Brij B. Gupta · Gregorio Martinez Perez
Dharma P. Agrawal · Deepak Gupta
Editors

Handbook of Computer Networks and Cyber Security

Principles and Paradigms

Springer

Handbook of Computer Networks and Cyber Security

Brij B. Gupta • Gregorio Martinez Perez
Dharma P. Agrawal • Deepak Gupta
Editors

Handbook of Computer Networks and Cyber Security

Principles and Paradigms

Springer

Editors
Brij B. Gupta
Department of Computer Engineering
National Institute
of Technology Kurukshetra
Kurukshetra, India

Gregorio Martinez Perez
Department of Computer Science
University of Murcia
Catedrático de Universidad
Murcia, Spain

Dharma P. Agrawal
Department of Electrical Engineering
and Computer Science
University of Cincinnati
Cincinnati, USA

Deepak Gupta
LoginRadius Inc.
Vancouver, BC, Canada

ISBN 978-3-030-22276-5 ISBN 978-3-030-22277-2 (eBook)
https://doi.org/10.1007/978-3-030-22277-2

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Dedicated to my wife, ***Varsha Gupta****, and daughter,* ***Prisha Gupta****, for their constant support during the course of this handbook*

—B. B. Gupta

Dedicated to my wife, ***Raquel****, and son,* ***Izan****, for their constant support during the course of this handbook*

—Gregorio Martinez Perez

Dedicated to my wife, ***Purnima Agrawal****, for her constant support during the course of this handbook*

—Dharma P. Agrawal

Dedicated to my family for their constant support during the course of this handbook

—Deepak Gupta

Preface

Computers have become an integrated part of the modern world and are being extensively used for storing and retrieving information. Business organizations are becoming more productive and efficient with the use of Internet-based applications. A significant rise in their use can be seen for personal purposes as they provide speedy and accurate solution for performing a variety of tasks.

However, the vast amount of data and information that is being stored and communicated among these computing devices is usually of confidential nature which requires high-end protection from the adversarial attacks. Cyberattacks have become a crucial concern for the economies across the globe. Hence, it has become inevitable to establish adequate security measures to safeguard the sensitive information and security critical systems and to identify and evaluate the underlying factors influencing their development.

This handbook contains chapters dealing with different aspects of computer networks and cybersecurity. These include:

- Fundamentals, overviews, and trends of computer networks and cybersecurity
- Security and privacy in ad hoc networks, e-services, mobile systems, wireless sensor networks, smart grid and distributed generation systems, social applications and networks, industrial systems, pervasive/ubiquitous computing, ambient intelligence, cloud computing, and e-services
- Security and privacy of robotic systems and Web service
- Cyber risk and vulnerability assessment for cybercrime
- Cybercrime and warfare
- Cyber threat analysis and modelling
- IoT threat analysis and modelling
- Human factors in security and privacy
- Cyber forensic tools, techniques, and analysis
- Visual analytics for cybersecurity
- Cybersecurity testbeds, tools, and methodologies
- Active and passive cyber defense techniques
- Critical infrastructure protection

- Intrusion detection and prevention
- Botnet detection and mitigation
- Biometric security and privacy
- Human factors in security and privacy
- Cybercrime and warfare,
- Cryptography, stenography, and cryptosystems
- Honeypots and security
- Security policies and access control
- Network security and management
- Wireless security
- Bluetooth, Wi-Fi, WiMAX, and LTE security
- Infrared communication security
- Cyber threats, implications, and their defense
- Security standards and law
- Security modelling

Specifically, this handbook contains discussion on the following:

- An Investigation Study of Privacy Preservation in Cloud
- Security Frameworks in Mobile Cloud Computing
- Latest Quantitative Security Risk Analysis Models for Information Systems with Respect to Cloud Computing
- AckIBE-Based Secure Cloud Data Management Framework
- Machine Learning Solution for Security-Cognizant Data Placement on Cloud Platforms
- Threats Behind Default Configurations of Network Devices: Local Network Attacks and Their Countermeasures
- Security and Privacy issues in Wireless Sensor and Body Area Networks
- Security in Underwater Wireless Sensor Networks
- Security Issues in Cognitive Radio Ad Hoc Networks
- Security and Privacy in Social Networks: Data and Structural Anonymity
- SOI FinFET for Computer Networks and Cybersecurity Systems
- Software-Defined Networking as an Innovative Approach to Computer Networks
- Software-Defined Network (SDN) Data Plane Security: Issues, Solutions, and Future Directions
- Survey on DDoS Attacks, Techniques, and Solutions in Software-Defined Network
- Classification of Cooperative Distributed Denial-of-Service (DDoS) Defense Schemes
- Epidemic Modelling for the Spread of Bots Through DDoS Attack in E-Commerce Network
- Physical Unclonable Functions (puf)-Based Security in IoT: Key Challenges and Solutions
- Fog Computing: Applications and Secure Data Aggregation
- A Comprehensive Review of Distributed Denial-of-Service (DDoS) Attacks in Fog Computing Environment

- Secure Machine Learning Scenario from Big Data in Cloud Computing via Internet of Things Network
- Heterogeneous-Internet of Vehicles (IoV) Communication in the Twenty-First Century: A Comprehensive Study
- A Review on Security and Privacy in Mobile Systems
- Investigation of Security Issues and Promising Solution in Distributed Systems Monitoring
- An Analysis of Provable Security Frameworks for RFID Security
- Computational Techniques for Real-Time Credit Card Fraud Detection
- Security and privacy in Industrial System
- Privacy Preservation of Electronic Health Record: Current Status and Future Direction
- QKD Protocols’ Security Between Theory and Engineering Implementation
- Survey of Security and Privacy Issues on Biometric System
- Design of a Fingerprint-Based Session Key Generation and Secure Communication Establishment Protocol
- Trees, Cryptosignatures, and Cyberspace Mobile Agent Interfaces
- Permutation-Substitution-Based Image Encryption Algorithms Using Pseudo Random Number Generators
- Recent Trends in Document Authentication Using Text Steganography
- Machine Learning-Based Intrusion Detection Techniques
- Feature Selection Using Machine Learning to Classify a Malware
- DeepDGA-MINet: Cost-Sensitive Deep Learning-Based Framework for Handling Multiclass Imbalanced DGA Detection
- ABFT: Analytics to Uplift Big Social Events Using Forensic Tools
- HackIt: A Real-Time Simulation Tool for Studying Real-World Cyberattacks in the Laboratory

Kurukshetra, India
Murcia, Spain
Cincinnati, OH, USA
Vancouver, BC, Canada
December 2019

Brij B. Gupta
Gregorio Martinez Perez
Dharma P. Agrawal
Deepak Gupta

Acknowledgment

Many people have contributed greatly to this *Handbook of Computer Networks and Cyber Security Principles and Paradigms*. We, the editors, would like to acknowledge all of them for their valuable help and generous ideas in improving the quality of this handbook. With our feelings of gratitude, we would like to introduce them in turn. The first mention is the authors and reviewers of each chapter of this handbook. Without their outstanding expertise, constructive reviews, and devoted effort, this comprehensive handbook would become something without contents. The second mention is the Springer publisher staff, especially Susan Lagerstrom-Fife, Senior Publishing Editor, and her team for their constant encouragement, continuous assistance, and untiring support. Without their technical support, this handbook would not be completed. The third mention is our family for being the source of continuous love, unconditional support, and prayers not only for this work but throughout our life. Last but far from least, we express our heartfelt thanks to the Almighty for bestowing over us the courage to face the complexities of life and complete this work.

Contents

About the Editors

Brij B. Gupta received his PhD from Indian Institute of Technology Roorkee, India, in the area of Information and Cybersecurity. In 2009, he was selected for Canadian Commonwealth Scholarship Award by the Government of Canada. He has published more than 250 research papers in international journals and conferences of high repute including IEEE, Elsevier, ACM, Springer, Wiley, Taylor & Francis, Inderscience, etc. He has visited several countries, i.e., Canada, Japan, Australia, China, Spain, Hong Kong, Italy, Malaysia, Macau, etc., to present his research work. His biography was selected and published in the 30th edition of *Marquis Who's Who in the World*, 2012. In addition, he has been selected to receive "2017 Albert Nelson Marquis Lifetime Achievement Award" by *Marquis Who's Who in the World*, USA. He also received Sir Visvesvaraya Young Faculty Research Fellowship Award in 2017 from the Ministry of Electronics and Information Technology, Government of India. Recently, he has been awarded with "2018 Best Faculty Award for Research Activities" and "2018 Best Faculty Award for Project and Laboratory Development" from the National Institute of Technology, Kurukshetra, India. He is also working as principal investigator of various R&D projects sponsored by various funding agencies of the Government of India. He serves as associate editor of *IEEE Transactions on Industrial Informatics* and *IEEE Access* and executive editor of *IJITCA* and Inderscience, respectively. Moreover, he also leads the *International Journal of Cloud Applications and Computing* (IJCAC), IGI Global, USA, as editor-in-chief. He also serves as reviewer for various journals of IEEE, Springer, Wiley, Taylor & Francis, etc. He also served as TPC chair of the 2018 IEEE INFOCOM: CCSNA, USA. He is senior member of IEEE; member of ACM, SIGCOMM, SDIWC, Internet Society, and the Institute of Nanotechnology; and life member of the International Association of Engineers (IAENG) and the International Association of Computer Science and Information Technology (IACSIT). He was also visiting researcher with Yamaguchi University, Japan (2015 and 2018); Deakin University, Australia (2017); and Swinburne University of Technology, Australia (2018). At present, he is working as assistant professor in the Department of Computer Engineering, National Institute of Technology, Kurukshetra, India. His research interest includes information security, cybersecurity, mobile/smartphone, cloud computing, web security, intrusion detection, computer networks, and phishing.

Gregorio Martinez Perez received his PhD in Computer Science at the University of Murcia (Spain). In 1997, he started working in the Computer Service of the same university on various projects on end-user products related to security and networking, and in 2014, he was appointed as full professor in the same department. His scientific activity is mainly devoted to cybersecurity, privacy, and 5G networking, including security considerations, management models, network slicing, and communication architectures. He is also working on the design and autonomic monitoring of real-time and critical applications and systems. He is working on different national (14 in the last decade) and European IST research projects (11 in the last decade) related to these topics, being principal investigator in most of them. He has published more than 160 papers in national and international conference proceedings, magazines, and journals. He has been guest editing more than 30 special issues in different journals and magazines in the last few years. He is member of the editorial board of 16 journals, most of them related to the topics being covered in this handbook. He has already supervised ten PhD students, several of them recognized with honors. He is currently the deputy director for Knowledge Transfer of the University of Murcia.

Dharma P. Agrawal is the Ohio Board of Regents distinguished professor and the founding director for the Center for Distributed and Mobile Computing in the Department of Electrical Engineering and Computing Systems. He has been a faculty member at the ECE Department, Carnegie Mellon University (on sabbatical leave); NC State University, Raleigh; and Wayne State University. His current research interests include applications of sensor networks in monitoring patients with Parkinson's disease and neurosis, fitness of athletes' personal wellness, and firefighters' physical condition in action, efficient and secured communication in sensor networks, secured group communication in vehicular networks, the use of femtocells in LTE technology and interference issues, heterogeneous wireless networks, and resource allocation and security in mesh networks for 4G technology. His recent contribution in the form of a coauthored introductory textbook entitled *Introduction to Wireless and Mobile Systems*, 4th edition, has been widely accepted throughout the world. The book has been reprinted both in China and India and translated into Korean and Chinese languages. His coauthored book entitled *Ad hoc and Sensor Networks*, 2nd edition, has been published in spring of 2011. A coedited book, entitled *Encyclopedia on Ad Hoc and Ubiquitous Computing*, has been published by the World Scientific, and coauthored books entitled *Wireless Sensor Networks: Deployment Alternatives and Analytical Modeling*; *Innovative Approaches to Spectrum Selection, Sensing, On-Demand Medium Access in Heterogeneous Multihop Networks*; and *Spectrum Sharing in Cognitive Radio Networks* have been published by Lambert Academic. He is a founding editorial board member of *International Journal of Distributed Sensor Networks*, *International Journal of Ad Hoc and Ubiquitous Computing* (*IJAHUC*), *Ad Hoc & Sensor Wireless Networks*, and *Journal of Information Assurance and Security* (*JIAS*). He has served as an editor of the IEEE *Computer Magazine* and the *IEEE Transactions on Computers*, *Journal of Parallel and Distributed Computing*, and *International Journal of High Speed Computing*. He has been the program chair and general chair for numerous international conferences and meetings. He has received numerous certificates from the IEEE Computer Society. He was awarded a *Third Millennium Medal* by the IEEE for his outstanding contributions. He has delivered keynote speech at 34 different international conferences. He has published over 655 papers and has given 52 different tutorials and extensive training courses in various conferences in the USA and numerous institutions in Taiwan, Korea, Jordan, UAE, Malaysia, and India in the areas of ad hoc and sensor networks and mesh networks, including security issues. He has graduated 72 PhD and 58 MS students. He has been named as an ISI Highly Cited Researcher and is a fellow of the IEEE, the ACM, the AAAS, and the World Innovation Foundation and a recent recipient of 2008 IEEE CS Harry Goode Award. Recently, in June 2011, he was selected as the Best Mentor for Doctoral Students at the University of Cincinnati. Recently, he has been inducted as a charter fellow of the National Academy of Inventors. He has also been elected a fellow of the IACSIT (International Association of Computer Science and Information Technology), 2013.

Deepak Gupta received his Master of Science degree from Illinois Institute of Technology, Chicago, USA, in the area of Computer Forensics and Cybersecurity with a specialization in Voice Over Internet Protocol (VOIP). As an undergraduate student, he became certified on the major networking platforms, first as a CCNA (Cisco Certified Network Administrator) and then as a MCP (Microsoft Certified Professional) which would come to serve him well in his professional life. As a graduate student, he continued to challenge himself by working on a number of research papers and projects related to computer network security and forensics research, including the topics of multi-boot computer systems with change of boot loader and MP3 steganography. He also developed and furthered his interest in VOIP technology by working on and leading research projects with Bell Labs, a prominent VOIP research lab based in Chicago. He also wrote research papers in this field on the topics of P2P communication and SIP protocols which won him the Best Student VOIP Project Award in 2007. Over the last 10 years of professional experience, he has gained a broad range of experience in computer security and technology that spans multiple fields and industries. After graduating with distinction with an MS in Computer Science, he went on to work for Sageworks, a financial software company based in Raleigh, NC. There, among other things, he developed a centralized integration process for core banking platforms that would allow customers to easily port and map their data to the central banking database. Deepak is a product visionary who founded a web agency and two other startups as a software entrepreneur to help businesses to simplify their user communication. It was during this time that his passion for innovation and entrepreneurship led him to found LoginRadius, a costumer identity and access management (CIAM) SaaS platform that helps businesses improve and optimize their customer experience by creating unified digital identities across multiple touch points, where he remains today as co-founder and CTO. At LoginRadius, he makes use of his expertise in security and forensics to innovate and improve how identity services are delivered and secured in the cloud identity space and helps businesses deliver social media integrations by a simplified REST API. Currently, LoginRadius is a leading provider of cloud-based CIAM solutions for mid-to-large-sized companies, and the platform serves over 3000 businesses with a monthly reach of 850 million users worldwide. The company has been named as an industry leader in the CIAM space by Gartner, Forrester, KuppingerCole, and Computer Weekly. Deepak is also passionate about helping businesses improve and optimize their customer experience. He lives and breathes this topic with customers everyday by helping them think through questions such as how do users interact with their website, how to simplify the customer's experience (via single sign-on, one touch login, etc.), and how to keep the customer's data secure. He is active member of the IEEE, ACM, OpenID Foundation, Cloud Security Alliance (CSA), and other tech communities. He is doing his current research in machine learning, artificial intelligence, and blockchain technologies. Web: www.guptadeepak.com, www.loginradius.com

Chapter 1
Security Frameworks in Mobile Cloud Computing

Chaitanya Vemulapalli, Sanjay Kumar Madria, and Mark Linderman

Abstract The concept of mobile cloud computing (MCC) combines mobile computing with cloud resources, and therefore, has opened up new directions in the field of mobile computing. Cloud resources can help in overcoming the memory, energy, and other computing resource limitations of mobile devices. Thus, the mobile cloud computing applications can address some of the resource constraint issues by offloading tasks to cloud servers. Despite these advantages, mobile cloud computing is still not widely adopted due to various challenges associated with security in mobile cloud computing framework including issues of privacy, access control, service level agreements, interoperability, charging model, etc. In this chapter, we focus on the challenges associated with security in mobile cloud computing, and key features required in a security framework for MCC. Initially, we describe key architectures pertaining to various applications of mobile cloud computing, and later, we discuss few security frameworks proposed for MCC in terms of handling privacy, security, and attacks.

Keywords Mobile cloud computing · Security · Mobile computing · Location Based services

1 Introduction

Mobile computing is becoming part of everyday life with wireless communication becoming ubiquitous. The technological advancement in mobile devices and invention of smart phones has taken the usage of mobile phones from the conventional use of voice communication to more now as the computing device. Incorporation

C. Vemulapalli · S. K. Madria (✉)
Missouri University of Science and Technology, Rolla, MO, USA
e-mail: sv2v7@mst.edu; madrias@mst.edu

M. Linderman
AFRL, Information Directorate, Rome, NY, USA
e-mail: mark.linderman@us.af.mil

B. B. Gupta et al. (eds.), *Handbook of Computer Networks and Cyber Security*,
https://doi.org/10.1007/978-3-030-22277-2_1

of sophisticated features like in-built camera, GPS, multimedia capabilities, etc. gave additional functionalities to the mobile devices. The range of functions that can be performed by mobile devices is the main driving force behind the growth of mobile computing. All these advanced features increase the software and processing overhead in mobile devices. Moreover, the advancement of software in mobile devices is happening at a more rapid pace compared to advancement in mobile hardware. Users are not able to fully exploit these advanced features due to hardware limitations of the mobile devices such as limited processing capabilities, insufficient storage, limited battery backup, etc.

In the last decade, with access to Internet becoming more and more ubiquitous, connecting to a cloud server via Internet from a mobile device is no longer a difficult proposition. This stimulated a new idea of using cloud resources for the processing and storage requirements of mobile device and gave rise to the new computing paradigm of mobile cloud computing. In this paradigm, to overcome the above said hardware limitations of mobile devices, storage tasks, communication, and computation intensive tasks are offloaded to cloud servers instead of performing them in mobile devices itself. The mobile devices will retain only thin client for user interface or display of results. Examples of such thin clients include mobile apps like YouTube, Facebook, etc.

Usage of smart phones and mobile cloud computing is also increasing at a rapid pace. According to ABI Research (Allied Business Intelligence, Inc.), a market intelligence company, the number of mobile cloud computing subscribers worldwide grew from 42.8 million subscribers in 2008 to over 100 million in 2014 [13]. Another study by Juniper Research said that the market of cloud-based mobile applications grew by about 88% from $400 million in 2009 to $9.5 billion in 2014 [23]. It was reported that more than 240 million of mobile cloud computing (MCC) customers will use cloud services with an earning revenue of 5.2 billion dollars in 2015. Gartner forecasts that global mobile phone shipments will increase 1.6% in 2018, with total mobile phone sales amounting to almost 1.9 billion units. In 2019, it will grow by 5% year over year. This growth in mobile cloud computing has opened up the possibility of enhancing applications like location-based services, information sharing, etc.

Use of mobile cloud computing in disaster recovery and emergency service has also been described in [26]. Though the concept of using cloud resources has made the mobile computing more useful and empowered it to perform any task without limitations, the security and privacy issues associated with cloud computing are deterring the large scale adoption of mobile cloud computing applications. In despite of efforts devoted in research both in industry and in academia, there are a number of loopholes in the security policies of mobile cloud computing. According to surveys [2, 27], 74% of IT executives are not interested to adopt cloud services due to security issues and risks associated with it. Some secondary limitations like limited processing power, low storage are mentioned as obstacles for computationally intensive and storage demanding applications on a mobile platform. The major data security risks such as data loss, data breach, and data privacy result from the fact that mobile users' data is stored and processed in clouds that are located at the service providers' end.

Rest of this chapter is organized as follows: In Sect. 2, we initially describe some of the architectures of mobile cloud computing proposed by researchers. In Sect. 3, we discuss the importance of security in mobile cloud computing and the security aspects that are necessary in MCC. In Sect. 4, we provide a review of the security frameworks proposed in the literature for authentication, privacy, secure storage, and secure computing. In Sect. 5, we discuss attacks, risk assessment, and vulnerability in mobile clouds. Section 6 is the discussion section comparing different techniques. And, finally, Sect. 7 concludes this chapter.

2 Architecture of Mobile Cloud Computing

Since the demand for smartphones and tablets is constantly increasing, manufacturers of these devices are improving the technology and usability of devices. It is because of handy shape and size, mobile devices are being used to perform most tasks that a desktop or laptop computer is currently used for. These devices can also connect to the resources of cloud computing called mobile cloud computing (MCC) which has increased the challenges due to the security loopholes. Mobile cloud computing is relatively a new computing paradigm and the basic general idea behind an architecture of mobile cloud computing involves mobile devices, mobile network, and cloud servers. Mobile devices access the Internet using wireless network, and through the Internet communicate with the cloud servers.

Figure 1.1 depicts a general architecture of mobile cloud computing. Though this is a basic architecture of mobile cloud computing, various other versions of mobile cloud computing architectures have been proposed based on the applications. Many of the services available under conventional cloud computing are also available for mobile computing. These include Data storage as a Service (DaaS), Communication as a Service (CaaS), Security as a Service (SecaaS), Software as a Service (SaaS), etc.

One of the main applications of mobile cloud computing already being widely used is data storage in cloud. Here, authorized users are allocated storage space in the cloud servers. In this architecture, data files such as images, videos, and other personal files are uploaded to the cloud server to overcome the storage limitations in mobile devices and give the flexibility of accessing the files anytime and from anywhere. Mobile apps like Dropbox, iCloud, SkyDrive, etc. are few such examples.

Another important type of usage or application of mobile cloud computing is where communication and computation are offloaded to the cloud. Figure 1.2 gives a pictorial representation of the architecture associated with this type of service/application of MCC. In this architecture, virtual smart phone devices are setup in the cloud to which the physical devices can connect and offload their tasks. These are called by different names such as virtual images [3], extended semi shadow images (ESSI) [11], etc., by different authors but the underlying idea is the same, i.e., having virtual machines in the cloud server. In this chapter, we use the term virtual image to describe these virtual machines in the cloud. These virtual images can be full or partial images. Virtual images are free of any physical

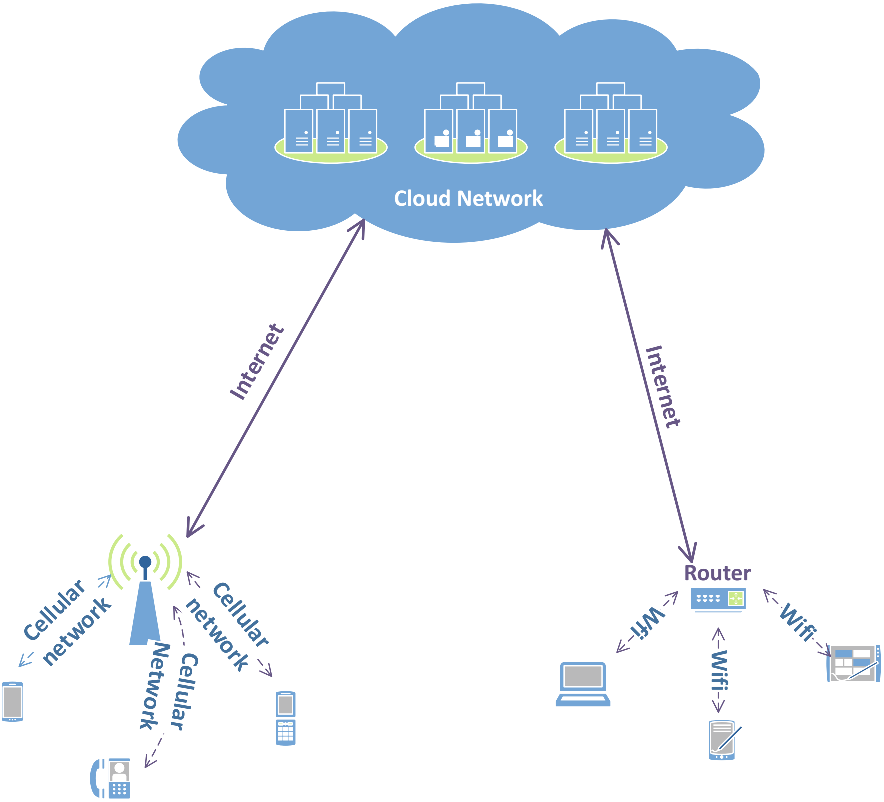

Fig. 1.1 General architecture of mobile cloud computing

limitations that are synonymous with physical mobile devices such as limited battery power and limited processing capabilities. Moreover, users can allocate/configure these virtual images as per requirement. Mobile devices connect to their respective virtual images in the cloud through the Internet from available wireless networks. Mobile devices connect to the nearby access points through wireless communication and access points are connected to cloud servers via the Internet in various ways with fixed network used at some point in the network. The mobile devices are connected to virtual images in the cloud using a secure communication channel through the Internet. The two main operations that result in high battery consumption in a mobile device are computing and communication tasks. The mobile devices can offload high CPU consumption tasks to the virtual image in cloud since it possesses more powerful computing resources and no battery limitation. Similarly, communication among physical mobile devices is affected by many factors such as mobility, range, battery power, and other environmental factors. Offloading the communication tasks to their virtual counter parts in the cloud can help in overcoming these factors since virtual images are fully connected and do not possess any battery limitations.

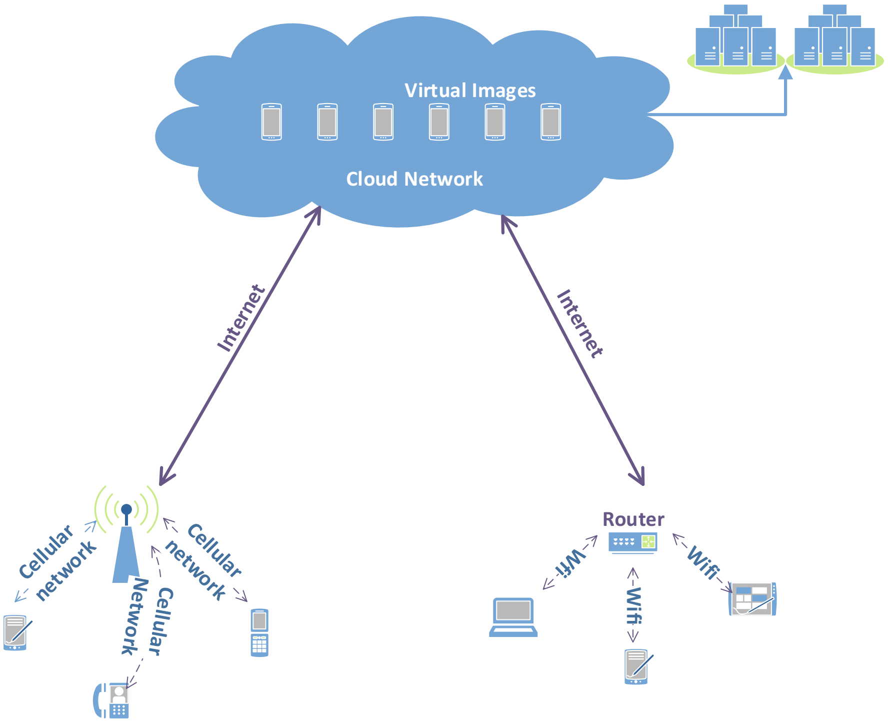

Fig. 1.2 Architecture of mobile cloud computing with virtual images

Olafare et al. [20] performed a research focused on the security challenges and possible solutions in MCC. They proposed the adoption of applications on the mobile device which keep a check on amount of information third-party applications can have access to. In addition, the validity and authenticity of third-party application needs to be checked before installing. Also, the third-party application signature or certificate needs to be checked in order to ensure that the updated version signature matches the original signature of the third-party application. The authors further discussed MCC models/architectures with security components to counter attacks. It is also being suggested to use SSL certificate for the security of communication channel. Without using SSL, it is easy for an attacker to bridge the data transmission and act as a cloud server to tamper the data. Using SSL, when the user starts using the cloud services, data sent to the user is an SSL encrypted data. The key for decryption of the data is sent to the user over a personal email account. The authors then classified the security threats into three major categories: mobile device threats, threats to the cloud (cloud computing), and network threats. For each category of security issues that are related to MCC, the author has designed a framework/architecture with security components.

3 Security Aspects of Mobile Cloud Computing

Most of the applications of mobile cloud computing involve exchange of data with cloud servers which are beyond the control of mobile users. This information may also include private data of users such as his location, usage details, etc. So it is very important to protect this user information from adversary. Since cloud provider is also a third party, it can also be considered as a potential adversary. The security requirements in MCC may slightly vary with the application but the basic and mandatory aspects of security in mobile cloud computing would be (1) authentication, (2) data integrity and confidentiality, and (3) privacy.

Authentication In mobile cloud computing, mobile users utilize the cloud resources for their storage needs, offloading computation and communication tasks. Since cloud servers will be used by number of users, there should be an authentication mechanism between mobile users and the cloud. In another architecture of MCC mentioned earlier, virtualization is used and virtual images are maintained in the cloud. This architecture requires added authentication mechanism between virtual images.

Data Integrity and Confidentiality One of the main applications of cloud computing is to use cloud resources for storing users' data. This is one of the major advantages of mobile cloud computing. Usually, mobile devices have limited storage capacity. In order to overcome this limitation, files are offloaded to the cloud servers so that they can be accessed from anywhere and at any time. But the cloud servers are not in the control of mobile users, and hence, cloud service providers could also be potential adversary. Therefore, efficient encryption mechanisms must be in place to preserve the confidentiality and integrity of the files stored in the cloud servers. Moreover, there should be provision for users to verify the integrity of files at any instant of time.

Privacy In mobile cloud computing, mobile users constantly communicate with cloud servers to access their resources. In this process, privacy of the mobile user needs to be protected from the cloud service provider as well. In some applications like location-based services using mobile cloud computing, this is more important as the user location information should be protected from other entities.

4 Security Frameworks for Mobile Cloud Computing

4.1 Authentication Frameworks for Mobile Cloud Computing

A Framework of Authentication in the Cloud for Mobile Users In the paper [7], the authors address the issue of device authentication in mobile cloud computing using policy based authentication. The proposed scheme uses the implicit authentication and trustcube. Unlike traditional authentication mechanisms which are based on aspects like what you have, what you know, and what you are, implicit authentication is based on what you do. By this users are identified by their habits, as opposed to their belongings, memorized data, and biometrics. Implicit authentication can be implemented in various ways like IP address, device profiles, etc. However, in this scheme, they use implicit authentication based on mobile data such as calling patterns, short messages (SMS) activity, website accesses, and location information which is automatically available with the network operators/carriers. This kind of implicit authentication gives an added security by protecting against unwanted access from stolen handsets. Implicit authentication is a statistical test and works based on comparison with threshold values. Based on the observed behavior of the users with mobile data, probabilistic authentication scores are calculated and assigned to client devices. The proposed authentication framework compares the calculated authentic score with the threshold values to verify whether the device is with legitimate user or not. The threshold value and amount of uncertainty allowed is dependent on the type of the application.

Figure 1.3 depicts the block diagram of the proposed framework. It has four main components: (a) client device, (b) data aggregator, (c) authentication engine, (d) authentication consumer. Client devices are the mobile devices on which the user performs his daily actions. The data aggregator constantly collects data on

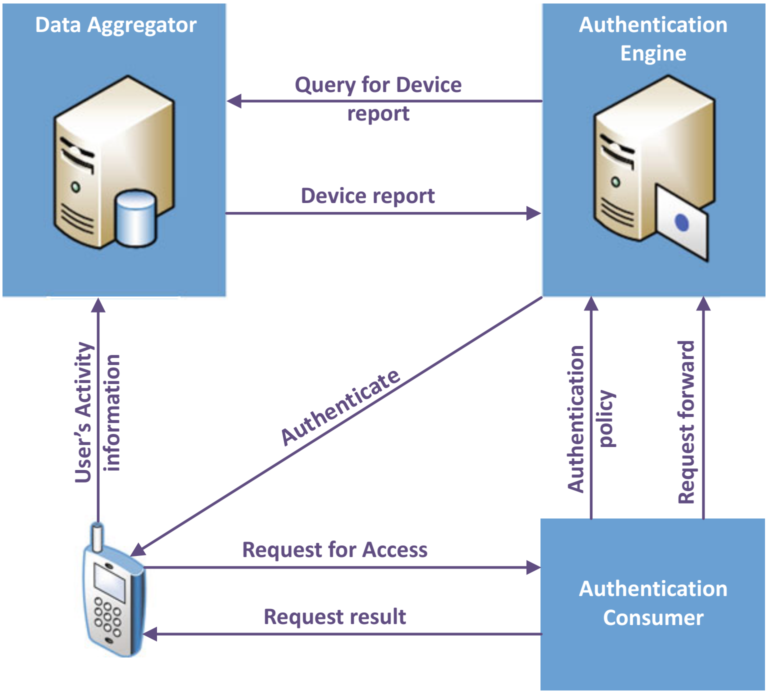

Fig. 1.3 Main components of the MCC framework and their interactions

context and action from the client devices. The authentication engine will obtain this information from data aggregator or from client device directly and the corresponding authentication policies from authentication consumer. Based on the results from the authentication engine, the authentication consumer responds to the clients' request.

Prior to the authentication process, authentication consumer prepares the list of access requests that require authentication. A policy is determined for each of the request and registered with the authentication engine. Each policy consists of at least three parts: the access request, the information to be collected from the client devices or data aggregator for this access request, and a policy rule. The policy rules consist of integrity check rules on the platform and environment, a threshold value for the authentication score, and the alternate authentication method if the authentication score is less than a threshold value. After the policy is registered with the authentication engine, when the authentication consumer receives an access request, it redirects the request to the authentication engine. Authentication engine obtains the required client info from the data aggregator or the client itself and then applies the authentication rule in the policy and determines the authentication result and sends this back to the authentication consumer. If the authentication result is successful, the authentication consumer will service the request. The proposed framework can also be scaled to large number of users by using multiple instances of authentication service within the cloud on demand.

Feasibility of Deploying Biometric Encryption in MCC In the work [31], Zhao et al. proposed an authentication framework for mobile cloud environment using biometric encryption (BE). Biometric encryption is more reliable compared to conventional security systems based on secret key due to its features that are difficult to forget, lose, share, and forge. The science of using physiological or behavioral features of human such as fingerprint, iris, face, signature, voice, etc. to identify him or her is called biometric identification. Combination of this biometric identification and cryptography is called biometric encryption. It combines biometrics and secret key, and they cannot be achieved in the templates stored in the system. Only when a living biometric feature was proposed to the system, the secret key would be generated. There are three encryption system models based on biometric encryption. First is the key release model in which the biometric feature and secret key are superposed to be the biometric feature template. Secret key is released only when the biometric feature matches. Second is the key binding model in which biometric feature and key materials are combined to be the biometric feature templates in encryption scheme. Third model is the key generation model in which secret key is extracted directly from the signal instead of from the external input.

The architecture of the proposed framework is depicted in Fig. 1.4. In the proposed framework, a separate cloud authentication center (CAC) is established to relieve the application server from the burden of analyzing and verifying requests from users. CAC is assumed to be a trusted party. Initially, BE application developers register their products in the platform when they are released. This informs the required parameters, including the category of the application, biometric

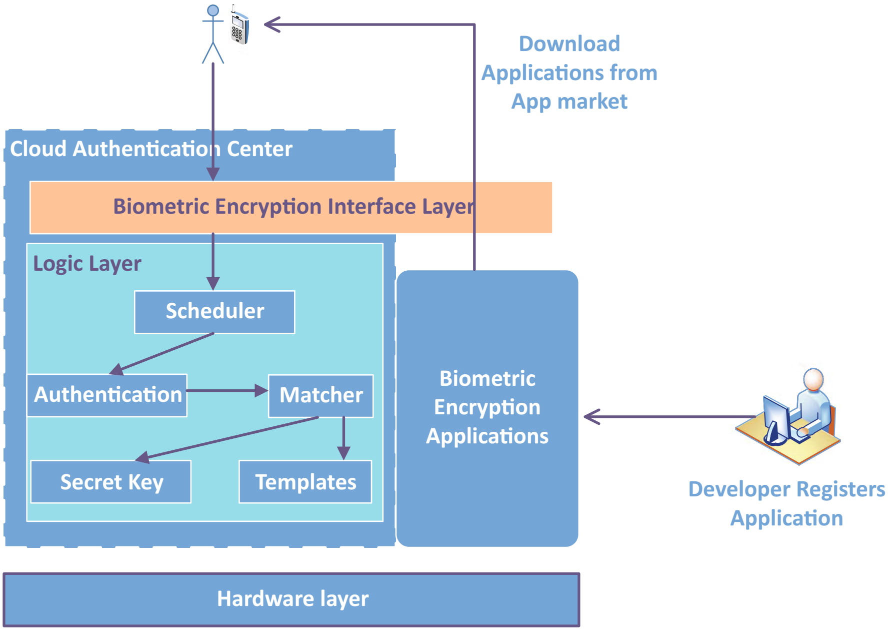
Download Applications from App market
Cloud Authentication Center
Biometric Encryption Interface Layer
Logic Layer
Scheduler
Authentication
Matcher
Secret Key
Templates
Biometric Encryption Applications
Developer Registers Application
Hardware layer

Fig. 1.4 Mobile cloud platform architecture for authentication using biometric encryption

features requested, security level, etc. These applications are downloaded by the users from app repository in the platform. Before a user can begin using the applications, a record containing his biometric features must be created on the platform and this is done through a specific interface. Application accomplishes this by calling BE module on the mobile device. CAC is the core component for the architecture. It schedules requests from clients, matches the submitted biometric data with the original ones, and also manages the biometric feature templates and secret keys. It makes the authorization for all the applications and users. Overall, the CAC analyzes the biometric data sent by applications and sends the result to application servers.

A Framework for Secure Mobile Cloud Computing The authors of this paper [25] discuss the use of biometric authentication framework to access the cloud. Biometric authentication supplies a bigger measure of protection and accuracy compared to other authentication methods with low hardware costs and secure entry. Biometric is the most effective method to authenticate the users and to protect them from illegal and unauthorized customers. The preprocessing steps and algorithms for extracting the features, and matching of the biometrics traits are discussed in detail. The authentication of fingerprint password is done over web-based services within cloud computing. The two phases discussed are biometric authentication framework enrollment and verification. The matching algorithm steps include comparing the input images with the template images. Template images are collected during the enrollment which are then compared with input images during the recognition phase. This phase decides if the input image and template image match or not. The authors proposed a novel matching score algorithm for considering features of biometrics. It is a combination of strong and weak classifiers which combines the matching scores of each subsystem to find multiple matching scores which are then sent to the decision phase. In this algorithm, the weak classifier is called for each iteration in order to generate a weak ranking. The matching algorithm decides to underline diverse parts of the training data. Hence, it was concluded that biometric authentication is the most effective authentication method as the fingerprints are unique.

Middleware Layer for Authenticating Mobile Consumers of Amazon S3 Data In [18], Lomotey and Deters proposed an authentication framework for mobile consumers of Amazon Simple Storage Service (Amazon S3) based on middleware oriented framework called MiLAMob and OAuth 2.0. Usually, to access Amazon S3, users have to provide credentials such as access key, secret access key, and a signature which is not very efficient for mobile environment as it contributes to HTTP traffic in request response architecture. Generating the hash message authentication code (HMAC) signature in mobile device also contributes to the computation overhead. Moreover, storing an access key Id, secret access key, and HMAC signature in mobile device is another security issue since the device can fall into wrong hands at any moment. The proposed framework overcomes these issues by introducing a middleware which handles the security and data request issues with Amazon S3 on behalf of the user. Architecture of the proposed framework shown in [18] is illustrated in Fig. 1.5.

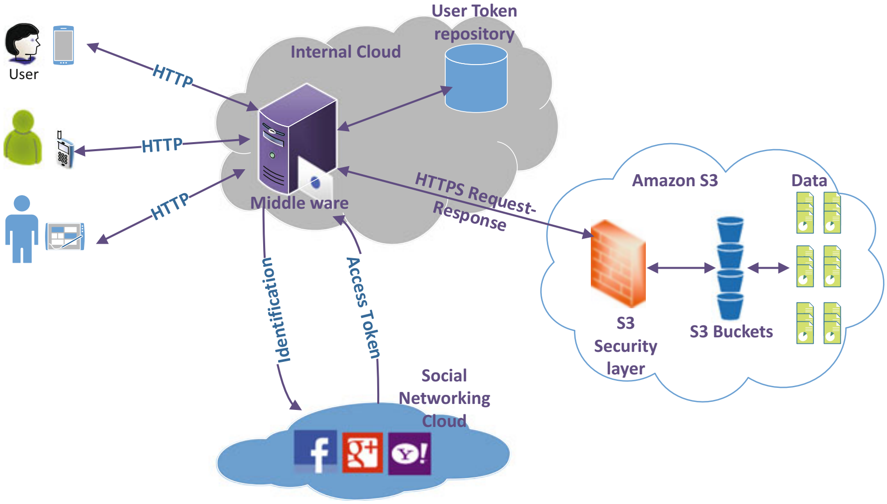

Fig. 1.5 Framework for authentication using middleware-layer for MCC

The proposed MiLAMob framework contains four major components. They are (1) mobile platform, (2) middleware, (3) the social networking platform, and (4) Amazon S3. For mobile platform, the framework advocates usage of mobile web frameworks approach rather than native approach mainly for the reason that it allows users to use heterogeneous mobile devices rather than being confined to a single mobile provider. The middleware is core of MiLAMob framework with three interfaces connected to mobile participants, social networking cloud, and Amazon S3. When a user wants to access Amazon S3, he/she first connects to middleware through publicly available URI. Middleware redirects the user to an authentication page where the user can chose a preferred authentication method. It could be either a personal login or through available social media like Facebook login, Google login, etc. If the user chooses to authenticate using Google credentials, then he is redirected to Google login page where he enters his id and password. After successful authentication, the middleware receives the users' security tokens and based on that it retrieves the user's Amazon S3 security credentials from its repository. The middleware then sends the request over HTTPS to Amazon S3 authentication system. If the request passes the authentication test, middleware retrieves the requested object and sends it to the mobile user. In this mechanism, user only interacts with middleware or social network media and Amazon S3 component is hidden from the user. Mobile users have no knowledge about Amazon S3 security tokens. Due to this, unauthorized use of system is prevented to some extent. Though this middleware component can be hosted on any public domain cloud, this paper advocates to host it on a private cloud to have full control of security issues. Incorporating authentication using social network media is the distinguishing feature of MiLAMob framework and it facilitates business-to-business (B2B) and business-to-consumer (B2C) support. Thus, by allowing user to authenticate using personal login or social network media, MiLAMob framework facilitates what is referred to as hybrid authentication mechanism.

Context Awareness Architecture in MCC Most of the authentication frameworks try to authenticate the device rather than the actual user and device may be lost or go into wrong hands very easily. This is an important issue when it comes to mobile devices. In order to overcome this issue, in [32], Zhou et al. proposed an authentication framework based on context aware data. Context aware data includes phone records, calendar, GPS applications, and battery data. Most of the other implicit authentication frameworks previously proposed take only time factor into consideration and does not take the periodic activities into consideration. The proposed context awareness architecture (CAA) in mobile cloud computing proposed in [32] is illustrated in Fig. 1.6.

The proposed CAA architecture primarily consists of three entities, namely the mobile client, cloud services, and CAA protocol. The mobile client/device has context aware data for mobile devices and corresponding protocol as the two major components. Decision-making device calculates the similarity of users recent behavior and activities with respect to the context awareness algorithm and then compares with the data in users characteristics database. It then passes the calculated

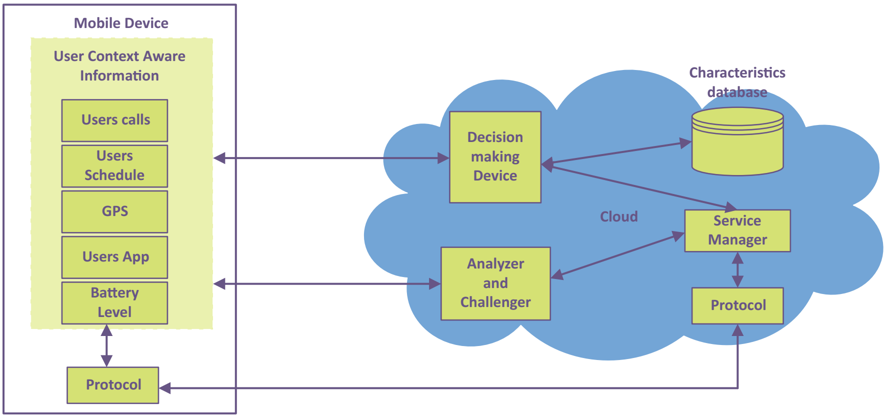

Fig. 1.6 Context aware architecture for authentication in MCC

similarity to the service manager. Service manager is the main component of this architecture. Based on the results provided by decision-making device, the service manager decides whether to allow the users to use the resources or to throw challenges through the Analyzer and Challenger. It also performs the task for formulating and implementing the new protocol and deciding whether to take the users frequent activities into users characteristics database. Data received by Analyzer and Challenger is divided into three kinds: high risk, medium danger, and low risk. If the received data is completely different from the one in characteristics database, then it is considered as high risk and the user is asked to enter a PIN code. If the user fails to enter the correct PIN code, he is denied access to the resources. In the medium danger condition, the user is asked to enter date of birth or a special phone number. In the low risk case, the user need not enter any further information for authentication and this reduces the explicit input of data. The user context data accepted by service manager as that of correct users is stored in users characteristic database for future authentication.

Consolidated Identity Management System for Secure MCC Security is the major obstacle while using the cloud server. In the survey conducted by the authors [14], it was noticed that more than 66% of the users tend to store personal identifiable information (PII) in unprotected text files, cookies, or applications. Mobile devices could be lost or stolen and compromised. These facts related to mobile devices make them attractive targets to obtain unauthorized access by intruders. In order to support the legitimate access process over the clouds, third-party identity management systems (IDMs) have been proposed. The access management systems depend on IDMs for identity generation, authentication, and authorization. However, IDMs are vulnerable to attacks which lead authors to introduce new IDM architecture dubbed consolidated IDM (CIDM) which countermeasures these vulnerabilities. It includes separating the credentials and distributing them over all the IDMs, adding second layer of authentication by allowing user to respond to human-based challenge–response and securing the communication link among cloud service provider and CIDM. A set of experiments were conducted over the IDMs and CIDMs and it was observed that the security provided by CIDM outperforms compared to the security provided by the current IDM systems. Also, it has less energy and communication overhead compared to the current IDM systems.

Identity Management Protocol for Secure MCC With increase in the use of mobile cloud computing, there is an increase in number of applications provided by the SP (service providers) which is causing traffic overload problems. This needs excessive network maintenance, creating an imbalance between profit and investment. The increasing number of mobile users has also caused identity management problems, which according to authors can be solved by using improved IDM3G protocol along with an additional authentication management protocol. The requirements for IDs include not just clarity for users, but also support for multiple IDs and maintaining anonymity and privacy. Interoperability, efficient management, and certification management are discussed in [22] which are considered to be the key network issues. The proposed method maintains the mobile operators (MOs) and constructs a trusted base with cross certification between service providers and MOs. It depends on public key infrastructure (PKI) to enable mutual dependence-based communication and ID management by service providers. It uses IDM which reduces the authentication steps leading to improvement in mobile network bandwidth and availability. The IDM protocol also maximizes the load balancing to cope with social engineering attacks and to reduce network cost. It maintains transparency, confidentiality, and ID management in mobile network. The new method when compared to existing IDM3G has minimum MOs data throughput and overall network cost and improved MOs availability in mobile networks.

4.2 Privacy Preserving Security Frameworks for MCC

Security Framework of Group Location-Based MCC Chen et al. [5] proposed a scheme to preserve the identity of user accessing location-based services. They proposed a security scheme that uses location-based group scheduling service called *JOIN* [16] to address this security problem. The architecture of the proposed framework [5] is illustrated in Fig. 1.7.

The *JOIN* system has three main components: (a) mobile devices/mobile users, (b) JOIN server, and (c) cloud database. *JOIN* server stores user data, friends around mobile user, and also handles the authentication of users. On the other hand, location information, services, and information about devices are stored in cloud database. Initially, the user gets registered with the *JOIN* system to start using its services. The mobile device transmits user identification, password, group name, and a key (K_A) to $JOIN$ server for registration. The key (K_A) is generated by applying a hash function on the international mobile subscriber identity $(IMSI)$. $(K_A) = H(IMSI)$. The *JOIN* server stores this information and generates a