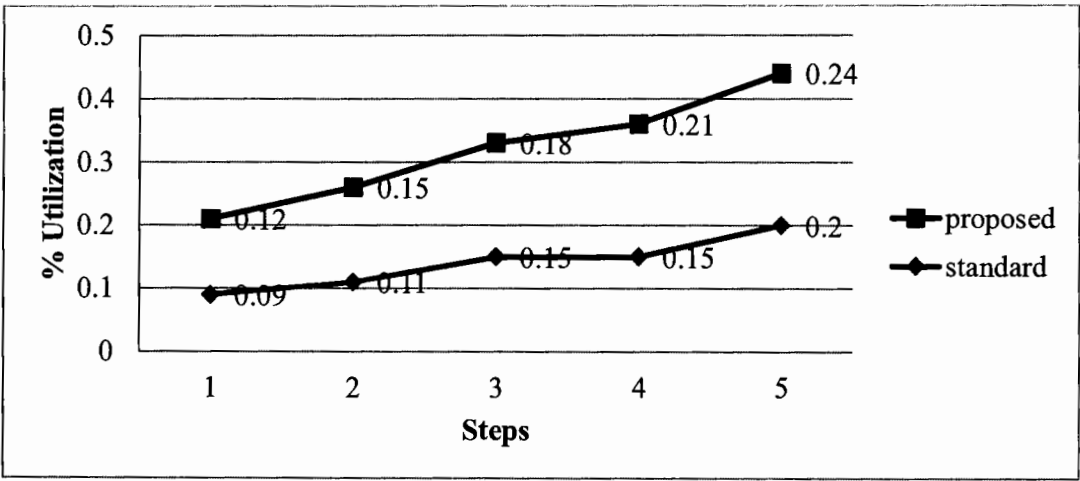


Figure 4.3 :Comparison between standard and proposed P-CSCF CPU utilization

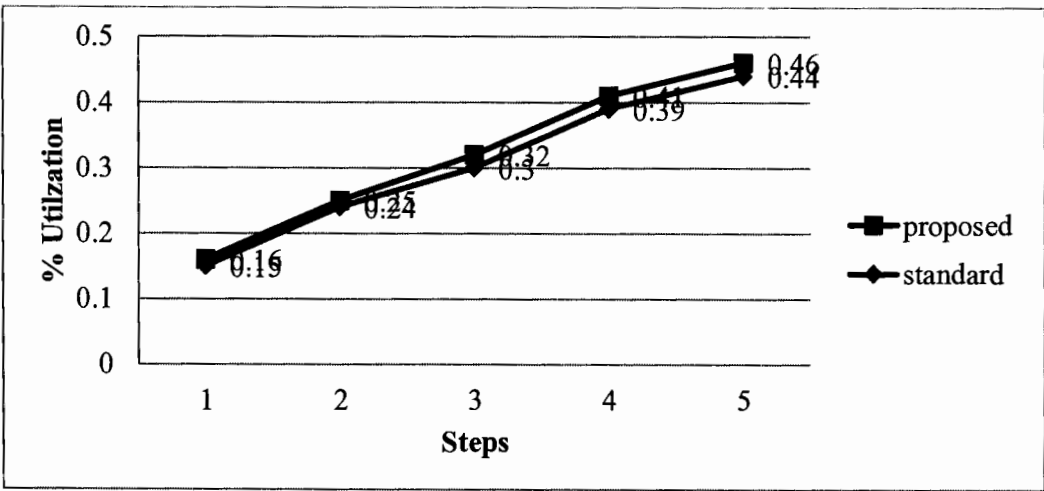


Figure 4.4 :Comparison between standard and proposed I-CSCF CPU utilization

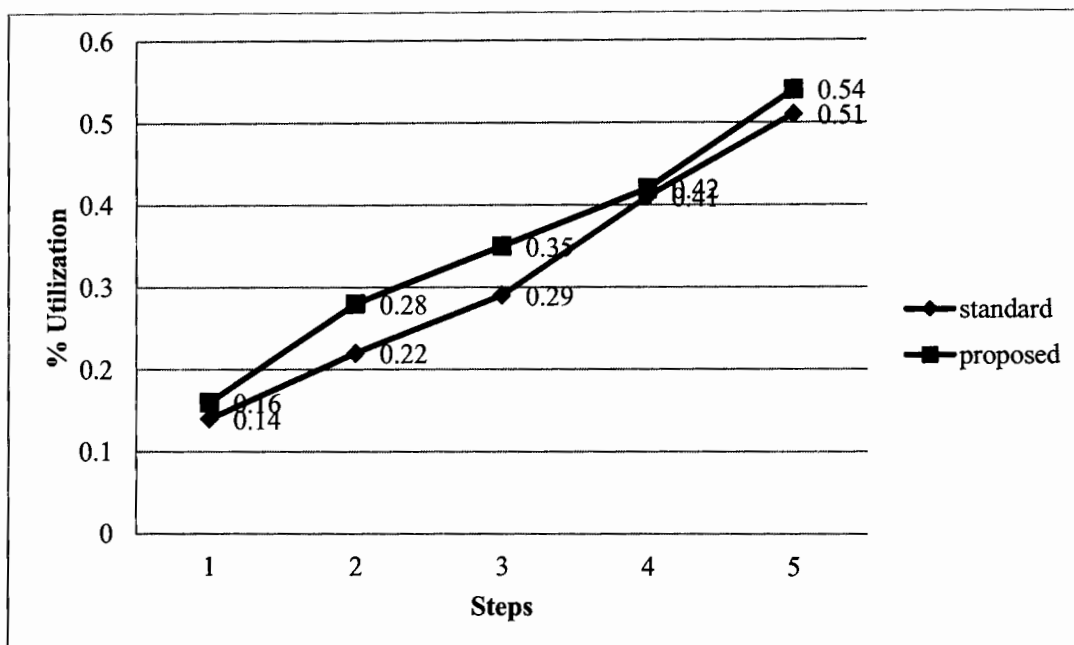


Figure 4.5: Comparison between standard and proposed S-CSCF CPU utilization

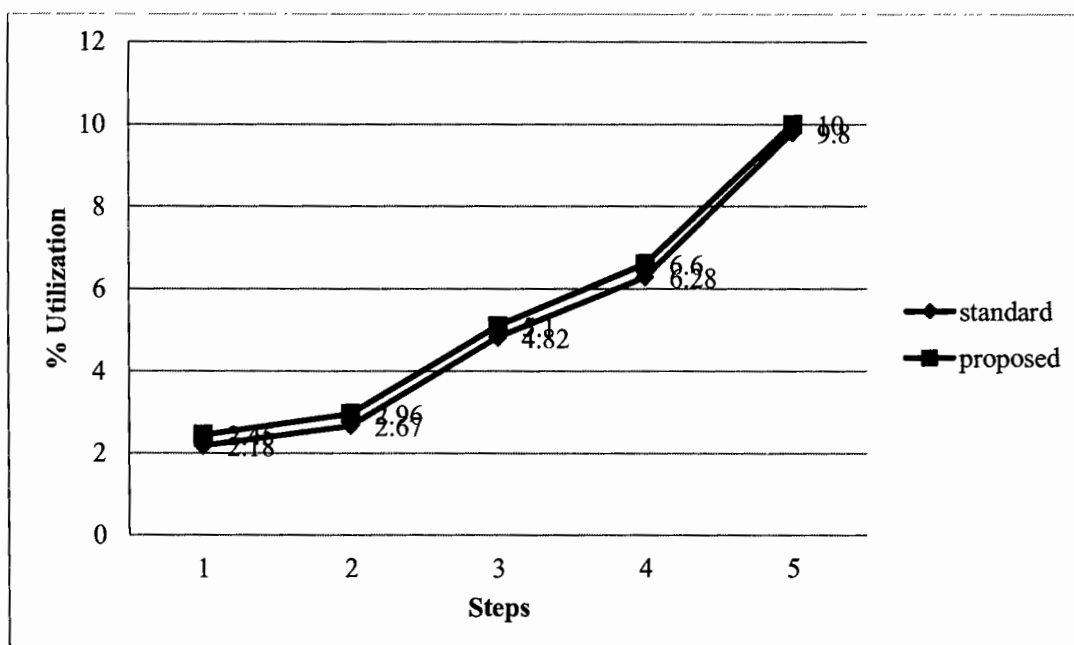


Figure 4.6: Comparison between standard and proposed HSS CPU utilization

Our objective is to make sure that there is no deviation in performance of the actual registration operations when comparing proposed and standardized architectures. A registration preamble was carried out with 4000 to provide a base for the de register and re-register scenarios.

The scenarios which are carried out during the benchmark runs may be registration of a user, de-registration of a user or either the re registration of a user. For the registration scenario 25 calls per second (CPS) target was set. The purpose was to exceed the total capacity of the test bed near the end of the test.

With the constant distribution till the scenarios executed reached 4000, the IMS bench program was configured to trigger 10 CPS. The stir phase of the test is planned to little randomize the starting conditions of the test. In order to achieve improved accuracy, certain functions have been exercised at least once. The step which is mix of registration, de registration and re registration scenarios executed at 5. The step consisted of 5 minutes.

The percentage of mix of the scenarios was 40% for registration, 40 % for de-registration and 20% re-registration. The the next step phase comprised to the number of scenarios as of the previous phase in the same ratio but steps are increased. Each step consisted of 5 minutes and there was an increase of 5 CPS per step. Total 25 number was set as a target for CPS resulting in 5 distinct steps. This resulting in a test run took roughly 36 minutes and 59 seconds. The test was conducted with and without the proposed architecture in place i.e for standard architecture and proposed architecture. Figure 4.3 - Figure 4.6 shows the % age CPU utilization of Call Session Control Functions Servers i.e P-CSCF , I-CSCF and S-CSCF and Home Subscriber Server. The graphs show that the besides scalable platform, reduction in session setup delay and use of light weight user equipment the percentage utilization of the the servers has increased which shows the system performs more better. The figure 4.6 shows that the HSS uses highest utilization of

the CPU due to the part it plays in the process of registration. Further it has been find out that the overall workload management has been improved.

4.5 Advantages of the proposed model

1. The User equipments are lightweight therefore it uses less computing resources.
2. Due to virtual IMS client and use of surrogate the communication time becomes low.
3. By the use of virtual machines for Virtualized IMS, the load balancing has been improved this will increase the scalability of the system.
4. The QoS will increase by un interrupted, continuous provision of services and measures for the load balancing mechanisms.
5. Better utilization of system resources due to virtualization.

4.6 Summary

In this chapter the proposed model has been described in detail. The UE communicates with the surrogate by using HTTP protocol and the Surrogate interacts with IMS core network using SIP protocol. In proposed model the virtualized IMS consists of three virtualized IMS machines. Shared DB is a shared database among the various IP Multimedia virtual machines instances. Operating System Ubuntu 14.04 LTS (OpenIMS) ,DNS Server (BIND-9.3.2), Web Server (Apache2) MySql Server,Wireshark Network Protocol Analyzer ,SIPp Traffic Generator Tool software are used. As described in Figure 4.3 – Figure 4.6 the session setup delay has been remarkably reduced in the proposed system as well as the percentage utilization of the server has increased. It means uninterrupted supply of traffic is insured with greater speed in the proposed system.

5. Security Fundamentals

5.1 Introduction

SIP security is one of the vital necessity in the communication Networks. Authentication is the key service needed by Session Initiation Protocol. An authenticated user can only use SIP service. Different authentication schemes have been introduced to make enhancement in SIP security. Session Initiation Protocol has been proposed by Internet Engineering Task Force.

It is signaling protocol being used in multimedia communication sessions. The Session Initiation Protocol defines messages for establishment, modification and termination of a session between two points. This protocol work at the application layer run User Datagram Protocol or Transmission Control Protocol[81][82]. The protocol is based on HTTP protocol is a text oriented protocol. A session established via SIP may have many types of media streams but there is no need for separate streams for the applications. Session Initiation Protocol defines two kind of message i.e SIP requests and SIP responses.

5.1.1 Password Guessing Attacks

An attacker may catch the communication between the server and by guessing the password by attempting various combination of password repeatedly and then verifies the correctness of all the guesses[83].

5.1.2 Replay threats

In such type of attack, the attacker impersonates another honest participants(s) through reuse of information in the protocol. The adversary may intercepts the message and re-transmit it.

5.1.3 Man-in-the-Middle Attack(MiTM)

In the MiTM-based threats, the attacker establishes an independent connection and secretly relays and may alter the communication between two victims. The victims assume that they are

communication with each other directly via private connection and actually the communication is entirely controlled by the attacker [84].

5.1.4 Stolen-Verifier Attacks

Password verifier is stolen from sever by some means and is used to masquerade as a genuine user in the authentication process later on.

5.1.5 Denning-Sacco Attacks

Old session key is compromised between server and user and the adversary keeps on trying to get the user password or the server's private key or session keys[84].

5.1.6 Registration Attacks

In the registration attack the adversary uses a spoofed unregister message to the server and the registration of the user is cancelled at the server.

5.1.7 Known-key Security

The role of the known key security is to a unique secret session key between user and server during establishing a session. In case one session key is not safe then the private and session keys are safe and are not compromised.

5.1.8 Session key security

For secure communication, it is vital that session key is only known to the server and the user which is ensured by session key security.

5.1.9 Perfect Forward Secrecy

This characteristics signifies that if the long term private secret keys of one or more entities are vulnerable the previous session keys of the two genuine users is not compromised.

5.1.10 Mutual Authentication

It means that the concerned participants authenticate each other after the implementation of the same protocol.

5.2 Review of HTTP Digest Authentication Scheme for SIP

As earlier discussed SIP is a text based Protocol. It is based on the HTTP protocol. To connect to network and to establish a call SIP uses REGISTER and INVITE messages. User authentication is very fundamental security service in Session Initiation Protocol.

When ever a client is keen to avail SIP service it has to be authenticated. The primary authentication mechanism is HTTP digest authentication[85]. This scheme works on the challenge-response methodology. A nonce is used to challenge the target.

Step 1:

REQUEST message sent by the user to the server

Step 2:

Generation of a nonce by the server and submission of error message for the sake of authentication

Step 3:

Nonce value is applied with a hash function which is obtained in the challenge. The user name and password is already shared with the server. The original request message along with the nonce value, response value, username and realm is sent back.

Step 4:

As per the user name the server obtains the password of the client. Then a verification of the nonce are carried out if it is correct then it finds a hash function of the nonce, password, realm and username. The result of the hash function is then compared with the response of the user. On

this verification the client is authenticated. This mechanism is easy in implementation and its performance is also high but there is a need to proof its security against numbers of attacks[86].

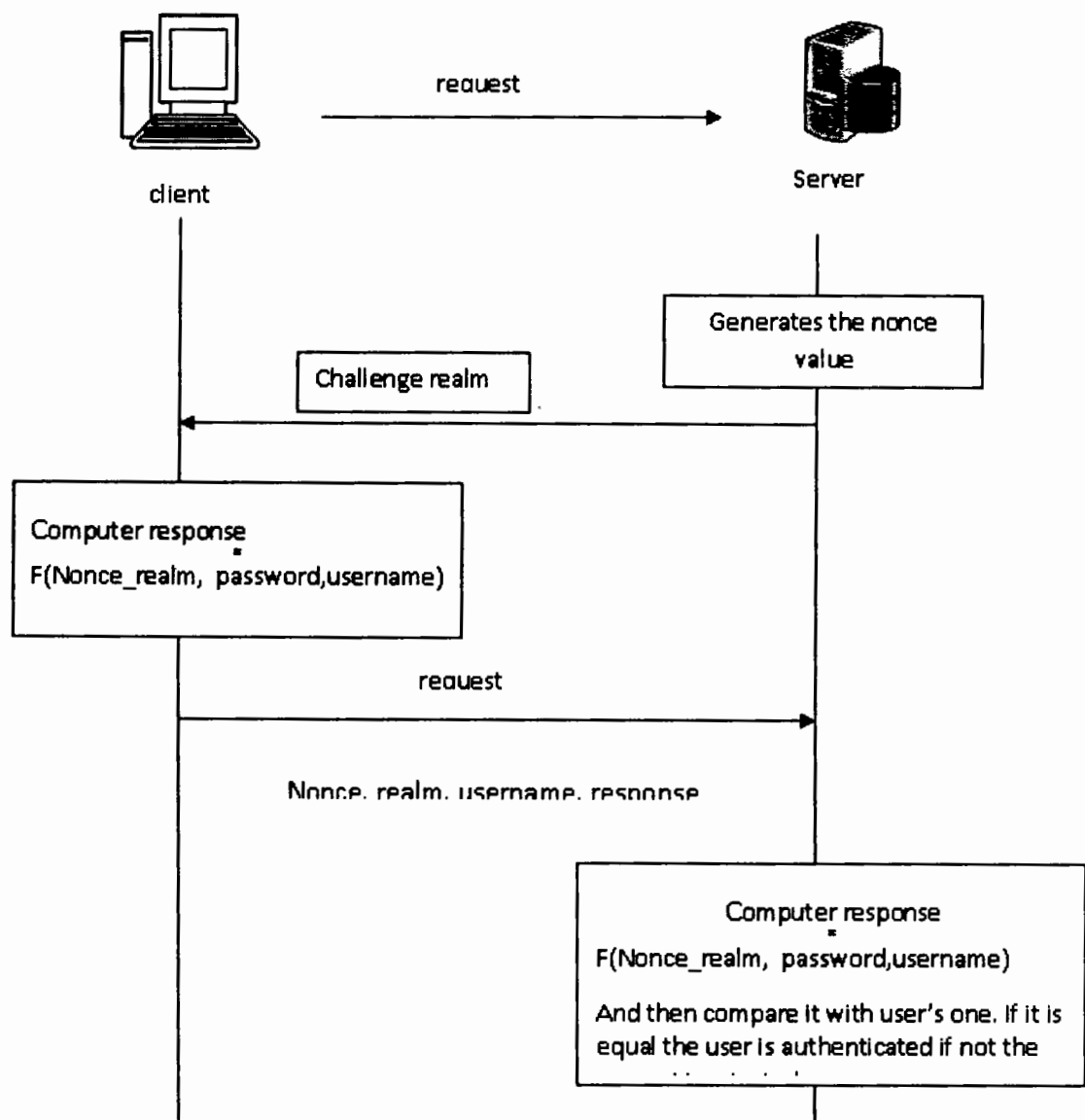


Figure 5.1. HTTP digest authentication scheme [102]

5.3. SIP Authentication Mechanisms

A number of authentication protocols have been introduced in the last decade and a few are described in what follows.

5.3.1 Authentication Methods Based on Diffie Hellman:

Yang et al.[86] showed that SIP authentication protocol based on HTTP digest authentication only ensures the unilateral authentication. It is susceptible to offline password guessing attacks as well as server spoofing attack. In [81] a SIP authentication scheme was introduced using Diffie-Hellman key exchange algorithm. The showed the flow of messages when a user access the resources of the server.

They described that the proposed scheme can defy the off-line password guessing attacks, replay threats and the server impersonation attacks. They showed the performance evaluation of their scheme with the HTTP digest scheme and Encrypted Key Exchange scheme and proved that their scheme is better in efficiency as compared to these schemes.

However their scheme has to maintain preconfigured password table. Their scheme also needed an exponential computation which does not suits the client device having limited computing resources [88].

5.3.2 Authentication Methods based on Elliptic Curve Cryptography

A SIP authentication scheme was proposed by Durlanik et al.[89] by using an elliptic curve cryptosystem. A small key size was used in this protocol and the computation of this protocol is also very fast. A comparison evaluation was made with DH and it was pointed out that its performance was far better than DH in terms of execution times and use of memory. As the server stores the user passwords in a plaintext so it is not safe with untrusted verifiers. Besides this it also susceptible to man in the middle attack as well [90].

Wu et al.[90] introduced Elliptic Curve Cryptography (ECC) based authentication and key exchange scheme. They assert that the proposed scheme offer access control, data integrity, perfect forward secrecy and data confidentiality. As per their claim the scheme is protected from man in the middle attacks, off line password guessing attacks, server masquerading attacks and replay attacks as well. This scheme is favorable in situation where the memory is low and and the

computations is fast. Wu's scheme is not protected against off line password guessing attacks and is not completely safe[91].

Yoon and Yoo[92,91] discovered that Tsai's scheme is susceptible to stolen verifier attacks, Denning-Sacco attacks, offline password guessing attacks and also lacks the perfect forward secrecy. They concluded that the authentication and key exchange protocol scheme introduced by Wu et al. is susceptible to offline password guessing attacks..

To counter these vulnerabilities they proposed a new scheme by using the DCDLP which is more effective than the earlier similar authentication schemes. Besides efficiency this authentication scheme is prone to password guessing threat, reply threat and stolen verifier threat[93].

To tackle attacks in Tsai, authentication scheme R, Arshad et al[94] suggested a new protocol which is more capable and secure based on elliptic curve discrete logarithm problem. But this scheme is still susceptible to offline password guessing attack. Based on DCDLP, Tang et al.[95] introduced a secure authentication protocol however this scheme is unsafe against registration attack and offline password guessing threat[84]. To counter the vulnerabilities in Tang et al. scheme, Sadat et al.[84] introduced a new SIP ECC based authentication scheme.

5.3.3 Authentication Methods based on Nonces

Based on the random nonce concept, a new secure authentication scheme was introduced by Tsai[96]. This authentication scheme provides a low computation cost and is also suitable for devices needing low computation. Yet this scheme is susceptible to attacks like Denning-Sacco attack, stolen-verifier threat and off-line password guessing threat. This scheme also fails to offer perfect forward secrecy[91,94]

5.4 Authentication Methods based on Identity based Encryption

The Identity authentication method is based on some ID parameter e.g. an email address to make the public key of the user. The generation of public key of user is made by a trusted third party

and is securely conveyed to the user. The primary advantage of this authentication scheme is that it is secure against security problems with passwords. It also removes problems with PKI certificates. Long signature is the only shortcoming in this mechanism. Ring et al.[97] introduced a SIP authentication scheme using identity based cryptography. This authentication scheme guarantees the mutual authentication however its computation cost is high. H.H,Kilinc[98] introduced a scheme with combination of ECDSA and identity based authentication schemes of Hess[99] Cha-Cheon [100] . The advantage of this scheme is that it is secure to password guessing attack and spoofing attack but this scheme uses large signature size. Rongwei Yu et al.[26] presented identity based authentication scheme using signatures to resolve the problem in SIP authentication. This scheme support the perfect forward secrecy and offer a low computational cost.

5.5 Authentication using Smart Card

The Session Initiation Protocol is being used to control Voice over Internet Protocol based communication session but it is insecure as it is inherently an open text based protocol. Security of SIP is a challenge and many solutions have been presented to secure the Session Initiation Protocol. Zhang et.al[103] proposed authentication scheme based on smart card without any password verifier database. This authentication scheme has some disadvantages and it can be optimized and made more secure in terms of cost of exchange .

In Zhang et.al scheme[103] a user sends a REQUEST message to server, an attacker may get the message. After intercepting the message the adversary may repaly the message towards server at other time. As the message has no timestamp or freshness, the server has to produce the challenge message. The servers will examine and will come to know the whether the message is valid or not in next step of response message send by the attacker. In this way a DOS attack may be initiated by the attacker.

Further if the server secrete is intercepted by an attacker he can reach to user's passwords. In this situation a single secret may expose the complete system if it is not safe. The Zhang scheme uses

one and half round trip and can bring to a single round trip. To overcome these problem following scheme has been presented.

5.5.1 A Single Round-Trip SIP Authentication Scheme for Voice over Internet Protocol using Smart Card

To eliminate the imperfection in Zhang et al. scheme this scheme has been proposed by using an authenticated key agreement protocol.

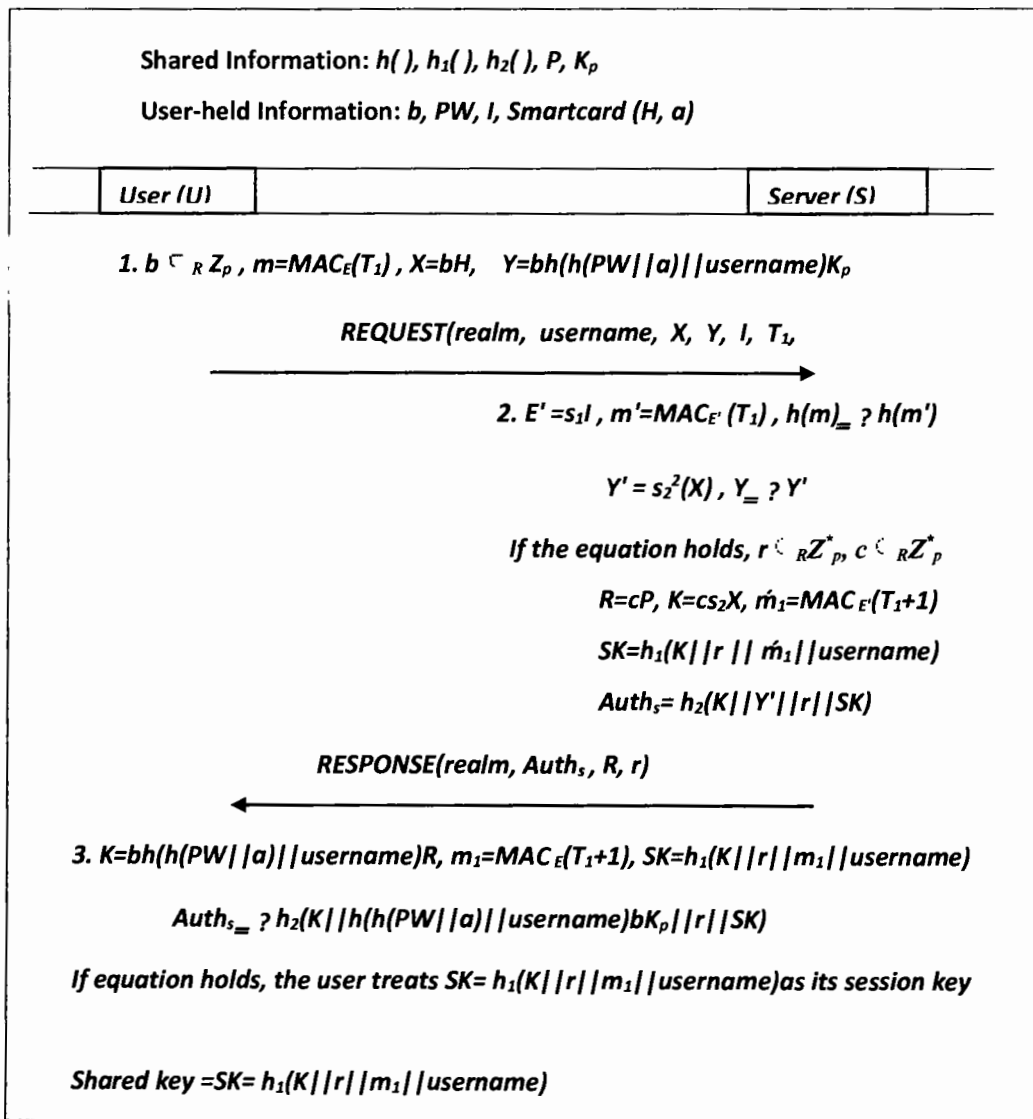


Figure 5.2. Proposed authentication scheme[104]

The authentication phase is completed in a single round trip phase in order to enhance the efficiency of the protocol in the proposed scheme. The scheme involves the authentication between smart card(user) and server. The authentication process is completed in system setup procedure, registration procedure, authentication and password updating procedures.

This authentication scheme provides security against following attacks

- Replay threats
- Man in the Middle Attack
- Modification threat
- Denning-Sacco Attack
- Offline dictionary threat without using Smart Card
- Offline dictionary threat using Smart Card
- Known key Security
- Mutual Authentication
- Session key Security
- Perfect forward Secrecy
- Secure password update

5.5.2 Comparison and Cost Analysis

The Zhang et al. protocol consisted of $9 T_{ESM} + 2 T_{EPA} + 10 T$ messages where as the proposed scheme has $7 T_{ESM} + 8 T_H + 4 T_{KH}$ messages. In a single run of the Zang et al. protocol, 9 scalar multiplication computations, 2 elliptic curve(EC) point additions and 10 hash operations are incurred. While the proposed protocol 1 incurs 7 scalar multiplication computations (T_{ESM}), 8 hash operations (T_H) and 4 keyed hash (T_{KH}) operations. It can be observed that the [104]scheme incurs two less T_{ESM} operations as compared to Zhang protocol. The detail is given in the table 5.1.

Schemes Types of messages	Zhang et. al. scheme	Proposed scheme
Registration messages	$1 T_{ESM} + 1 T_H + 1 T_{INV}$	$1 T_{ESM} + 1 T_H + 2 T_{INV}$
Authentication messages	$9 T_{ESM} + 2 T_{EPA} + 10 T_H$	$7 T_{ESM} + 8 T_H + 4 T_{KH}$
Password Update messages	$2 T_{ES} + 2 T_{DS} + 1 T_{ESM} + 6 T_H + 1 T_{INV}$	$2 T_{ES} + 2 T_{DS} + 1 T_{ESM} + 6 T_H + 1 T_{INV}$
Total messages	$11 T_{ESM} + 17 T_H + 2 T_{INV} + 2 T_{EPA} + 2 T_{ES} + 2 T_{DS}$	$9 T_{ESM} + 19 T_{H/KH} + 3 T_{INV} + 2 T_{EPA} + 2 T_{ES} + 2 T_{DS}$

Table 5.1 Comparison of Zhang et al scheme, and Azeem et.al[104]

The performance analysis shows that the contributed scheme is more efficient as compared than the Zhang Schemes. Table 5.2 shows various attacks on both the schemes.

Schemes Threats /Roundtrips	Zhang et al. scheme	Proposed scheme
1. Modification threat	S	S
2. MiTM threat	S	S
3. Replay threat	S	S
4. Mutual Authentication	S	S
5. DoS threats	IS	S
6. Known key security	S	S

7. Perfect forward security	S	S
8. Session key secrecy	S	S
9. Stolen verifier threat	S	S
10. Denning sacco threat	S	S
11. Single Round trip of protocol	NP	P

Table 5.2: Attacks on protocols under different conditions[104]

5.5 Summary

This chapter consists of definitions and brief descriptions of various types of security attacks e.g password guessing attacks, replay threat, MiTM threat, Stolen-verifier threat and other various important attacks. Different authentication schemes has also been introduced during the last decade. Few authentication schemes for example authentication methods based on Diffie Hellman, Authentication methods based on Elliptic curve cryptography , Authentication methods based on nonces and Authentication methods based on identity based encryption are described in detail in this chapter.

6. Proposed System Security

6.1 Introduction

The IMS provides a generic framework for voice, data and video communication services available to mobile and land users [2,134]. The advantage of IP Multimedia Subsystem is to offer, by using its middleware, unique and common methods for QoS standards, charging criteria, authentication and security etc. This framework is based on SIP [104], which is a text-oriented client server protocol to manage multimedia sessions [119]. It is one of the frequently used protocols to establish online communicating sessions for multimedia services between user and server. For making use of the SIP protocol, the client needs to be authenticated from SIP server initially, which is quite significant for secure multimedia-based communicating sessions.

In the last decade, several SIP protocols could be witnessed in the academia [2, 106, 117, 120, 125]. For this, a pioneer scheme was demonstrated by Franks et al. for HTTP [111]. Onwards, Yang et al. [123] remarked that the current SIP protocol as based on HTTP, is less secure for having vulnerability for offline password guessing threat and stolen verifier threat. Besides, the scheme was not appropriate for low end power deficient devices. [108, 113]. Due to the short key size of ECC, it is being employed in various cryptographic protocols, including SIP protocols. Durlanik et al. [109] also presented an efficient ECC-based SIP protocol. Afterwards, Wu et al. [143] demonstrated another ECC-based SIP protocol. However, the schemes [109, 122] are found to be prone for offline password guessing and stolen verifier attack by Yoon et al. [126]. Also, Yoon et al. put forward another improved SIP-based scheme. However, Gokhroo et al. [110] and Pu [129] indicated Yoon et al. protocol is also susceptible to guessing and replay attacks. Thereafter, Tsai [114] presented a symmetric cryptography based SIP scheme using XOR operation, but was discovered to be vulnerable to many attacks [103, 107, 116, 124]. Yoon et al. [124] put forwarded a SIP scheme after finding attacks on Tsai [114]. Nonetheless, Xie [121] pointed out few limitations including guessing and stolen-verifier attacks in [124], and introduced an enhanced protocol. Then, Farash et al. [112] discovered impersonation attack and guessing attack in Xie's protocol, and presented an improved SIP protocol. Thereafter, Zhang et al. [128] designed a simple and efficient password-based SIP authentication protocol, however, Lu et al. [115] discovered that [128] is not able to resist insider attacks and fails to offer mutual

authentication. Lu et al. presented an enhanced scheme countering the limitations in [129]. Afterwards, Chaudhary et al. [105] found user and server impersonation attacks in [115]. Recently, Dongqing et al. [127] found stolen verifier attack in Lu et al. and session key attack in Chaudhary et al. [105], and presented an improved scheme. We have found discover that Dongqing et al. [127] is again vulnerable to privileged insider attack, DoS threat, and session specific temporary information threat. Besides, the scheme bounds the system to be adhere time synchronization feature, which is a tough assumption to be implemented. Considering those drawbacks, we propose an proficient and secure protocol as demonstrated formally using BAN logic analysis which can be witnessed from the forthcoming sections.

6. 2. Preliminaries

We briefly illustrate hash-based function, Bio-hashing and elliptic curve cryptography.

6.2.1 Hash Function

A symmetric key-based one sided hash digest $h: \{0, 1\}^* \rightarrow Z_q^*$ encompasses the subsequent properties:

1. The hash-digest function h generates a message of predefined size on receiving an input of random length.
2. Using the hash function, i.e $h(a)=b$, it is an intractable problem to calculate $h^{-1}(b)=a$;
3. If we are given a , it is hard to calculate a' , such that $a' \neq a$, but $h(a')=h(a)$;
4. Additionally, it is also intractable to calculate a pair a, a' given that $a' \neq a$, but $h(a')=h(a)$.

6.2.2 Elliptic Curve Essentials

The elliptic curve cryptography can be defined with elliptic curve E/F_q as a set of points located in a prime field F_q , on a non-singular elliptic curve [27] as shown below:

$$y^2 \bmod q = (x^3 + ux + v) \bmod q \quad (1)$$

such as $u, v, x, y \in F_q$ and $(4u^3 + 27v^2) \bmod q \neq 0$. We characterize an elliptic curve point as $P(x, y)$ as if Eq. (1) is conformed, where the point $Q(x, -y)$ being negative version of P , also we can say $Q = -P$. We take $P(x_1, y_1)$ and $Q(x_2, y_2)$ as two separate points on the above equation (1), though, the line ln , as tangent of the above equation (1) meets P and Q while intersection the

curve at point $-R(x_3, -y_3)$. Similarly, its reflection on x-axis is on point $R(x_3, y_3)$, i.e. $P+Q=R$. The range of points E/F_q including *point at infinity* (O) comprise an elliptic-curve cyclic group, i.e. $G_q = \{(x, y) : x, y \in F_q \text{ and } (x, y) \in E/F_q\} \cup \{O\}$. We can describe a scalar point multiplication using G_q as $\tau.P$ denotes the repetitive additions of P in itself, where $P \in G_q$ characterize an order n , provided n being smallest positive integer, furthermore $(n \cdot P = O)$ holds as well.

6.2.3 Bio-hashing

The Bio hashing function [128] is employed to capture biometric features of a person such as finger prints so that it can be used for authentication purpose. Jin et al. [131], in 2004 demonstrated a two-factor authentication protocol for capturing fingerprint attributes for a particular user, and also engenders a tokenized pseudorandom number, which is then used to generate a compact code particular to some user, also known as bio-hashing. Thereafter, a more developed and worked Bio-hashing operation was demonstrated by Lumini et al. [132]. Actually, this Bio-hashing operation maps the user's oriented biometric properties on exclusive random vectors to construct a Biocode that discretizes projection coefficients, and then the resultant code could be remarked as a protected Bio-hashed password.

6. 3. Working and Crypanalysis of Dongqing et al Scheme

The design of Dongqing et al. protocol is explained in the following section.

6.3.1 Working of Dongqing et al. protocol

There are three stages in the Dongqing et al.'s protocol [127] i.e registration, login and the mutual authentication procedure as described in the Figure 6.1. Some significant symbols employed in this protocol are mentioned in the table 6.1 as below.

Symbols	Description
U_i, S_j, RC	ith user, jth server, Registration centre
ID_i, SID_j	Identifies of U_i and Server
PW_i, BIO_i	U_i 's password , biometric impression
S_p, Q_s	S_j 's secret key
$Q_s = S_p P$	S_j 's public key

TS_u, TS_s :	Timestamps
$H(.)$:	Bio-hashing function
ΔT :	Threshold for Timestamp difference
SK_{ij} :	A mutual Session Key between S_j and U_i
$ /\oplus$:	concatenation and XOR functions

Table 6.1 Notations

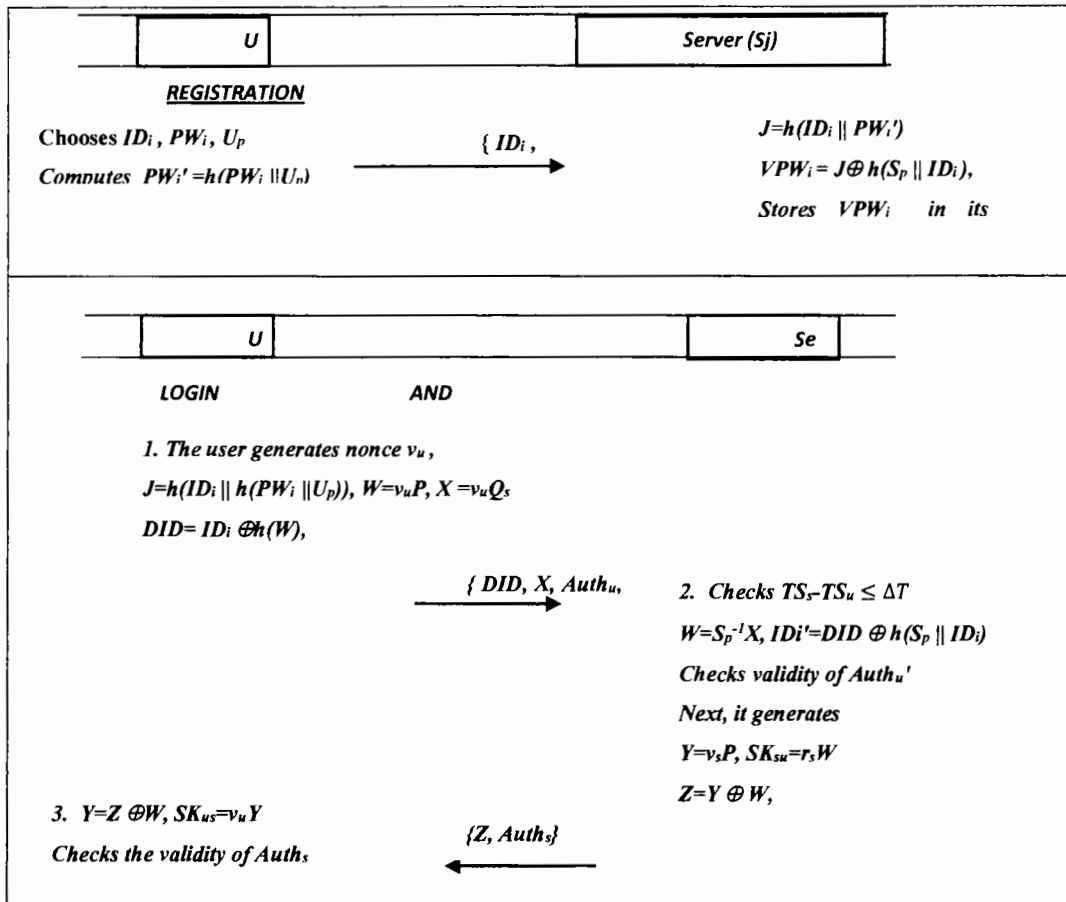


Figure 6.1. Flow of registration, login and authentication phase of Dongqing et al. model

6.3.1.1 Server Registration Phase

This scheme implies many service providers S_j , where $j=1, \dots, \psi$. S_j produces a secret key S_p and public key $Q_s = S_p P$. The S_p is held secretly, while the public key is publicly accessible by all subscribers.

6.3.1.2 User Registration Phase

During user registration phase, a user is registered from S_j initially by selecting ID_i , PW_i and U_p . To proceed, it computes $PW_i' = h(PW_i || U_p)$ and submits $\{ID_i, PW_i'\}$ to server using secret channel. Thereafter, the server computes $J = h(ID_i || PW_i')$, $VPW_i = J \oplus h(S_p || ID_i)$ and stores VPW_i in its database to conclude the registration phase.

6.3.1.3 Mutual Authentication Procedure

1. In login phase, U_i produces a nonce v_u and computes $J = h(ID_i || h(PW_i || U_p))$, $W = v_u P$, $X = v_u Q_s$, $DID = ID_i \oplus h(W)$ and $Auth_u = h(J || W || TS_u)$ and submits the login request $\{DID, X, Auth_u, TS_u\}$ to server.
2. During the phase of authentication, the server computes the timestamp and compares the difference against the threshold, i.e. $TS_s - TS_u \leq \Delta T$. If true, then it further computes $W' = S_p^{-1} X$, $ID_i' = DID \oplus h(S_p || ID_i)$ and computes $Auth_u'$ and verifies $Auth_u'$. If true, it validates the user's authenticity. Otherwise, discards the message. Further, it generates v_s and computes $Y = v_s P$, $SK_{su} = r_s W$, $Z = Y \oplus W$, $Auth_s = h(SK_{su} || J || Y || W)$ and sends the message $\{Z, Auth_s\}$ towards user.
3. The user computes $Y = Z \oplus W$, $SK_{us} = v_u Y$ and checks the validity of $Auth_s$ parameter. It discards the message if the validity is not authenticated. Otherwise, validates the server and creates the session key as $SK_{us} = SK_{su}$.

6.3.2 Weaknesses in Dongqing et al. protocol

Dongqing et al. scheme, privileged attack, DOS threat as well as session specific temporary information attacks are explored in this section. Besides, the scheme has a time synchronization problem that is difficult to implement in practical scenario. The limitations of Dongqing et al. scheme are described as below.

6.3.2.1 Privileged Insider threat

In this type of threat, a malicious insider in an organization may intercept the registration message contents and could manipulate it later for its malicious intentions. For instance, if the

adversary (insider) gets the registration message contents, the former may initiate user impersonation attack through steps taken below:

1. Having access to ID_i and $PW_i' = h(PW_i || U_p)$, the adversary may compute $J = h(ID_i || h(PW_i || U_p))$.
2. Next, it generates nonce v_a and further computes $W_a = v_a P$, $X_a = v_a Q_s$, $DID_a = ID_i \oplus h(W_a)$ and $Auth_a = h(J || W_a || TS_a)$ and sends the forged message $\{DID_a, X_a, Auth_a, TS_a\}$ to server.
3. Upon getting the message, the server computes the timestamp and compares the difference against the threshold, i.e. $TS_s - TS_a \leq \Delta T$. After finding it as true, the server further computes $W_a = S_p^{-1} X_a$, $ID_i = DID_a \oplus h(W_a)$, $J = VPW_i \oplus h(S_p || ID_i)$, and ultimately $Auth_a'$ and could verify $Auth_a'$ as positive, however fake. In this manner, an insider adversary may forge server by impersonating as a user, comfortably.

6.3.2.2 Session Specific Temporary Information threat

In this attack, if the temporary session variables are leaked to the adversary, the later could calculate the corresponding session key constructed between user and server. In Dongqing et al. scheme, if the adversary can access the temporary session variables, the former may easily plan this threat by adopting the following steps:

1. Assume, the assailant comes to know the temporary integer v_u , then it may compute $W = v_u P$ and onwards it may derive Y from Z by computing $Y = Z \oplus W$.
2. Next, the adversary may compute the shared session key SK_{us} by computing $SK_{us} = v_u Y$.

6.3.2.3 Denial of Service (DoS) Attack

In authentication protocols, where the user verifiers' database is maintained on the end of server, an adversary may exploit this feature by repeatedly submitting fake requests. An attacker may replay the message $\{DID, X, Auth_u, TS_a\}$ with adding an updated timestamp TS_a , without modifying the other parameters $DID, X, Auth_u$.

Once the messages are received, the server computes the timestamp and compares the difference against the threshold, i.e. $TS_s - TS_a \leq \Delta T$. After finding it as true, it further computes $W = S_p^{-1} X$,

$ID_i' = DID \oplus h(S_p \parallel ID_i)$ and computes $Auth_u'$. Obviously, the verification of $Auth_u'$ shall fail since the timestamp is outdated in $Auth_u$. However, the adversary becomes successful in overburdening the server for computation with fake requests. Hence, the Dongqing et al. protocol is prone to Denial-of-service threat.

6.3.2.4 Time-Synchronization Problem

The Dongqing et al.'s scheme requires a strict clock-based time synchronization for the implementation of the protocol to avoid the replay attacks, which is however, considered as unrealistic in a practical scenario. The replay attacks could be better dealt with nonce-based methods that eliminate the stricter requirement of time synchronization.

6.4. Proposed Model

Our proposed protocol is consisted of four stages. These stages include initialization stage, user registration, logic and authentication stage and password modification stage. These phase are illustrated in section 6.4.1, 6.4.2, 6.4.3, 6.4.4.

6.4.1 Initialization Phase

The proposed scheme engages the participants such as a user U_i and a trusted SIP server S_j . The user performs the registration process with S_j using a confidential channel. The S_j selects its master key S_p in this phase, that is used not only for registration purpose but also to verify the users in authentication phase. Next, it also constructs a public key $Q_s = S_p P$. The master key S_p is held secretly by the server, while its public key is publicly accessible by all subscribers.

6.4.2 Registration procedure

The registration of the user with server is performed in this procedure. The undermentioned steps are involved in the registration process.

1. U_i selects ID_i , PW_i , U_p , a_i , and imprints BIOi impression on the sensor. It then calculates $PW_i' = h(PW_i || U_p)$ and $J = h(ID_i || PW_i') \oplus h(a_i)$. Next, it sends $\{ID_i, J\}$ to the server.
2. Once the server obtained the messages it computes $Q = J \oplus h(S_p || ID_i)$ and store it in smart card and forwarded to user by adopting a secured channel.
3. The user, then computes $R = Q \oplus h(a_i)$ and replaces Q in smart card. It further computes $R_1 = h(ID_i || PW_i || U_p)$, $R_2 = H(BIO_i) \oplus U_p$ and stores R_1 and R_2 in smart card as well.

6.4.3 Mutual Authentication Procedure

1. To initiate the mutual authentication procedure for obtaining the authenticated access to S_j 's services, U_i employs its smart card. For this sake, U_i inputs its ID_i , PW_i and then imprints BIOi into the scanner device. Then smart card calculates $U_p = H(BIO_i) \oplus R_2$, $R_1' = h(ID_i || PW_i || U_p)$, and matches the equality for $R_1' = R_1$. If true, then computes $PW_i' = h(PW_i || U_p)$. It, then generates random high entropy integers v_u and n_1 and compute $h(S_p || ID_i) = h(ID_i || PW_i') \oplus R$, $W = v_u P$, $X = v_u Q_s$, $DID = ID_i \oplus h(W)$ and $Auth_u = h(h(S_p || ID_i) || W || n_1)$. In the end finally it forwards the message $\{DID, X, Auth_u, n_1\}$ to S_j for authentication.
2. Next, S_j receives parameters and computes $W = S_p^{-1} X$, $ID_i' = DID \oplus h(W)$, $Auth_u' = h(h(S_p || ID_i') || W || n_1)$, and checks the validity of $Auth_u'$. Next, it generates random integers v_s , n_2 , and compute $Y = v_s P$, $SK_{su} = h(v_s W || h(S_p || ID_i'))$, $Z = Y \oplus W$, $Auth_s = h(SK_{su} || n_1 || n_2 || Y || W)$. Now it forwards the message $\{Z, Auth_s, n_2\}$ to user. The user further verify this message.
3. U_i gets the message and computes $Y = Z \oplus W$, $SK_{us} = h(v_u Y || h(S_p || ID_i'))$ and $Auth_s = h(SK_{us} || n_1 || n_2 || Y || W)$. After that it tests whether $Auth_s$ is valid. If it holds true, then computes $Auth_{us}' = h(SK_{us} || n_1 \oplus n_2 || Y || W)$ and forwards $Auth_{us}'$ to server for confirmation.

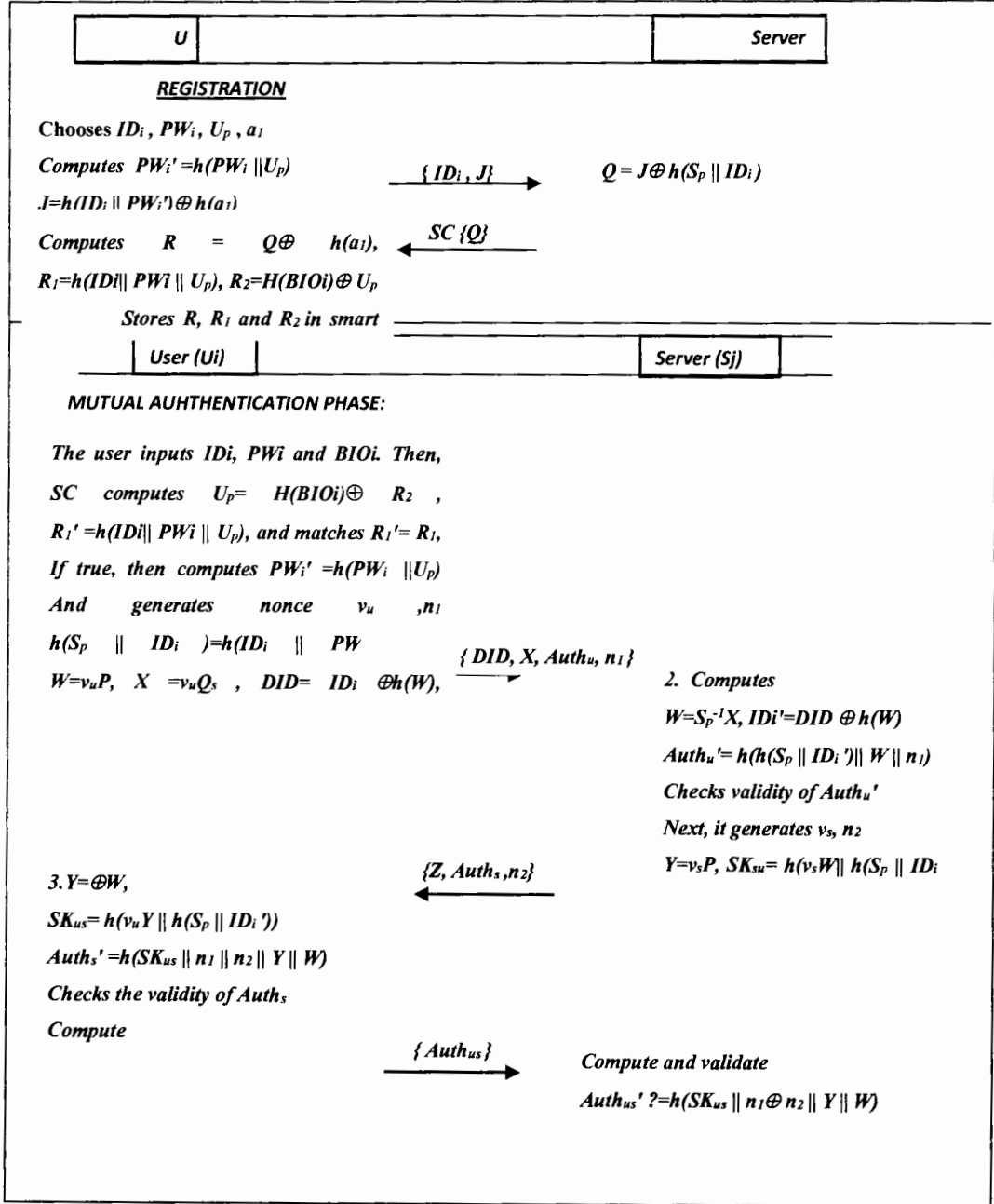


Figure 6.2 Proposed Authentication Protocol

4. S_j gets the message and calculate $Auth_{us}' = h(SK_{us} || n_1 \oplus n_2 || Y || W)$. Then, it compares the equality $Auth_{us}' ? = Auth_{us}$. If the equation is true, the user is treated as a valid user otherwise the session is terminated.

6.4.4 Password Modification Phase

Ui may update its password with a novel password i.e. PWi^{new} upon calling the specified procedure. Smart card is inserted into the scanner first and inputs the related identity, password besides imprinting the biometric factor ($BIOi^*$) in biometric scanner device.

Next, SC finds out $U_p = H(BIOi) \oplus R_2$, $R_1' = h(IDi || PWi || U_p)$, and matches the equation for $R_1' = R_1$. If true, then it permits the user to alter the password by taking the following steps:

1. The Ui computes $R_1^{new} = h(IDi || PWi^{new} || U_p)$ by employing the new password PWi^{new} .
2. Next, it calculates $h(S_p || ID_i) = h(IDi || h(PWi || U_p)) \oplus R$.
3. After deriving $h(S_p || ID_i)$ it further computes $R^{new} = h(IDi || h(PWi^{new} || U_p)) \oplus h(S_p || ID_i)$.
4. Next, it replaces the parameters R_1 and R in smart card with R_1^{new} and R^{new} .

6.5 Security Analysis

Security, automated security verification and BAN logic-oriented (form analysis) of the proposed authentication scheme has been described in the following section.

6.5.1 Security Discussion

Informal discussion regarding security of the our proposed authentication scheme has been elaborated in this section.

6.5.1.1 Replay Attacks

When an attacker repeats the catch the message content to betray any true participant such kind of attacks can launched. The adversary with open messages $\{DID, X, Auth_u, n_1, Z, Auth_s, n_2, Auth_{us}\}$ can replay those contents in order to forge the legitimate users on the both sides. By verifying $Auth_s' ?= Auth_s'$, the Ui validates Sj and removes the chances of the replay attack. $Auth_s'$ consists of n_1 parameter which is concatenated with other parameters to thwart the replay attack. In the third stage of the protocol in similar way the Sj may foil the replay threat by calculating and verifying the equation $Auth_{us}' ?= Auth_{us}$.

While computing the $Auth_{us}$, the n_2 parameter makes sure that the replay threat is defeated. In this way the proposed authentication scheme foil any kind of repaly attack.

6.5.1.2 Offline-Password Guessing Threat

This threat will be posed to the system if an attacker attempts to get either a U_i 's password upon capturing the publicly available messages $\{DID, X, Auth_u, n_1, Z, Auth_s, n_2, Auth_{us}\}$ or stealing the smart card factors $\{R, R_1, R_2\}$. In all of these factors, only R_1 is calculated with the combination of password PWi , i.e. $R_1 = h(ID_i || PWi || U_p)$. An opponent might not be able to compute a password from R_1 until it extracts the U_p factors from R_2 , which again depends upon the access of BIO_i parameter. Thus, the proposed scheme is resistant to offline-password guessing threat.

6.5.1.3 Stolen Verifier Attacks

The information stored on server's end is vulnerable and the attacker can steal valuable information. If the server has database of user-specific verifiers e.g password or any other shared secret. The adversary may use it to masquerade as legitimate user it is called stolen verifier attack.

The proposed protocol unlike Dongqing et al. protocol does not supervise any verifiers' database on the side of S_j server which is an important prerequisite for this attack.

6.5.1.4 Stolen Smart Card Threat

In this kind of attack, the attacker obtains a smart card and exploit the extracted data and launch brute force attack. By means of a stolen smart card, an adversary might attempt to exploit the recovered data. Nonetheless, as remarked in sub-section 5.1.2, The attacker is unable to guess password by stolen smart card parameters $\{R, R_1, R_2\}$. Therefore the attacker is not able to launch any type of guessing or impersonation attack despite of stealing the smart card contents as the adversary donot have BIO_i parameter information.

6.5.1.5 Session Key Security

This security characteristic advocates that the established session key must be merely in the notice of legal session members, i.e U_i or S_j .

In contributed model, the session key is produced by calculating $SK_{su} = SK_{us} = h(v_u Y || h(S_p || ID_i'))$. For generating a legitimate session key the assailant needs to access v_u and BIO_i parameters for accessing $h(S_p || ID_i')$, besides getting the smart card contents.

The high entropy integer v_u , and cannot be find out in polynomial time, and the construction of $v_u Y$ is bounded by ECDLP. Similarly, the unavailability of BIO_i parameter to the adversary leads to the protection of session key SK, and cannot be computed until the above parameters are accessed.

6.5.1.6 Known-Key Security

In know- Key Security the private keys are kept protected if the existing session key is stolen by the attacker.

In the proposed authentication schem the attacker is unable to guess usr's password PW_i or server master key S_p if the session key $SK_{su} = SK_{us} = h(v_u Y || h(S_p || ID_i'))$ is leaked by any means. Therefore the proposed scheme is well secured for the known key security.

6.5.1.7 Perfect Forward Secrecy

Perfect Forward Secrecy guarantees the confidentiality of session keys, if the high entropy private key of either U_i or a S_j has been obtained by the adversary.

The contributed protocol complies with perfect forward secrecy, notwithstanding the fact, that the long-term and high entropy secrets of participating members are exposed. That is, if the server's master key S_p is leaked, an attacker may not be able to calculate previous session keys due to missing of information of $v_u Y$ in a session key $SK_{us} = h(v_u Y || h(S_p || ID_i'))$.

6.5.1.8 Mutual Authentication

Mutual authentication feature makes sure that within the same authentication, the members must verify each other identities. The contributed authentication schem has capability to authenticate both legitimate user U_i and legitimate server S_j .

The attacker may intercept the publicly available messages $\{DID, X, Auth_u, n_1, Z, Auth_s, n_2, Auth_{us}\}$ and try to change or replay the message on both sides to deceive the true participating members. However due to the mutual authentication of U_i and S_j the probability of modification or replay threat is nullified by computing and checking the equations $Auth_{us}' = h(SK_{us} || n_1 \oplus n_2 || Y || W)$ and $Auth_s' = h(SK_{us} || n_1 || n_2 || Y || W)$. In this both the entities mutually authenticate one another.

6.5.1.9 Anonymous Authentication

The anonymous authentication ensures the anonymity feature to a subscriber during the mutual authentication phase when the subscriber communicates with S_j server. From the intercepted message contents, the attacker is unable to specify the real identities of the intercepting members. In proposed scheme, U_i submits its dynamic identity DID in the form of $DID = ID_i \oplus h(W)$ after comutation of the factor W . An attacker cannot get back the user's identity ID_i from DID , until it gets access to server's master key S_p and compute W from X . Therefore, this scheme provides sufficient anonymity to the user.

6.5.1.10 Privileged Insider threat

In the privileged inside threat, the registration request and its contents are may be intercepted by a malicious insider during the registration process.

In our proposed scheme, we used a random number a_1 to encrypt $h(ID_i || PW_i')$ parameter. As a result, the malicious insider, after encryption is unable to derive $h(ID_i || PW_i')$ from J due to that encryption. The server again encrypts the same with $h(S_p || ID_i)$ and submits the smart to user after storing the result in it. The user finally decrypts the same using a_1 and recovers the result. In

this manner, a malevolent insider may not be capable to recover any secret parameter from the registration request and hence, the proposed scheme is resilient to malicious insider attack.

6.5.1.11 Session-Specific Temporary Information(SSTI) Threat

An attacker may attempt to find the session keys if the session-specific temporary integers are disclosed. Nonetheless, unlike Dongqing et al., the proposed protocol ensures protection against this threat. Because in the suggested protocol, the session key $SK_{su} = SK_{us} = h(v_u Y || h(S_p || ID_i'))$ can be computed if the adversary succeed to access both $v_u Y$ and $h(S_p || ID_i')$ parameters. Even, if the v_u parameter is leaked to the adversary, it may compute $v_u P$, however, it may not access the other parameter, which can only be computed using BIO_i biometric value. Therefore our scheme is resilient to temporary information attack.

6.5.2 Automated Security Verification

ProVerif is one of the widely recognized automated protocol-verifier as adopted by most researchers in the current protocols. Proverif is employs applied π calculus rules in order to verify the protocols implementing encryption, hash, and Diffie-Helman operations etc. We also used this tool for testing the security strength of our proposed scheme.

We begin with the verification and testing procedure through identifying two communication channels, i.e., a private channel Sec_Ch and a public channel Pub_Ch between participants. The channels, constants and variables, constructor & de-constructor, equations, events and queries as used in the Proverif simulation of proposed model, is shown in Figure 6.2.

```

(*****Channels*****
free Sec_Ch:channel[private]. (*Secure Channel*)
free Sec_Ch:channel (*Public Channel*)
(*****Channels & Variables*****
const P:bitstring.
free IDi:bitstring.
free PWi:bitstring[private].
free a1:bitstring[private].
Free Up: bitstring[private].
Free SP: bitstring[private].
Free BIOi: bitstring[private].
(*****Constructor*****
fun h(bistring):bistring
fun XOR(bitstring,bitrstring):bitstring.
fun CONCAT(bitstring,bitrstring):bitstring.
fun ECPM(bitstring,bitrstring):bitstring.
fun INVERSE(bitstrin):bitstring.
(***** Destructive & Equation*****
equation forall a.bitstring,b.string XOR(XOR a,b),b)=a
equation forall c.bitstring,b.string INVERSE(INVERSE(c))=c
(*****Events*****
event_begin_User_U(bitstring)
event_end_User_U(bitstring)
event_begin_Server_S(bitstring)
event_end_Server_S(bitstring)
(*****Queries*****
free SK:bitstring[Private]
query attacker(SK)
query id.bitstring;inj-event(End_User_U(id)==>inj-event(Begin_User_U(id)

```

query id.bitstring;inj-event(End_Server_U(id)==>inj-event(Begin_Server_S(id)

Figure 6.3. Channels, constructor, destructor, events and equations

```

(*****User Ui*****)
let User I=
(*****Registration*****)
new a1:bitstring;
new UP:bitstring
let PWi'=h(CONCAT(PWi,Up))In
let J=XOR(h(CONCAT(IDi,PWi')),h(a1))in
out=(Sec_Ch,(IDi,J));
in(Sec_Ch,(xQ:(bitstring);
let R=XOR(Q,h(a1))in
let R1=h(CONCAT(IDi, PWi,Up))in
let R2=XOR(BIOi),Up in
(*****Login and Authentication*****
Event begin_User_U(IDi);
let Up=XOR(H(BIOi),R2)in
let R1'=h(CONCAT(IDi,PWi,Up))in
New vu=bitstring;
New N1=bitstring;
let h(CONTACT(SP,IDi)=XOR(h(CONCAT(IDi,PWi')),R in
let W=ECPM(vu,P)in
let X=ECPM(vu,Qs)in
let DID=XOR(IDi,h(W))in
let Authu=h(CONCAT(h(Sp, IDi)W,n1))n1
Out=(Pub_CH)(DID,X,Authu,n1);
In(Pub_Ch)(xZ:bitstring,xAuthus:bitstring, xn2: bitstring))
let y=XOR(xZ,W)in
let SKus=h(CONCAT(ECPM)(vu,Y),h(CONCAT(Sp,IDi'))in
let Auths'=h(CONCAT(SKus,n1,n2,Y,W))in

```

```

If Auths'=Auths then
let Authus=h(CONCAT,SKus, XOR(n1,n2),Y,W)in
Out(Pub_ch(Auths))
Event End_User(IDi)
Else
0

```

Figure 6.4: UserUi process

The two events have been modeled between user and server. The initiating and ending event for the user are `begin_User_U(bitstring)` and `End_User_U(bitstring)`. Similarly, these events for the server are `Begin_Server_S(bitstring)` and `End_Server_S(bitstring)`. We have described two separate procedures, i.e., `User_U` and `Server_S` for modelling user and server processes, respectively. The process `User_U` submits the calculated parameters `IDi`, `PWi'`, `Up`, `a1` using secure channel `Sec_Ch` towards `Server_S`. Then, after getting the registration request, the `User_U` process further computes `Q` and forwards to user. The user computes `R1`, `R2` and stores in smart card. In mutual authentication procedure, the `User_U` process compares `Ri` and `Ri'` after calculating `Ri'`. It further produces `PWi'`, `W`, `X`, `DID` and `Authu`. Then, it submits `{DID, X, Authu, n1}` towards `Server_S` using `Pub_Ch`. Next, it receives `{xZ, xAuths, xn2}` from `Server_S`. It calculates `Y`, `SKus`, `Auths'` and compares `Auths` and `Auths'`. Finally, it submits `Authus` towards `Server_S` for verification, and proceeds for calculating the session key `SK` as shown in Fig. 4. Likewise, the `Server_S` process receives `xIDi`, `xJ` from `User_U` process as registration request. Next, it computes `Q` and submits to `User_U` utilizing secure channel `Sec_Ch`. In mutual authentication phase, the `Server_S` process receives `{xDID, xX, xauthu, xn1}` and computes `W`, `IDi'`, `Authu'` and compares `Authu'` with `Authu`. If positive, then computes `Y`, `SKsu`, `Z` and `Auths` and submits `{Z, Auths, n2}` to `User_U` using `Pub_Ch`. Further, it receives `xAuthus` from the same process, and computes `Authus'`. Next, it validates the user on matching the two parameters `Authus'` and `xAuthus`. Otherwise, it aborts the protocol, as shown in Figure 6.5.

```

(*****Server(Sj)*****)
let Server_S=
(*****Registration*****)
In(Sec_Ch,(xIDi:bitstring,Xj:bitstring));

```

```

Let Q=XOR(J,h(CONCAT(Sp,IDI)))in
Out(Sec_Ch(Q));
(*****Login and Authentication*****)
Event Begin_Server_S(Qs);
In(Pub_Ch,(Xdid:bitstring,xX:bitstring, xAuthu:bitstring,xn1:bitstring));
let W=MULT(INVERSE(Sp,xX)in
Let IDi'=XOR(xDID,h(W)in
Let Authu'=h(CONCAT(h(CONCAT)(Sp,IDI'),W,xn1))in
If(Aut'=xAuthu) then
New vs:bitstring;
New n2:bitstring;
let Y=ECMP(Vs,P)in
let Y=ECMP(vs,P) in
let SKsu=h(CONCAT(ECMP(vs,W),h(CONCAT(Sp,IDI')))) in
let Z=XOR(Y,W)in
let Auths=h(CONCAT(SKsu,xn1,n2,Y,W)in
out(Pub_Ch,(Z,Auths,n2));
in(Pub_Ch,(x,Authus,bitstring);
let Authu'=h(CONCAT(SKus,XOR(xn1,n2),Y,W))in
if Authu's=xAuthus then
event End_Server_S(Qs)
else
0

```

Figure 6.5. ServerSj process

The two participants may interact for an unbounded number of sessions, so these two processes are considered to be in replication as illustrated below.

process
 ((!User_U) | (!Server_S))

We have the following findings after applying queries for this simulation.

RESULT inj-event(End_Server_S(id)) \implies inj-event(Begin_Server_S(id)) is true. (1)

RESULT inj-event(End_User_U(id_1683)) \implies inj-event(begin_User_U(id_1683)) is true.(2)

RESULT not attacker(SK[]) is true. (3)

The results from Eq. (1) and Eq. (2) depict that both processes initiated and terminated successfully, while the result in Eq. (3) suggests that the attacker query could not expose the session key as constructed between the processes in mutual authentication procedure.

6.5.3 Formal Security Analysis (BAN Logic)

Security analysis employing Burrows-Abadi-Needham logic(BAN) logic and random oracle model(ROM) has been carried out in this section.

The BAN logic defines and analyzes the security features involving mutual authentication and the incapability of computing session key. Key terms and notations used in the proposed scheme in applying the BAN logic is as under.

Principals means the the active participating agents in our proposed protocol.

Keys are meant for symmetric encryption.

Nonces are non-repeatable portions of the message.

Following are further important notations which are used in analysis of BAN logic.

$\Phi \models Y$: Φ believes Y .

$\Phi \triangleleft Y$: Φ sees Y .

$\Phi \mid \sim Y$: Φ once said Y .

$\Phi \Rightarrow Y$: Φ has got jurisdiction over Y ;

$\#(Y)$: The message Y may be treated as fresh.

$(Y)Z$: The formulae Y is used in combination with formulae Z .

(Y, Z) : Y or Z represent a component of the message (Y, Z) .

$(Y, Z)_K$: Y or Z is encrypted with the key K .

$\Phi \xrightarrow{K} \Phi'$: Φ and Φ' may secretly contact through shared key K .

$\langle Y, Z \rangle_K$: Y or Z is hashed with key K .

Some of the logical rules are employed in this proof as listed below:

- R1*: Message meaning rule: $\frac{\Phi \equiv \Phi \xleftrightarrow{K} \Phi', \Phi \triangleleft (Y)_Z}{\Phi \equiv \Phi' \mid \sim Y}$
- R2*: Nonce verification rule: $\frac{\Phi \equiv \#(Y), \Phi \equiv \Phi' \mid \sim Y}{\Phi \equiv \Phi' \mid \equiv Y}$
- R3*: Jurisdiction rule: $\frac{\Phi \equiv \Phi' \Rightarrow Y, \Phi \equiv \Phi' \mid \equiv Y}{\Phi \equiv Y}$
- R4*: Freshness conjunction rule: $\frac{\Phi \equiv \#(Y)}{\Phi \equiv \#(Y, Z)}$
- R5*: Belief rule: $\frac{\Phi \equiv (Y), \Phi \equiv (Z)}{\Phi \equiv (Y, Z)}$
- R6*: Session keys rule: $\frac{\Phi \equiv \#(Y), \Phi \equiv \Phi' \mid \equiv Y}{\Phi \equiv \Phi \xleftrightarrow{K} \Phi'}$

By applying the BAN logic, our proposed scheme must achieve the understated goals to support the security features.

- G1 : $S_j \mid \equiv U_i \xleftrightarrow{SK_{su}} S_j$
- G2 : $S_j \mid \equiv U_i \mid \equiv U_i \xleftrightarrow{SK_{su}} S_j$
- G3 : $U_i \mid \equiv U_i \xleftrightarrow{SK_{us}} S_j$
- G4 : $U_i \mid \equiv S_j \mid \equiv U_i \xleftrightarrow{SK_{us}} S_j$

First, we convert the communicated message contents into idealized form as shown underneath:

- $M_1: U_i \rightarrow S_j: DID, X, Auth_u, n_1: \{ \langle ID_i \rangle_{h(W)}, v_u Q_s, \langle h(S_p \parallel ID_i), n_1 \rangle_W, n_1 \}$
- $M_2: S_j \rightarrow U_i: Z, Auth_s, n_2: \{ Z, \langle h(v_s v_u P \parallel h(S_p \parallel ID_i')), n_1, n_2 \rangle_{Y, W}, n_2 \}$
- $M_3: U_i \rightarrow S_j: Auth_{us}: \langle h(v_u v_s P \parallel h(S_p \parallel ID_i')), n_1 \oplus n_2 \rangle_{Y, W} \}$

Secondly, to prove the security of the proposed work following assumptions have been developed.

- §1 : $U_i \mid \equiv \# n_1$
- §2 : $S_j \mid \equiv \# n_2$
- §3 : $U_i \mid \equiv S_j \xleftrightarrow{(SK_{us}, W, Y)} U_i$
- §4 : $S_j \mid \equiv S_j \xleftrightarrow{(SK_{su}, W, Y)} U_i$
- §5 : $U_i \mid \equiv S_j \mid \equiv U_i \xleftrightarrow{(SK_{us}, W, Y)} S_j$
- §6 : $S_j \mid \equiv U_i \mid \equiv U_i \xleftrightarrow{(SK_{su}, W, Y)} S_j$

$$\S7 : U_i \models S_j \Rightarrow v_s P$$

$$\S8 : S_j \models U_i \Rightarrow v_u P$$

Next, the produced idealized forms i.e M_1 , M_2 and M_3 of our proposed protocol we can be evaluate the above mentioned postulates.

Following derivations are obtained by the above notations, idealization and the premises.

Considering the idealized forms, i.e. M_1 and M_3 :

$$M_1: U_i \rightarrow S_j: DID, X, Auth_u, n_1: \{ \langle ID_i \rangle_{h(W)}, v_u Q_s, \langle h(S_p \parallel ID_i), n_1 \rangle_W, n_1 \}$$

$$M_3: U_i \rightarrow S_j: Auth_{us}: \langle h(v_u v_s P \parallel h(S_p \parallel ID_i')), n_1 \oplus n_2 \rangle_{Y, W} \}$$

By applying the seeing rule, we have

$$Q1: S_j \triangleleft DID, X, Auth_u, n_1: \{ \langle ID_i \rangle_{h(W)}, v_u Q_s, \langle h(S_p \parallel ID_i), n_1 \rangle_W, n_1 \}$$

$$Q2: S_j \triangleleft Auth_{us}: \langle h(v_u v_s P \parallel h(S_p \parallel ID_i')), n_1 \oplus n_2 \rangle_{Y, W} \}$$

Now using Q1, Q2, §3 and R1, we say

$$Q3: S_j \models U_i \sim \{ \langle ID_i \rangle_{h(W)}, v_u Q_s, \langle h(S_p \parallel ID_i), n_1 \rangle_W, n_1 \}$$

$$Q4: S_j \models U_i \sim \langle h(v_u v_s P \parallel h(S_p \parallel ID_i')), n_1 \oplus n_2 \rangle_{Y, W} \}$$

Referring Q3, Q4, §1, R4 and R2, we say

$$Q5: S_j \models U_i \models \{ \langle ID_i \rangle_{h(W)}, v_u Q_s, \langle h(S_p \parallel ID_i), n_1 \rangle_W, n_1 \}$$

$$Q6: S \models U_i \models \langle h(v_u v_s P \parallel h(S_p \parallel ID_i')), n_1 \oplus n_2 \rangle_{Y, W} \}$$

Referring Q5, Q6, §4, §8 and R3, we get

$$Q7: S_j \models \{ \langle ID_i \rangle_{h(W)}, v_u Q_s, \langle h(S_p \parallel ID_i), n_1 \rangle_W, n_1 \}$$

$$Q8: S_j \models \langle h(v_u v_s P \parallel h(S_p \parallel ID_i')), n_1 \oplus n_2 \rangle_{Y, W} \}$$

Using Q7, Q8, §4, ($SK_{su} = SK_{us} = h(v_u Y \parallel h(S_p \parallel ID_i'))$) and R6, we get

$$Q9: S_j \models U_i \xleftrightarrow{SK_{su}} S_j \quad (G1)$$

According to Q9, §6 we apply R6 as

$$Q10: S_j \models U_i \models U_i \xleftrightarrow{SK_{su}} S_j \quad (G2)$$

Next, again evaluating the idealized form M_2 :

$$M_2: S_j \rightarrow U_i: Z, Auth_s, n_2: \{ Z, \langle h(v_s v_u P \parallel h(S_p \parallel ID_i')), n_1, n_2 \rangle_{Y, W}, n_2 \}$$

By applying seeing rule, we get

$$Q11: U_i \triangleleft Z, Auth_s, n_2: \{ Z, \langle h(v_s v_u P \parallel h(S_p \parallel ID_i')), n_1, n_2 \rangle_{Y, W}, n_2 \}$$

According to Q11, §4 and R1, we can say

$$Q12: U_i \models S_j \sim \{Z, \langle h(v_s v_u P \parallel h(S_p \parallel ID_i')), n_1, n_2 \rangle_{Y, W, n_2}\}$$

Using Q12, §2, *R4* and *R2*, we say

$$Q13: U_i \models S_j \models \{Z, \langle h(v_s v_u P \parallel h(S_p \parallel ID_i')), n_1, n_2 \rangle_{Y, W, n_2}\}$$

Referring Q13, §3, §7 and *R3*, we get

$$Q14: U_i \models \{Z, \langle h(v_s v_u P \parallel h(S_p \parallel ID_i')), n_1, n_2 \rangle_{Y, W, n_2}\}$$

From Q14, §3, ($SK_{su} = SK_{us} = h(v_u Y \parallel h(S_p \parallel ID_i'))$), and *R6*, we get

$$Q15: U_i \models U_i \xleftrightarrow{SK_{us}} S_j \quad (G3)$$

According to Q15, §5, we apply *R6* as

$$Q16: U_i \models S_j \models U_i \xleftrightarrow{SK_{us}} S_j \quad (G4)$$

The presented analysis of BAN logic formally verifies that our contributed scheme makes sure mutual authentication while the constructed session key (*SK*) is agreed and shared mutually between the participants (*Sj* and *Ui*).

6. 6. Performance Evaluation Analysis

In this section, we evaluate and compare the security of the contributed protocol with Dongqing et al.'s SIP authentication scheme and other contemporary schemes. Table 6.2 depicts the comparison of different protocols for vulnerability to threats, which indicates the proposed scheme as a robust authentication scheme against Dongqing et al. The comparison in Table 6.2 comprises Dongqing et al.[127], Chaudhary et al.[106], Zhang et al. [128] and our introduced scheme, which indicates that this scheme shows more resistance to attacks than its contemporary schemes. Although the scheme bears a little extra cost in comparison with [106, 127-128] schemes, however it is resilient against many threats such as replay threat, offline-password guessing threat, privileged insider threat, denial of service threat, session specific temporary information threat, and session key attack. The extra cost of proposed scheme is in terms of few more hash operations, that does not adds much to the cost, however the proposed scheme becomes resilient to attacks as posed to earlier schemes.

For the purpose of the evaluation of computational costs given in Table III, we represent one-way hash function with T_H and elliptic scalar point multiplication T_{ESM} , and lightweight XOR function is negligible cost. The delay for T_H and T_{ESM} are reported in[136] as 0.0023 ms and 2.226 ms respectively. The computational cost of Zhang et al., Chaudhary et al., Dongqing et al.'

scheme and proposed scheme amounts to $10T_H + 6T_{ESM}$, $7T_H + 6T_{ESM}$, $9T_H + 6T_{ESM}$ and $13T_H + 6T_{ESM}$ with computational delays amounting to 13.379ms, 13.372ms, 13.376ms, 13.859ms, respectively. Most of these protocols utilize 6 scalar point multiplications, but the number of hash operations varies. Although, there is little difference in computational cost of these protocols, however the resistance to attacks varies with each protocol. For instance, the proposed scheme resists all threats, while Dongqing et al.'s protocol is prone to privileged insider threat and session-specific temporary information threat. The Chaudhary et al.'s protocol is found to be susceptible for session key attack, and Zhang et al. does not offer anonymity feature to user, and is also prone to impersonation attack.

The scalar point operation could be the decisive factor for measuring the efficiency of a protocol. The Lin et al. takes 4 T_{ESM} operations, while the proposed scheme takes 6 T_{ESM} operations. Although, Lin et al. takes two less point multiplication operations as compared to proposed scheme, however, the later is resistant to many attacks that Lin et al. scheme doesn't. Thus, according to the performance analysis shown in Table II and III, we can say the proposed scheme is a more resilient authentication scheme as compared to Lin et al., with a bit added computational cost than its counterpart.

	Zhang et al. [128]	Chaudhary et al. [106]	Dongqing et al. [127]	Ours
Anonymity	×	√	√	√
Resist privileged insider threat	√	√	×	√
Mutual Authentication	√	√	√	√
Resist Stolen smart card threat	√	√	√	√
Resist Replay attack	√	√	√	√
Resist Offline password guessing threat	√	√	√	√
Resist session specific temporary information threat	√	√	×	√
Resist user impersonation threat	×	√	√	√
Resistant to Session key threat	×	×	√	√
Resist Denial-of-service threat	√	√	×	√

No strict time synchronization required	√	√	×	√
Perfect forward secrecy	√	√	√	√

Table 6.2: Comparison for Multi-server schemes

	Zhang al. [128]	et et [106]	Chaudhary al. [106]	Dongqing et [127]	Ours al.
Authentication messages	$10T_H$ $6T_{ESM}$	+	$7T_H$	$6T_{ESM}$ $9T_H$	$6T_{ESM}$ $13T_H$
Delay (ms)	13.379		13.372	13.376	13.3859

Table 6.3: Computational comparison

6.7.Summary

The SIP protocol provides IMS structural framework the basis for the maintenance of voice and multimedia based sessions. Recently, Dongqing et al. discovered limitations in Lu et al. and Chaudhary et al.’s SIP authentication protocols, and demonstrated an improved SIP authentication protocol. In this work, we elaborated that Dongqing et al.’s scheme is still vulnerable to privileged insider attack, Denial of Service (DoS) attack, and session specific temporary information attacks, other than a limitation of time synchronization. Thus, to counter the limitations in Dongqing et al., we propose an improved SIP authentication scheme which is formally proved as secure using BAN logic analysis in the previous sections. The comparative analysis of proposed and contemporary schemes depicts the supremacy of proposed scheme in terms of security and efficiency.

7. Conclusion and Future Work

7.1 Contribution

In this thesis, research work on enhancing QoS and security in IP Multimedia Subsystem (IMS) using virtual machines has been presented. Following contributions are made in research in this thesis.

At first, basics of the IMS e.g architectural requirements of IP Multimedia Subsystem, IP Multimedia Subsystem entities and their functionalities, databases, service functions, registration etc has been described. Then quality mechanism, quality of service protocols, policy-based QoS architectures, Quality of Service management, QoS attributes related to policy decision point etc has been described. Then concept of cloud computing has been explained in detail. Cloud computing has emerged as a result of the research on different computing paradigm e.g storage elasticity, pay per use on demand, grid computing and distributed computing. Characteristics of cloud computing, service models, virtualization has been described.

Virtual concept is used in the cloud computing. In this concept one or more virtual machines can be run on a single computer. By using this technique, memory, storage resources and processors can be utilized in optimal manner and has also evolved energy efficient computing resources.

Then concept of virtual IMS client has been described in details. Virtual IMS client architecture and details of QoS and virtual IMS Client have been explained. In the proposed system a server known as surrogate presented in[5] is used. The surrogate performs the role of the virtual server and it offers the SIP based accessibility to the users.

In the previous models single web server was used for better work load balancing the number of servers with shared memory has been introduced. The user equipment interacts with the surrogate using HTTP and the surrogate interacts with the IMS core network through SIP protocol. In the proposed architecture three virtualized IMS machines with shared memory has been used.

OpenIMS was installed on Ubuntu 14.4 LTS operating system along with DNS Server (BIND-9.3.2), a Web Server (Apache2, MySql Server, Wireshark Network Protocol Analyzer and SIPp Traffic generator tool. The process delay in OpenIMS, Post Dial Delay results were obtained

from simulation which shows remarkable improvement in the proposed model. Test was also conducted to measure the % CPU utilization of Call Session Control Functions Servers i.e P-CSCF, I-CSCF and S-CSCF and Home Subscriber Server. The graphs shows that the besides scalable platform, reduction in session setup delay and use of light weight user equipment the percentage utilization of the the servers has increased which shows the system performs more better. The results also shows that the HSS uses highest utilization of the CPU due to the part it plays in the process of registration. Further it has been find out that the overall workload management has been improved in all scenorios.

The IP Multimedia Subsystem uses SIP protocol to establish voice and multimedia based sessions. Dongqing et al. discovered limitations in Lu et al. and Chaudhary et al.'s SIP authentication protocols, and suggested an improved SIP authentication protocol. In this thesis, we have proved that Dongqing et al.'s scheme is still prone to privileged insider attack, Denial of Service attack, and session specific temporary information attacks. The Dongqing et al.'s authentication scheme has also the limitation of time synchronization. In order to overcome the limitations in Dongqing et al., we proposed an improved SIP authentication scheme. This scheme is formally proved as secure using BAN logic analysis. In terms of the security and efficiency, the comparative analysis of the proposed and contemporary schemes has been done which shows the supremacy of the proposed scheme.

7.2 Future Work

In future, bandwidth requirement for the signaling messages, various scenarios usage, delay in session establishment loss models can be considered for future research. Further traffic models ensuring quality of service while implementing virtual machines needs to be explored. Besides, the traffic congestion in peak timings can seriously undermine the overall performance of the system, thus there is also scope to examine the effects of different overloaded servers e.g Web Servers, Application Servers etc. As for SIP security is concerned our future work lies with the detection of malformed messages in SIP environment, and reducing the SIP flooding as well as distributed DoS attacks. Besides, the SIP authentication protocol may be further optimized to reduce the number of costly crypto-primitives in the authentication protocol which can reduce the impact of DoS threats as well as realize the cost-effective signaling.

Refereces

- [1] Zoric, S., Barakovic, J., & Hodzic, H., ("). QoS architecture in IP multimedia subsystem of UMTS," *International Symposium ELMAR*, vol. 1, no. IEEE, pp. 253–256, Sep. 2008.
- [2] "3rd Generation Partnership Project," *Multimedia Tools and Applications*, vol. V11.4, p. 3GPP TS 23.228, Oct. 2012.
- [3] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., ... & Schooler, E, "SIP: session initiation protocol," *RFC3261*, 2002.
- [4] "3rd Generation Partnership Project," in *Technical Specification Group Services and System Aspects; Policy and charging control architecture*, 2012, vol. V11.5.0, p. 3GPP TS 23.203.
- [5] Islam, S., & Grégoire, J. C., "Policy and Charging Control for Virtual IMS Client," *Journal of network and systems management*, pp. 22(4), 609-628., 2014.
- [6] Poikselkä, M., Niemi, A., Khartabil, H., & Mayer, G., *The IMS: IP Multimedia Concepts and Services John Wiley & Sons.*, 2007.
- [7] Psimogiannos, N., Sgora, A., & Vergados, D. D., "An IMS-based network architecture for WiMAX-UMTS and WiMAX-WLAN interworking. Computer Communications," pp. 34(9), 1077-1099., 2011.
- [8] Chen, J. L., Wuy, S. L., Larosa, Y. T., Yang, P. J., & Li, Y. F., "IMS cloud computing architecture for high-quality multimedia applications," in *7th International Wireless Communications and Mobile Computing Conference*, 2011, pp. 1463–1468.
- [9] "3rd Generation Partnership Project," *Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging*, vol. V11.3.0, p. 3GPP TS 32.260, 2012.
- [10] Cai, Y., & Liu, C. Z., "Online Charging for Roaming Users in a Proxy Online Charging System of a Visited Network U.S," Patent No. 8,175,575, 2012.
- [11] "3rd Generation Partnership Project," *Policy and Charging Control (PCC) over Gx/Sd reference point.*, vol. V11.4.0, p. . 3GPP TS 29.212, 2012.
- [12] "3rd Generation Partnership Project," *(Service requirements for the Internet Protocol (IP) multimedia core network subsystem*, p. TS 22.228, 2004.
- [13] J. W. & Sons., "IP Multimedia Concepts and Services," *The IMS: IP Multimedia Concepts and Services John Wiley & Sons.*, 2006.
- [14] "3rd Generation Partnership Project," *IP Multimedia Subsystem (IMS).*, p. 3GPP TS 23.228.

- [15] "3rd Generation Partnership Project," *Technical Specification Group Core Network; Numbering, addressing and Identification.*, p. 3GPP TS 23.003, 2005.
- [16] "3rd Generation Partnership Project," *Characteristics of the USIM application*, p. 3GPP TS 31.102, 2016.
- [17] "3rd Generation Partnership Project," *Service principles*, p. 3GPP TS 22.101, 2009.
- [18] "3rd Generation Partnership Project," *USIM and IC card requirements*, p. 3GPP TS 21.111, 2006.
- [19] K. I. Lakhtaria, "Enhancing QoS and QOE in IMS enabled next generation networks, Int. J. Appl. graph theory Wireless ad hoc networks Sensor networks," p. 2(2) 61-71., 2010.
- [20] Truong, T. H., Nguyen, T. H., & Nguyen, H. T., "On relationship between quality of experience and quality of service metrics for IMS-Based IPTV networks," in *IEEE RIVF International Conference on Computing & Communication Technologies, Research, Innovation, and Vision for the Future*, 2012, pp. 1–6.
- [21] "Deploying QoS for Cisco IP and next generation networks: the definitive guide," *Morgan Kaufmann.*, 2009.
- [22] D. de T. R. a. la C. De servicio, "UIT-T, Recomendación UIT-T E.800," 2008.
- [23] Raouyane, B., Bellafkih, M., & Ranc, D., "QoS management in IMS: DiffServ model," in *Third International Conference on Next Generation Mobile Applications, Services and Technologies*, 2009, pp. 39–43.
- [24] Evans, J. W., & Filisfilis, C., "Deploying IP and MPLS QoS for Multiservice Networks," *Theory & Practice. Elsevier*, 2007.
- [25] Ageal, M., Good, R., Elmangosh, A., Ashibani, M., Ventura, N., & Ben-Shatwan, F., "Centralized policy provisioning for inter-domain IMS QoS," In *IEEE EUROCON*, no. IEEE, pp. 1793–1797, 2009.
- [26] Siddiqui, M. S., Shaikh, R. A., & Hong, C. S., "QoS control in service delivery in IMS," *11th International Conference on Advanced Communication Technology*, vol. 1, no. IEEE, p. pp. 157–160, 2009.
- [27] Raouyane, B., Bellafkih, M., Ranc, D., & Ramdani, M., "INQA: management project of QoS in an architecture IMS," *International Conference on Multimedia Computing and Systems*, no. IEEE, pp. 366–371, 2009.
- [28] Sarmiento, D. A. L., Segura, D. A., & González, F. J., "Comportamiento de los servicios diferenciados (DiffServ)," y los servicios integrados (IntServ) en redes IP pequeñas. *Redes de Ingeniería*, p. 2(1), 4-18, 2011.
- [29] Wisely, D. (2009). IP for 4G. John Wiley & Sons

-
- [30] Yavatkar, R., Pendarakis, D., & Guerin, R, "A framework for policy-based admission control," p. Rfc2753, 2000.
 - [31] Egger, C., Happenhofer, M., Fabini, J., & Reichl, P., "BIQINI—A Flow-based QoS Enforcement Architecture for NGN Services," in *International Conference on Testbeds and Research Infrastructures*, 2010, pp. 653–667.
 - [32] "3rd Generation Partnership Project," *Quality of Service (QoS) Concept and Architecture.*, p. 3GPP TS 23.107.
 - [33] 3rd Generation Partnership Project (2015) End-to-end Quality of Service (QoS) concept and architecture 3GPP TS 23.207,2015
 - [34] G. Pallis, "Cloud computing: the new frontier of internet computing," *IEEE internet computing*, pp. 14(5), 70-73.
 - [35] Peng, J., Zhang, X., Lei, Z., Zhang, B., Zhang, W., & Li, Q., "Comparison of several cloud computing platforms," in *Second international symposium on information science and engineering*, 2009, pp. 23–27.
 - [36] X. Xu, "From cloud computing to cloud manufacturing. Robotics and computer-integrated manufacturing," p. 28(1), 75-86., 2012
 - [37] N. Kshetri, "Cloud computing in developing economies. Computer," pp. 43(10), 47–55, 2010.
 - [38] "The NIST definition of cloud computing (NIST special publication 800-145)," *National Institute of Standards and Technology, Tech. Rep.*, 2011.
 - [39] Lei, X., Zhe, X., Shaowu, M., & Xiongyan, T., "Cloud computing and services platform construction of telecom operator," in *2nd IEEE International Conference on Broadband Network & Multimedia Technology*, pp. 864–867.
 - [40] Chen, X., Wills, G., Gilbert, L., & Bacigalupo, D, "Using cloud for research: A technical review," Available: <http://eprints.soton.ac.uk>, p. 271273/, 2010.
 - [41] Mollah, M. B., Islam, K. R., & Islam, S. S., "Next generation of computing through cloud computing technology," in *25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, 2012, pp. 1–6.
 - [42] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M., "A view of cloud computing. Communications of the ACM," pp. 53(4), 50–58, 2010.
 - [43] Gregoire, J. C., Islam, S., Prasad, A., Buford, F., & Gurbani, V., "Virtual terminals for IMS. Future Internet Services and Service Architectures," pp. 15, 295., 2011.
 - [44] W. W. Lu, "Fourth-generation mobile initiatives and technologies," *IEEE Communications Magazine*, pp. 40(3), 104-105., 2002.

- [45] Fodor, G., Eriksson, A., & Tuoriniemi, A., "Providing quality of service in always best connected networks," *IEEE Communications Magazine*, , pp. 41(7), 154-163., 2003.
- [46] Balbás, J. J. P., Rommer, S., & Stenfelt, J., "Policy and charging control in the evolved packet system," *IEEE Communications Magazine*, p. 47(2), 68-74., 2009.
- [47] A. A. D. de Gouveia F. C. Corici M. I. & Magedanz T., "The PCC rule in the 3GPP IMS policy and charging control architecture," in *IEEE Globecom 2008-2008 IEEE Global Telecommunications Conference*, 2008, pp. 1–5.
- [48] "3rd Generation Partnership Project," *GPRS enhancements for EUTRAN access.*, pp. 3GPP, TS 23.401, 2008.
- [49] "3rd Generation Partnership Project," *Architecture Enhancements for Non-3GPP Accesses.*, p. 3GPP TS 23.402, 2013.
- [50] Zhuang, W., Gan, Y. S., Loh, K. J., & Chua, K. C, "). Policy-based QoS-management architecture in an integrated UMTS and WLAN environment," *IEEE Communications Magazine*, pp. 41(11), 118-125., 2003.
- [51] Marocco, E., Manzalini, A., Sampò, M., & Canal, G., "Interworking between P2PSIP overlays and IMS networks—scenarios and technical solutions," in *In Proceedings of the International Conference on Intelligence in Service Delivery Networks*, 2007.
- [52] T. Bessis, "Improving performance and reliability of an IMS network by co-locating IMS servers. Bell Labs," *Improving performance and reliability of an IMS network by co-locating IMS servers. Bell Labs Technical Journal*, pp. 10(4), 167-178., 2006.
- [53] Fabini, J., Jordan, N., Reichl, P., Poropatich, A., & Huber, R, "' IMS in a Bottle': Initial Experiences from an OpenSER-based Prototype Implementation of the 3GPP IP Multimedia Subsystem," in *International Conference on Mobile Business*, 2006, pp. 13–13.
- [54] Matuszewski, M., & Garcia-Martin, M. A., "A distributed IP multimedia subsystem (IMS)," in *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, 2007, pp. 1–8.
- [55] Dutta, A., Makaya, C., Das, S., Chee, D., Lin, J., Komorita, S., ... & Schulzrinne, H, "Self organizing IP multimedia subsystem," in *IEEE International Conference on Internet Multimedia Services Architecture and Applications (IMSAA)*, 2007, pp. 1–6
- [56] Hasswa, A., Taha, A. E., & Hassanein, H., "On extending IMS services to WLANs," in *32nd IEEE Conference on Local Computer Networks (LCN 2007)*, 2007, pp. 931–938.
- [57] Munasinghe, K. S., & Jamalipour, A., "A 3GPP-IMS based approach for converging next generation mobile data networks," in *2007 IEEE International Conference on Communications*, 2007, pp. 5264–5269.

- [58] Munasinghe, K. S., & Jamalipour, A., "Interworking of WLAN-UMTS networks: an IMS-based platform for session mobility," *IEEE communications magazine*, pp. 46(9), 184–191, 2008.
- [59] Munir, A., & Wong, V. W., "Interworking architectures for IP multimedia subsystems," *Mobile Networks and Applications*, pp. 12(5–6), 296–308, 2007.
- [60] Udugama, A., Kuladinithi, K., Görg, C., Pittmann, F., & Tionardi, L., "NetCAPE: Enabling seamless IMS service delivery across heterogeneous mobile networks," *IEEE Communications Magazine*, pp. 45(7), 84–91., 2007.
- [61] Dutta, A., Manousakis, K., Das, S., Lin, F. J., Chiba, T., Yokota, H., ... & Schulzrinne, H., "Mobility Testbed for 3GPP2-based multimedia domain networks," *IEEE Communications Magazine*, pp. 5(7), 118–126, 2007.
- [62] Lee, Y., Kang, N., Ko, S., & Kim, Y., "An efficient QoS control mechanism for IMS based convergence network," in *2nd IEEE/IFIP International Workshop on Broadband Convergence Networks*, 2007, pp. 1–12.
- [63] Vallejo, A., Zaballos, A., Canaleta, X., & Dalmau, J., "End-to-end QoS management proposal for the ITU-T IMS/NGN architecture," in *16th International Conference on Software, Telecommunications and Computer Networks*, 2008, pp. 147–151.
- [64] Mani, M., & Crespi, N., "Inter-domain QoS control mechanism in IMS based horizontally converged networks," in *International Conference on Networking and Services*, 2007, pp. 82–82.
- [65] T. De Gouveia F. C. & Magedanz, "A framework to improve QoS and mobility management for multimedia applications in the IMS," *Seventh IEEE International Symposium on Multimedia (ISM'05)*, no. IEEE, pp. 216–222, 2005.
- [66] Vázquez, E., Álvarez-Campana, M., García, A. B., & Hernández, A., "Efficiency and quality of service issues in MPLS transport for the UMTS access network. Computer communications," pp. 29(7), 820–826., 2006.
- [67] T. Usui, Y. Kitatsuji, T. Hasegawa, and H. Yokota, "A proposal of feasible architecture for harmonizing IMS with MPLS based traffic engineering," *International Journal of Information Society*, p. .1(2)2–11, 2009.
- [68] S. A. El Kouch R. Bellafkih M. & Raouyane B., "Functioning and management of MPLS/QoS in the IMS architecture," in *2011 International Conference on Multimedia Computing and Systems*, 2011, pp. 1–6.
- [69] ToTompros, S. L., Kavadias, C. D., Vergados, D. D., & Mouratidis, N. P., "A strategy for harmonised QoS manipulation in heterogeneous IMS networks," *Wireless personal communications*, pp. 49(2), 197–212, 2009.

- [70] Ageal, M., Good, R., Elmangosh, A., Ashibani, M., Ventura, N., & Ben-Shatwan, F., "Centralized policy provisioning for inter-domain IMS QoS," in *IEEE EUROCON 2009*, pp. 1793–1797.
- [71] Mohammed, E., Brahim, R., & Mostafa, B., "Fuzzy logic for QoS control in IMS network," *International Journal of Computer Applications*, pp. 28(9) pp39-45, 2011.
- [72] Lai, C. F., & Chen, M, "Playback-rate based streaming services for maximum network capacity in IP multimedia subsystem," *IEEE Systems Journal*, pp. 5(4), 555–563, 2011.
- [73] Abdelkarim, T., Mohamed, O., Brahim, R., & Mostafa, B., "NSIS-based Quality of Service Management in IMS Network," *International Journal of Computer Applications*, pp. 83(4)11–15, 2013.
- [74] Cortes, M., Ensor, J. R., & Esteban, J. O., "On SIP performance. Bell Labs Technical Journal," p. 9(3), 155-172., 2004.
- [75] B. H. M. E. & van Bommel J., "SIP message prioritization and its applications. Bell Labs Technical Journal," pp. 11(1), 21-36., 2006.
- [76] Siddiqui, M. A., Guo, K., Rangarajan, S., & Paul, S, "End-to-end QoS support for SIP sessions in CDMA2000 networks," *Bell Labs Technical Journal*, pp. 9(3), 135-153., 2004
- [77] Molina, M., Quittek, J., Brunner, M., & Melia, T, "Scalable and efficient QoS support for SIP-signalled voice calls," *International Journal of Communication Systems*, pp. 19(4), 407-424., 2006.
- [78] Huang, S. M., Wu, Q., Lin, Y. B., & Yeh, C. H., "SIP mobility and IPv4/IPv6 dual-stack supports in 3G IP multimedia subsystem," *Wireless Communications and Mobile Computing*, pp. 6(5), 585-599., 2006.
- [79] Wang, Q., & Abu-Rgheff, M. A, "Signalling analysis of cost-efficient mobility support by integrating mobile IP and SIP in all IP wireless networks," *International Journal of Communication Systems*, pp. 19(2), 225-247., 2006.
- [80] Lee, H., Song, J. Y., Lee, S. H., Lee, S., & Cho, D. H., "Integrated mobility management methods for mobile IP and SIP in IP based wireless data networks," *Wireless Personal Communications*, pp. 35(3), 269–287, 2005.
- [81] *Postel, J. Rfc793: Transmission control protocol*, 1981.
- [82] Schulzrinne, H., Casner, S., Frederick, R., & Jacobson, V., Ed., *RFC 3550: RTP: A transport protocol for real-time applications*. Status: PROPOSED STANDARD, 2003.
- [83] Yoon, E. J., Ryu, E. K., & Yoo, K. Y., "Attacks and solutions of Yang et al.'s protected password changing scheme. Informatica," pp. 16(2), 285-294., 2005.

- [84] Mousavi-Nik, S. S., Yaghmaee-Moghaddam, M. H., & Ghaznavi-Ghouschi, M. B., "Proposed secure SIP authentication scheme based on elliptic curve cryptography," *International Journal of Computer Applications*, p. 58(8), 2012.
- [85] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., & Stewart, L, Ed., *HTTP authentication: Basic and digest access authentication*. Rfc 2617, 1999.
- [86] Yang, C. C., Wang, R. C., & Liu, W. T., "Secure authentication scheme for session initiation protocol," *Computers & Security*, pp. 24(5), 381–386, 2005.
- [87] "New directions in cryptography," *IEEE transactions on Information Theory*, pp. 22(6), 644–654., 1976.
- [88] Liao, Y. P., & Wang, S. S., "A new secure password authenticated key agreement scheme for SIP using self-certified public keys on elliptic curves," *Computer Communications*, pp. 33(3), 372–380., 2010.
- [89] "Analysis of key-exchange protocols and their use for building secure channels," in *International Conference on the Theory and Applications of Cryptographic Techniques*, 2001, pp. 453–474.
- [90] Wu, L., Zhang, Y., & Wang, F., "A new provably secure authentication and key agreement protocol for SIP using ECC," *Computer Standards & Interfaces*, pp. 31(2), 286–291., 2009.
- [91] Yoon, E. J., & Yoo, K. Y., "Cryptanalysis of NAKE Protocol based on ECC for SIP and Its Improvement," in *2008 Second International Conference on Future Generation Communication and Networking Symposia*, 2008, p. Vol. 2, pp. 25–28.
- [92] Yoon, E. J., & Yoo, K. Y., "A new authentication scheme for session initiation protocol," in *2009 International Conference on Complex, Intelligent and Software Intensive Systems*, 2009, pp. 549–554.
- [93] Q. Xie, "A new authenticated key agreement for session initiation protocol," *International Journal of Communication Systems*, pp. 1(25), 47–54., 2011.
- [94] "A novel mutual authentication scheme for session initiation protocol based on elliptic curve cryptography," in *13th International Conference on Advanced Communication Technology*, 2011, pp. 705–710.
- [95] "Cryptanalysis of Arshad et al.'s ECC-based mutual authentication scheme for session initiation protocol," *Multimedia tools and applications*, p. 65(3), 321–333., 2012
- [96] J. L. Tsai, ("). Efficient Nonce-based Authentication Scheme for Session Initiation Protocol," *IJ Network Security*, pp. 9(1), 12–16., 2009.

- [97] Ring, J. W., Cho, K. K. R., Foo, E., & Looi, M. H., "A new authentication mechanism and key agreement protocol for SIP using identity-based cryptography," *Proceedings of AusCert R&D Stream*, pp. 61–72., 2006.
- [98] Kilinc, H. H., Allaberdiev, Y., & Yanik, T., "Performance evaluation of ID based authentication methods in the SIP protocol," in *2009 International Conference on Application of Information and Communication Technologies*, 2009, pp. 1–6
- [99] F. Hess, "Efficient identity based signature schemes based on pairings," *{In International Workshop on Selected Areas in Cryptography}*, no. Springer, Berlin. Heidelberg. pp. 310–324, 2002.
- [100] Choon, J. C., & Cheon, J. H., "An identity-based signature from Gap Diffie-Hellman groups," *International workshop on public key cryptography*, no. springer. berlin, heidelberg, pp. 18–30, 2003
- [101] Yu, R., Du, G., Yuan, J., & Li, P., "An identity-based mechanism for enhancing SIP security," in *2012 IEEE International Conference on Computer Science and Automation Engineering*, 2012, pp. 447–451.
- [102] B. H. El Abbadi J. A. M. A. L. & Habbani A., "Survey of SIP authentication mechanism," *Journal of Theoretical & Applied Information Technology*, pp. 58(2),357-365, 2013.
- [103] "Elliptic curve cryptography based mutual authentication scheme for session initiation protocol," *Multimedia tools and applications*, pp. 66(2), 165–178, 2013.
- [104]. Zhang Z, Qi Q, Kumar N, Chilamkurti N, Jeong HYg, "A secure authentication scheme with anonymity for session initiation protocol using elliptic curve cryptography," *Multimed Tools Appl*, pp. 74(10):3477–3488, 2015.
- [105] Chaudhry, S. A., Khan, I., Irshad, A., Ashraf, M. U., Khan, M. K., & Ahmad, H. F., "A provably secure anonymous authentication scheme for Session Initiation Protocol," *Security and Communication Networks*, p. 9(18), 5016-5027, 2016
- [106] Chaudhry, S. A., Naqvi, H., Sher, M., Farash, M. S., & Hassan, M. U., "An improved and provably secure privacy preserving authentication protocol for SIP," *Peer-to-Peer Networking and Applications*, pp. 10(1), 1-15., 2015.
- [107] Chen, T. H., Yeh, H. L., Liu, P. C., Hsiang, H. C., & Shih, W. K., "A secured authentication protocol for SIP using elliptic curves cryptography," in *International Conference on Future Generation Communication and Networking*, 2010, pp. 46–55
- [108] Denning, D. E., & Sacco, G. M., "Timestamps in key distribution protocols," *Communications of the ACM*, pp. 24(8), 533–536, 1981.
- [109] Durlanik, A., & Sogukpinar, I. (2005). SIP authentication scheme using ECDH. *World Enformatika Soc Trans Eng Comput Technol.* 8, 350-353.

- [110] Gokhroo, M. K., Jaidhar, C. D., & Tomar, A. S., "Cryptanalysis of SIP secure and efficient authentication scheme," in *2011 IEEE 3rd International Conference on Communication Software and Networks*, 2011, pp. 308–310.
- [111] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., & Stewart, L., "RFC2617: HTTP authentication: basic and digest access authentication." 1999
- [112] Farash, M. S., & Attari, M. A., "An enhanced authenticated key agreement for session initiation protocol," *Information Technology and Control*, pp. 42(4), 333–342, 2013.
- [113] He, D., Chen, J., & Chen, Y., "A secure mutual authentication scheme for session initiation protocol using elliptic curve cryptography," *Security and Communication Networks*, pp. 5(12), 1423–1429, 2012.
- [114] J. L. Tsai, "Efficient Nonce-based Authentication Scheme for Session Initiation Protocol," *IJ Network Security*, p. 9(1), 12-16, 2009.
- [115] Lu, Y., Li, L., Peng, H., & Yang, Y., "A secure and efficient mutual authentication scheme for session initiation protocol," . *Peer-to-Peer Networking and Applications*, p. 9(2), 449-459, 2016.
- [116] Lin, C. L., & Hwang, T., "A password authentication scheme with secure password updating," . *Computers & Security*, pp. 22(1), 68-72., 2003.
- [117] Liao, Y. P., & Wang, S. S., "A new secure password authenticated key agreement scheme for SIP using self-certified public keys on elliptic curves," *Computer Communications*, pp. 33(3), 372-380., 2010.
- [118] Odelu, V., Das, A. K., & Goswami, A., "A secure effective key management scheme for dynamic access control in a large leaf class hierarchy," *Information Sciences*, pp. 269(4), 270–285, 2014.
- [119] Salsano, S., Veltri, L., & Papalilo, D., "SIP security issues: the SIP authentication procedure and its processing load," *IEEE network*, pp. 16(6), 38–44, 2002.
- [120] M. Thomas, "SIP security requirements," . *IETF Internet dren (draftthomas-sip-sec-reg'OO. txt)*., 2001.
- [121] Q. Xie, "A new authenticated key agreement for session initiation protocol," . *International Journal of Communication Systems*, pp. 25(1), 47-54., 2012.
- [122] Wu, L., Zhang, Y., & Wang, F., "A new provably secure authentication and key agreement protocol for SIP using ECC," *Computer Standards & Interfaces*, pp. 31(2), 286–291, 2009.
- [123] Yang, C. C., Wang, R. C., & Liu, W. T., ("). Secure authentication scheme for session initiation protocol," *Computers & Security*, p. 24(5), 381-386, 2005.

- [124] Yoon, E. J., & Yoo, K. Y., "Cryptanalysis of DS-SIP authentication scheme using ECDH," in *2009 international conference on new trends in information and service science*, 2009, pp. 642–647.
- [125] Yoon, E. J., Shin, Y. N., Jeon, I. S., & Yoo, K. Y., "Robust mutual authentication with a key agreement scheme for the session initiation protocol," *IETE Technical Review*, pp. 27(3), 203-213., 2010.
- [126] Yoon, E. J., Yoo, K. Y., Kim, C., Hong, Y. S., Jo, M., & Chen, H. H., "A secure and efficient SIP authentication scheme for converged VoIP networks," *Computer Communications*, pp. 33(14), 1674–1681, 2010.
- [127] Xu, D., Zhang, S., Chen, J., & Ma, M., "A provably secure anonymous mutual authentication scheme with key agreement for SIP using ECC," *Peer-to-Peer Networking and Applications*, pp. 11(5), 837–847, 2018.
- [128] Zhang, Z., Qi, Q., Kumar, N., Chilamkurti, N., & Jeong, H. Y., "A secure authentication scheme with anonymity for session initiation protocol using elliptic curve cryptography," *Multimedia Tools and Applications*, pp. 74(10), 3477-3488., 2015
- [129] Q. Pu, "Weaknesses of SIP authentication scheme for converged VoIP networks," *IACR Cryptol ePrint Arch*, p. 464., 2010.
- [130] A. Vanstone, "Elliptic curve cryptosystem—the answer to strong, fast public-key cryptography for securing constrained environments," 1997.
- [131] Jin, A. T. B., Ling, D. N. C., & Goh, A., "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern recognition*, pp. 37(11), 2245-2255., 2004.
- [132] "An improved biohashing for human authentication," *Pattern recognition*, pp. 40(3), 1057-1065., 2007.
- [133] Burrows, M., Abadi, M., & Needham, R. M., "A logic of authentication. Proceedings of the Royal Society of London," *A. Mathematical and Physical Sciences*, pp. 426(1871), 233–271, 1989.
- [134] Poikselkä, M., Niemi, A., Khartabil, H., & Mayer, G., *The IMS: IP Multimedia Concepts and Services.*, p. John Wiley & Sons. 2007.
- [135] Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I, "Cloud computing and emerging IT platforms," *Vision, hype, and reality for delivering computing as the 5th utility. Future Generation computer systems*, p. 25(6), 599-616., 2009.
- [136] Kilinc, H. H., & Yanik, T., "A survey of SIP authentication and key agreement schemes," *. IEEE Communications Surveys & Tutorials*, pp. 16(2), 1005-1023., 2013.