Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH Open Access

Energy-efficient service-oriented architecture for mobile cloud handover

Qassim Bani Hani* and Julius P. Dichter

Abstract

Mobile cloud computing uses features to deliver outsourcing data to remotely available mobile devices. However, the flexible nature of the mobile device is a critical challenge for the mobile cloud computing environment. The mobile phone significantly degrades the data transfer performance when initiating the handover process. Thus, an energy-efficient handover process could improve the quality of service (QoS). Here, we introduce a secure energy-efficient and quality-of-service architecture (EEQoSA) for the handover process in the mobile cloud computing environment. The proposed architecture involves four layers: application, the Internet protocol multimedia subsystem (IPMS), communication, and media with connectivity layers.

These four layers collectively handle the energy-efficiency, security and QoS parameters. Existing service-oriented architectures designed for mobile cloud computing are based on the symmetric encryption cryptography to support different media services. However, this approach easily allows an adversary to expose the symmetric key and gain access to private data. Thus, our proposed architecture uses the secure and strong authentication (SSA) process at the IPMS layer by protecting the media services from unauthorized users, as the IPMS is the central layer that could be the entry point for an adversary. Furthermore, to extend the mobile lifetime during the handover process, an energy detection (ED) model is deployed at the communication layer to detect the energy level of the mobile device prior to the handover initialization process. The media with the connectivity layer supports the secure handover process using a priority enforcement module that allows only legitimate users to complete the re-registration process after initiating the handover. Finally, the architecture is tested using the CloudSim simulation environment and validated by a comparison with other known service-oriented architectures.

Keywords: Mobile cloud computing, Efficient handover process, Service-oriented architecture, Energy detection, Secure and Strong authentication priority enforcement module

Introduction

Mobile cloud computing is an evolving platform in which data storage and data handling are performed outside of the mobile device [1]. Mobile cloud applications transport the data through the mobile device into the cloud servers, attracting many mobile subscribers [2]. Mobile cloud computing is promoted as a promising platform to support different media services [3, 4]. Additionally, the use of smartphones has increased the importance of mobile cloud computing considerably, as the data stored on the mobile cloud servers is easily accessible anytime and anywhere except network and services are unattainable. Today, the usage of mobile subscribers continues to increase due to the provision of new exciting features, such as GPS navigation, MP3, MP4, multimedia messaging services, dispatching emergency responders, Bluetooth, built-in projector personal digital assistant functions, streaming video, camcorders, memory card readers, and instant messaging [5, 6]. These additional smartphone features have been utilized to facilitate the acquisition of outsourcing data (e.g., contractual-execution for the exchange of agreed services) from mobile cloud servers. However, mobility is one of the key challenges for mobile cellular phones [7, 8]. This issue is apparent when

* Correspondence: qbanihan@my.bridgeport.edu
Department of Computer Science & Engineering, University of Bridgeport, Bridgeport, CT 06604, USA

a mobile device initiates the handover process, which leads to a reconnection process and in turn to additional energy being consumed. In addition, the data-exchange performance may degrade or be hacked by an attacker because the attacker can install its malicious node into the entry point of the access point (AP) or base station (BS). Thus, the mobility management process should be properly addressed prior to accessing the mobile cloud computing environment [9, 10]. Several mobility management approaches have been proposed to handle the handover process in cloud computing [11–13]. However, these existing approaches still use the traditional methods to obtain the cloud services from the servers. As a result, excess energy consumption and quality of service (QoS) degradation occur.

Handover management and interference mitigation problems for the mobile cloud computing environment were examined in [14]. Thus, a low-complexity management approach is introduced to combine the cloud radio access network with small cells. Fast mobility Internet Protocol version-6 (FMIPv6) was introduced to handle the handover process in mobile cloud computing [15]. The protocol reduced the handover latency and packet loss using buffering and tunneling procedures. As a result, these mechanisms work well in the ad hoc wireless network but could suffer in the mobile cloud computing environment [16–18]. A service-aware location updated paradigm was introduced to identify the frequency and location of mobile devices without using the periodic registration update (PRU) [19]. A service-oriented architecture was introduced for the heterogeneous cloud network to handle the handover management process, which combines the features of cloud computing and the heterogeneous small cell network. However, the architecture particularly focuses on the cloud computing extenuation management process. A robust architecture that can improve the handover process in the mobile cloud computing environment is urgently needed [20]. Furthermore, adversaries attempt to attack sensitive data during the handover process and slow down the services [21, 22]. As a result, the privacy, integrity and authentication of the legitimate users are compromised [23]. Secure packet authentication was introduced to restrict the access of adversaries to mobile cloud computing during the handover process. However, such authentication provides minimal user-privacy support [24]. The architecture attempts to reduce the handover computational cost but not the energy consumption. Existing proposed mechanisms for the handover process in mobile cloud computing focus on reducing the computational cost, flow of the media contents and network connectivity. Hence, the architecture must properly support the energy-efficient handover process while maintaining secure communications and improving the QoS parameters in mobile cloud computing.

Thus, we introduce a state-of-art, service-oriented architecture comprised of four layers: application, the Internet protocol multimedia subsystem (IPMS), communication and media with connectivity. These four layers collectively help the mobile device access the cloud computing resources efficiently. Furthermore, this paper presents a priority enforcement module, which allows only legitimate users to complete the re-registration process after initiating the handoff and thus enables reliable data access and content delivery. A substantial amount of energy and bandwidth are saved through the fast and seamless handoff process. Furthermore, this paper outlines the secure and strong authentication (SSA) to secure the services available on the IPMS layer (e.g., web, video-conference, video-on-demand, Internet, fax, email, telephone, and voice over IP service). In addition, the SSA helps store the key on different mobile clouds, making it difficult for the attacker to break the key. Finally, this paper discusses the energy detection model that calculates the energy consumption of the mobile device when initiating the handoff (as this model provides the updated energy status of the mobile phone). The remainder of this paper is organized as follows: Energy-efficient, service-oriented architecture section presents the energy-efficient, service-oriented architecture designed for the handover process (including the strong secure authentication and priority-based module), Experimental setup and simulation results section presents the simulation results and analysis, and the paper is concluded in Conclusion section.

Energy-efficient, service-oriented architecture

Mobile cloud computing aims to provide mobile devices with appropriate and rapid access to the data on the mobile cloud server. The handover process is one of the major challenges in the mobile cloud computing environment. The mobile handover process introduces problems because of the limited energy, restricted processing capability, wireless connectivity, and security threats. As a result, these factors could lead to performance degradation [25]. Furthermore, low-bandwidth and less reliable transmission can affect the handover process and thus have a significant effect on the QoS [26, 27]. The security threats caused by the handoff process affect several functions of mobile applications. Therefore, maintaining the confidentiality and privacy in mobile

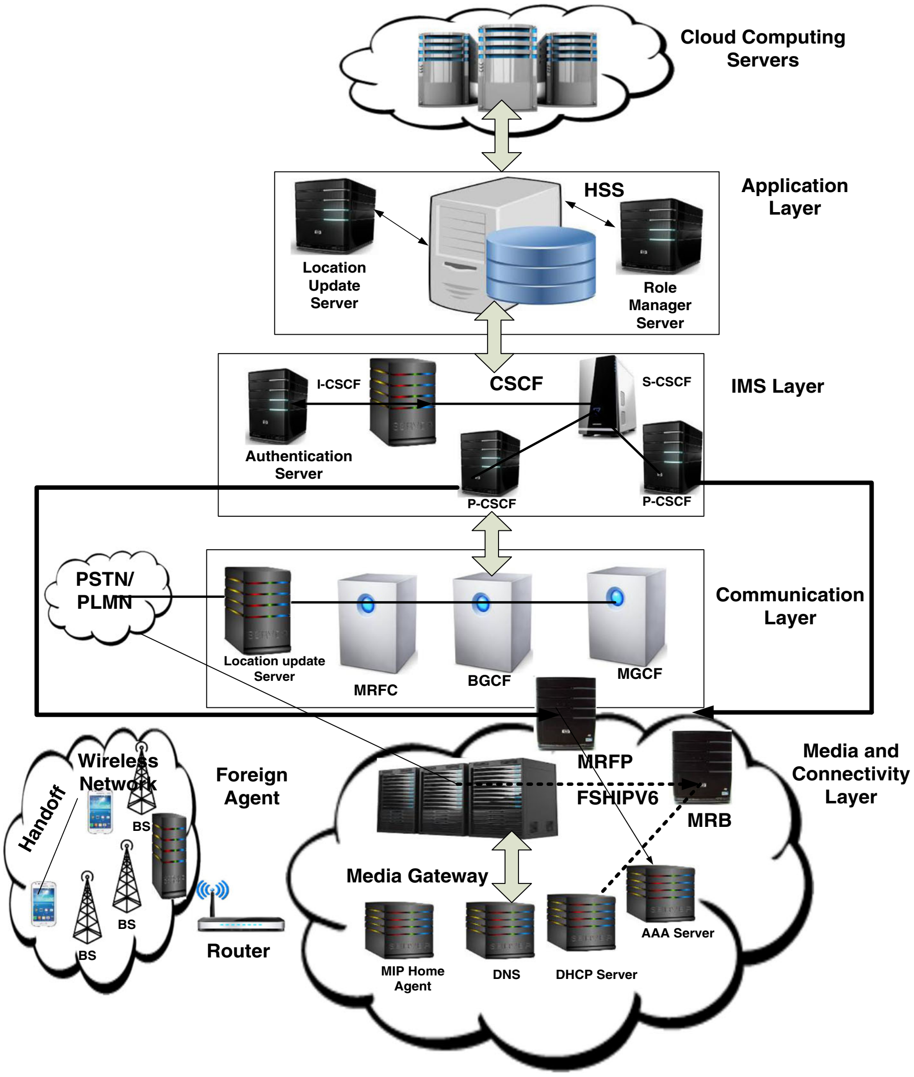

Fig. 1 Secure, energy-efficient and quality-of-service-supported service-oriented architecture

cloud computing is unpredictable. Thus, there is a high demand for secure and energy-efficient architectures to support the handover process in the mobile cloud computing environment. Understanding such an important need for a secure and energy-efficient handover and maintaining these apprehensions as the top priority, we introduce an energy-efficient and secure service-oriented architecture to support an effective handover that evades data loss and security concerns. The architecture is composed of four layers, as shown in Fig. 1.

- Application layer
- IPMS layer
- Communication layer
- Media with connectivity layer

Application layer

This layer constitutes the home subscriber server (HSS) that interconnects with the cloud computing servers as an enterprise server. The HSS also links to the IPMS layer to successfully maintain data communication. The HSS involves the subscription-related information (SRI) server, location update (LU) server and role manager server. The mobile cloud user profiles are stored in the SRI, and the LU stores the mobile cloud user's current location. Prior to transferring the cloud data to a legitimate mobile cloud user, encryption is performed for secure data communication. The attribute-based model is used to support the HSS encryption at the application layer.

Internet protocol multimedia subsystem (IPMS) layer

The IPMS layer offers utility services, such as web-browsing, video-on-demand, videoconferencing, fax, email, Internet, and voice over IP (VoIP) service. The IPMS involves the registration process, which helps obtain updated location information from the mobile cloud user. The IPMS uses a call session control function (CSCF) to bind a public user identity to the IP address of a mobile cloud user.

The IPMS offers exceptional expediency for individual and business cloud users. Tractability and expandability would permit retailers to bring new cloud services online as those services develop and advance without compelling subscribers to change carriers often. The mobile cellular phone may change location rapidly, resulting in frequent session handoff. The current handoff mechanisms do not properly support different services that bring unnecessary energy consumption and degrade the different QoS requirements during the handoff process. We apply a multi-service handoff mechanism that applies the list method of the Session Initiation Protocol (SIP) to keep all services active during the handoff. Furthermore, our protocol provides seamless mobility support for mobile cloud users that request real-time services (such as streaming, VoIP, and shared game playing). Thus, rapid and seamless handovers for the MIPv6 (FSMIPv6) are used to reduce the packet loss and extend the handover latency. The CSCF consists of the following components:

- Proxy-CSCF (P-CSCF)
- Serving-CSCF (S-CSCF)
- Interrogating-CSCF (I-CSCF)

Proxy-CSCF (P-CSCF)

The session initiation protocol proxy is the entry point to be used to connect with the IPMS layer. The P-CSCF can be used with either a foreign network or home network. The P-CSCF is comprised of the session frame controller (SFC), which is used to establish the user network interface. Hence, the features of the SFC help protect the IPMS. The P-CSCF is assigned to the IPMS prior to registration and is not altered during the entire process. The P-CSCF also accepts the encrypted signal and declines the unencrypted signal to help protect the communication. Furthermore, the P-CSCF consists includes a policy decision function, which helps maintain the QoS of the media resources. The policy decision function fully organizes the bandwidth utilization.

Serving-CSCF (S-CSCF)

The S-CSCF controls the session and is fixed in the home network. It maintains the registration process and sets the timer by involving two significant features. First, the S-CSCF provides the interface used to download the profile of mobile cloud device and makes the implication. Second, it supports the trail of the signaling messages and monitors all of the traffic for the locally registered mobile cloud devices. The S-CSCF has decision capability regarding the handover and directs and manages the policy of the network operation.

Interrogating-CSCF (I-CSCF)

The I-CSCF acts as an alternate SIP. It is responsible for sharing the identity with the domain name system (DNS). The I-CSCF also includes two components: the profile record (PR) and the name controlling pointer (NCP). Both of these components are used to determine the available remote cloud server, which facilitates the registration process for the SIP packets. Furthermore, the PR has the additional task of stipulating the data in a DNS, which traces an appropriate port number and hostname of the particular service when a mobile cloud device initiates the handover process. The I-CSCF also forwards the SIP request to the S-CSCF to refresh the exiting registration process and informs the network of the updated status of the mobile cloud device. Therefore, the mobile cloud device is able to complete the re-registration process efficiently.

The secure and strong authentication (SSA) process is used in this layer to protect the web, videoconferencing, video-on-demand, Internet, fax, email, telephone, and VoIP services. The authentication process is performed using the SSA algorithm. The cloud service server only has an idea about the encryption but requires full authentication support to protect different types of services. The authentication key is fragmented and stored on different cloud servers, making it difficult for an adversary to collect all the fragmented parts to access the services. Even if the adversary obtains all pieces of the key, it is incapable of recognizing the key patterns used. The SSA can easily secure our services and confidential data from the adversary in mobile cloud computing. When a mobile user intends to gain access to the service in this strong authentication process, the key from the cloud service server is required. The key acquisition process is detailed in Algorithm 1.

Algorithm 1: Key acquisition process using the SSA

```
1.  Initialization: { $U_i$= user, $C_{ss}$ = cloud service server
    $A_s$ = authentication server, $M_{cu}$: mobile cloud user, $L_{mcu}$: legitimate mobile
    cloud user; S: services}

2.  Input: { token,$C_{ss}$}
3.  Output: {S}
4.  $M_{cu}$ requests =>$C_{ss}$ // The mobile cloud user requests an authentication
    process to be performed by the cloud service server
5.  $C_{ss}$ forwards =>$A_s$// The cloud service server redirects the request of the
    mobile cloud user to the authentication server
6.  $A_s$ issues token =>$M_{cu}$// The authentication server issues the token to the
    mobile cloud user if it is a legitimate mobile cloud user
7.  $M_{cu}$maps token to $C_{ss}$ // The issued token is compared with the profile of the
    mobile cloud user
8.  Set access to $C_{ss}$ // Access is given to different cloud service servers to collect
    the keys to use for authentication purposes in steps 9–11
9.  Key $_1$ =>$C_{s1}$
10. Key $_2$ =>$C_{s2}$
11. Key $_3$ =>$C_{s3}$
12. If $M_{cu} \in L_{mcu}$ then // If the keys collected by the mobile cloud user are
    authentic, then access is granted for the service in step 13; otherwise, it is
    denied in step 14
13. Grant access to S otherwise
14. Deny S
15. end if
```

The authentication process starts with the request of the mobile cloud user. The request is sent to the cloud service server (main server). Upon receipt of the request, the cloud service server redirects it to the authentication server, and the authenticity of the mobile cloud user is verified based on the stored profile on the authentication server. If the mobile cloud user is found to be a legitimate user, then the server issues the token; otherwise, the request is dropped, and the user is considered to be an adversary. If the mobile cloud user is legitimate, a token is given to the cloud service server. In response, the cloud service server checks the information and decides, based on that information, whether to grant the user access to other servers to collect the remaining segments of the key. If the mobile cloud user is illegitimate, then it blocks the user. If the mobile cloud user possesses the valid key, and the key from the user matches the cloud server, then the cloud service server provides the user with access to use the resources. The complete SSA process is shown in Fig. 2.

Communication layer

This layer routes the data and synchronizes the media and IPMS layers. It consists of the media gateway controller function (MGCF), media resource function controller (MRFC) and breakout gateway control function (BGCF). The BGCF acts as the SIP proxy, which is responsible for processing the request to route the data from the S-CSCF whenever it determines that a session cannot be established using a DNS. Furthermore, the BGCF contains the routing features based on the telephone records.

The MGCF is considered as the SIP endpoint and manages the call exchange between the bearer-independent call control (BICC) and SIP. The MRFC is the signaling component that infers information looming from the S-CSCF with an application server (AS) to manage the MRFP. During this process, determination of the energy consumption is of high significance to route and synchronize the data. Furthermore, the location update server initiates the re-registration process, which is comprised of two levels: periodic re-registration (PRR) and re-

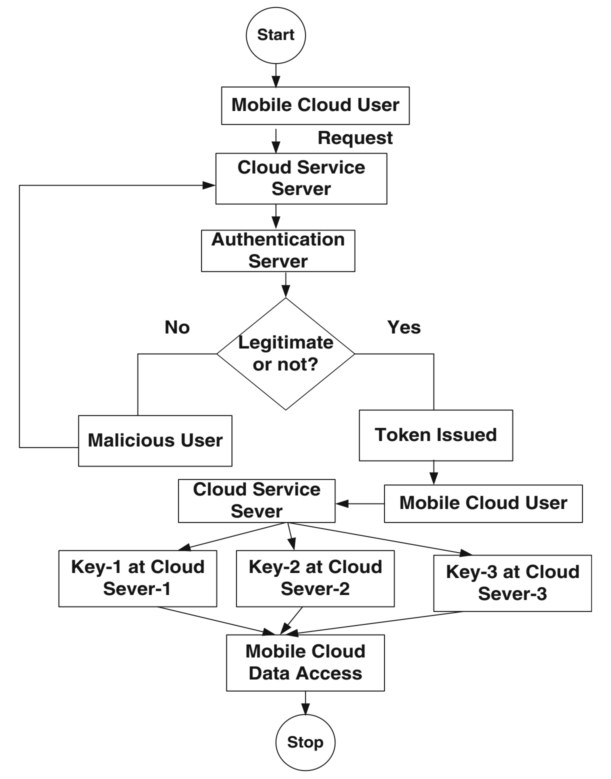

Fig. 2 Secure and strong authentication process for mobile cloud computing

registration for change capabilities (RRCC). The PRR and RRCC levels involve the messaging process to complete the re-registration. Hence, the energy for the re-registration process should be calculated after completion of the handover process to help determine the remaining power of the mobile device.

Energy Consumption for the Re-Registration Process

When the mobile device initiates the handover process, the re-registration and re-attachment processes with a new AP require a sufficient energy level to complete the handover process. When the distance between the mobile phone and its old attached AP 'A_p' is smaller than the threshold distance 'Th_d', the energy consumption of the mobile device should be counted before the handover completion process. Hence, we first determine the energy of the mobile device prior to the handover process.

$$E_{in1} = D_s \left\{ \pi' Th_d^2 \gamma P_s + \sum_{i=0}^{\pi' Th_d^2 \gamma} \in \beta \left(A_x - A_i\right)^2 + \left(B_x - B_i\right)^2 \right\} \tag{1}$$

When the distance between the mobile phone and its old attached AP 'A_p' is larger than the threshold distance 'Th_d', the energy consumption for the package transmission by the mobile device can be calculated using Eq. (2). Eq. (2) is the exponential time of Eq. (1). Reducing the time needed to perform the handover process can lower the energy consumption.

$$E_{ah1} = D_s \left[\Psi - \pi' Th_d^2 \gamma P_s + \sum_{i=0}^{\Psi - \pi' Th_d^2 \gamma} \in \rho \left\{ \left(A_x - A_i\right)^2 + \left(B_x - B_i\right)^2 \right\}^2 \right] \tag{2}$$

Equations (3) and (4) describe the energy consumed from the mobile nodes to receive the RESPONSE message from the APs/BS. The condition of receiving the range of APs/BS is similar to receiving the RESPONSE message. Thus, Eqs. (3) and (4) are related to the receiving energy. We can determine when the mobile device is far from the APs/BS when the number of long-distance handovers is twice the number of mobile devices. The conclusions drawn from Eq. (3) are well established.

$$E_{in2} = D_s \left\{ \pi' Th_d^2 \gamma P_r + \sum_{i=0}^{\pi' Th_d^2 \gamma} \in \beta \left(A_x - A_i\right)^2 + \left(B_x - B_i\right)^2 \right\} \tag{3}$$

After the second handoff process, several mobile devices can join the nearest AP or BS.

$$E_{ah2} = D_s \left[\left(\Psi - \pi' Th_d^2\right) \gamma P_r + \sum_{i=0}^{\Psi - \pi' Th_d^2 \gamma} \in \rho \left\{ \left(A_x - A_i\right)^2 + \left(B_x - B_i\right)^2 \right\}^2 \right] \tag{4}$$

The mobile device requires re-registration and sends the control messages 'M_c', which consumes energy. Eq. (5) is used to calculate the energy consumption of the mobile cloud server and mobile device 'E_{ms}'. We measure the energy consumption of the mobile cloud server because the mobile cloud server could potentially run out of power and thus would not be able to deliver the data to the mobile device. Here, the APs/BS are independent in our calculation. Furthermore, the energy of the APs/BS is unbounded, which provides an indication of the broadcasting and receiving energy such that a calculation is not required.

$$\begin{aligned} E_{ms} = M_c \Big[& \Psi (1 - w_t) \gamma P_s + \Psi * w_t * \gamma P_r \\ & + \sum\nolimits_{i=0}^{\Psi(1-w_t)\gamma} \in \beta \left(A_y - A_i\right)^2 + \left(B_y - B_i\right)^2 \Big] \end{aligned} \tag{5}$$

By combining Eqs. (1), (2), (3), (4) and (5), we obtain the total energy consumption 'E_t' from the mobile device and cloud mobile server while initiating the handover process.

$$E_t = (E_{ms} + E_{ah1} + E_{ah2} + E_{in2} + E_{in1}) \tag{6}$$

A description of the notations is given in Table 1.

Media with connectivity layer (MCL)

This layer offers media- and connectivity-related functionalities (e.g., voice stream and tome, including rapid handover). The MCL is comprised of the media resource function controller (MRFC) and the media resource agent (MRA). The MRFC mixes the media streams and handles the shared resources. The MRA controls the existing media resource function information and forwards the appropriate information to the authentication server. The MRA also contains queries and in-line modes. In the query mode, the MRA organizes the calls by obtaining the reply of the in-line mode and media resource function. Furthermore, the MRA enables the SIP request. Thus, the handover process is managed effectively. The MRFC and MRA modules are interrelated with IPv6 to ensure proper handover. Additionally, the MRA is coupled to the Dynamic Host Configuration Protocol (DHCP) server to support the handover process, as shown in Fig. 3. The media gateway is linked with the DNS. The MRFP is connected to the authentication, authorization, and accounting (AAA) servers. We deploy a rapid, seamless handoff process for the mobile cloud user for QoS provisioning. The priority enforcement module (PEM) provides the context-based administration to apply the application-layer security and arrangement. It also enforces the network access procedures and guidelines based on the mobile cloud service user roles, app flows, device types and location. Furthermore, the PEM offers user-level responsiveness for all traffic across the network.

Table 1 Notations used in this work and their descriptions

Notation	Description
E_{in1}	Energy of the mobile device before the first handover process
D_s	Data sent
Th_d	Threshold distance
γ	Number of mobile nodes accessing the same BS or AP for registration
P_s	Packet size sent by the sender
P_r	Packet size sent by the receiver
β	Number of mobile devices in the range of APs/BS that want to initiate handover
A_x, B_x	Location information of the AP/BS
A_i, B_i	Location information of the nodes
Ψ	Range of the APs/BS
E_{ah1}	Energy of the mobile device after the first handover process
ρ	Number of mobile devices in the range of APs/BS that want to initiate the re-registration process
M_c	Control messages
E_{ms}	Energy consumption of the mobile cloud server and a mobile device
w_t	Wait time for the re-registration process

Rapid, Seamless handover procedure

A mobile cloud device can change its attachment from its respective home domain. This could lead to re-attachment with another domain and the possibility of several handovers during the process. The handover process affects the QoS parameters including the end-to-end delay and packet loss. Handing this situation to the mobile cloud computing environment, we introduce the fast, seamless handover mobile IPv6 (FSHIPv6) to support the mobility management. The FSHIPv6 includes the mobility management utilities to reduce the unexpected signaling load within the intra domain when several mobile cloud users initiate the handover processes. As a result, the packet-drop and latency are greatly increased. In our approach, the handover process involves two states: periodic re-registration (PRR) and re-registration for change capabilities (RCC). In the PR, the mobile cloud device remains attached with same AP (AP)/BS to keep sending the data until it becomes attached with either another AP or BS. The timer is kept as active and ON during both steps. In the RCC, the mobile cloud user uses the utility features, and the attachment process is completed with another AP/BS.

The PR aims to identify whether the mobile cloud user is still registered with the home network. In this state, the home network begins the re-registration process because the registration timer has timed out. The RCC aims to intimate the change in the location of the mobile cloud user to the home network. During the re-registration process, the timer triggers the RCC, whereas the PR controls the changing parameters. The registration timer is required for both the RCC and PR to efficiently initiate the new session. In our proposed fast, seamless handover, the IPMS identifies the current registration status of the mobile cloud device. The process is also supported with the priority enforcement module (PEM) that reduces the traffic load when the handover is in progress, as this feature assigns the priority to each device based on the nature of the traffic. Furthermore, the IPMS also refreshes the registration timer during the session establishment process and cloud server-access. As a result, the time consumed for the PR can be reduced in our approach.

Experimental setup and simulation results

The performance of our proposed secure energy-efficient and quality-of-service architecture (SEEQoSA) is confirmed through the CloudSim simulation environment. The CloudSim simulator is installed on the Ubuntu Linux

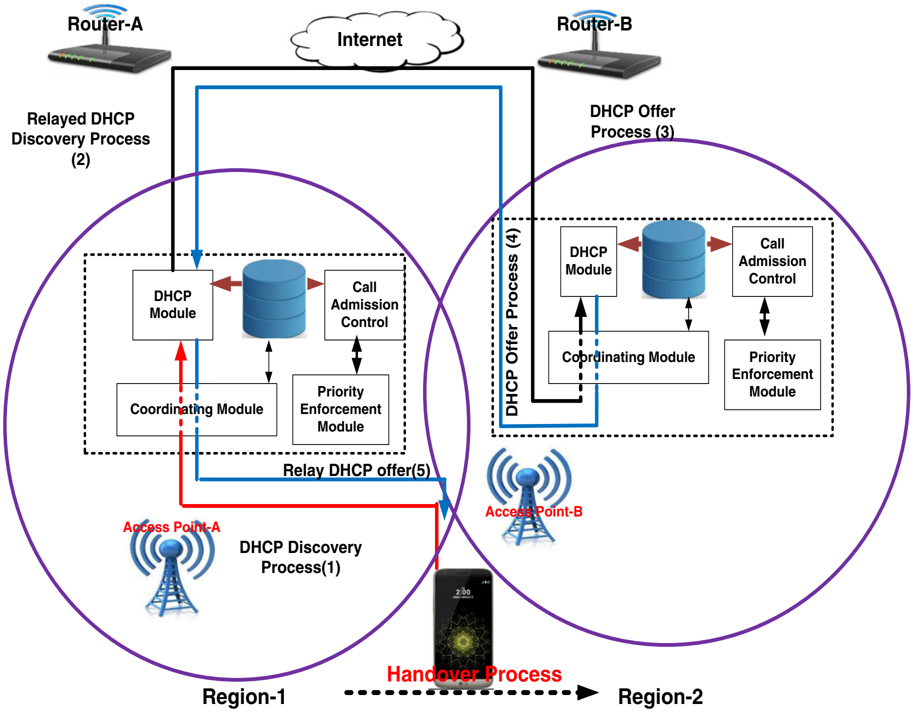

Fig. 3 DHCP server-supported handoff process

operating system. All the experiments are performed on a laptop with an Intel Pentium Dual-Core E6500 Wolfdale Dual-Core 2.93 GHz and 5 GB of RAM. The computing machine uses the 64-bit version of Windows 8.

The network size is approximately 1400 × 1800 m. At the application layer, 1900 chassis switches, 1452 line cards and 48 ports are deployed. At the IPMS layer, 230 chassis switches, 150 line cards, and 52 ports are used. A total of 64 servers with 20,000 mobile cloud devices are deployed and repeatedly perform the handover processes. Each mobile cloud device performs a maximum of 20 handover processes during the entire simulation time of 30 min. There are 256 and 16 racks deployed at the IPMS and application layers, respectively. Each rack consists of 128 hosts, and each host covers 16 processors with 164 GB of memory, 480 GB of storage, and a 300 GB of virtual disk space. We set a 280 GB bandwidth for the application layer, 100 GB for the IPMS layer, 20 GB for the communication layer and 7 GB for the media with the connectivity layer. The size of the packet with header is 1280 KB. Some of the parameters used are summarized in Table 2.

We analyzed the performance of the proposed (SEE-QoSA) that supports the handoff and then compared it with well-known service-oriented architectures designed for mobile cloud computing, including the market-oriented architecture for mobile cloud computing (MOMCC) [28], mobile cloud computing based on the

Table 2 Showing the simulation parameters and its description

Simulation parameter	Description
Machine	Intel Pentium Dual-Core E6500 Wolfdale Dual-Core 2.93 GHz
RAM	*5 GB*
Operating system	Windows 08 + *Ubuntu Linux*
Network size	1400 m × 1800 m
Chassis switches	1900
Line cards	1452
Ports	48
Servers	64
Mobile cloud devices	20000
Maximum number of handover	20
Simulation time	27 min
Racks at application layer	16
Racks at IPMS layer	256
Hosts	128 hosts in each rack
Processor	16 processors in each rack
Packet size	1280 KB
Processor memory	164 GB
Storage	480 GB
Virtual disk space	300 GB

service-oriented architecture (MCLSOA) [29], service-oriented heterogeneous resource sharing (SOHRS) [30], cloud-based semantic service-oriented content provisioning architecture (CSSCPA) [31] and the service-based arbitrated multi-tier infrastructure (SAMI) [32]. Based on the experimental results, the collected data were used in MATLAB to graph the following parameters:

- Energy Consumption
- Malicious Detection Probability
- Reliable Data Delivery
- Bandwidth Consumption
- Latency in the presence of a Malicious Node
- Average Throughput

Energy consumption

The lifetime of the networks depends entirely on the amount of energy available in the mobile phone [33, 34]. The lack of the energy significantly affects the performance and efficiency of the mobile cloud device including running applications on the cloud [35, 36]. Based on the experimental results, we observed that the energy consumption of the mobile devices increased when the mobile device initiated the handover process. The trend of energy consumption shows that our proposed SEEQoSA consumes overall less energy when compared with the SAMI, CSSCPA, SOHRS, MCLSOA and MOMCC approaches, as shown in Fig. 4. However, this impact of minor energy consumption in our case does not affect the mobile cloud data outsourcing and transfer because the mobile cloud device still has substantial energy to effectively perform its function. Our approach is particularly designed to support a wide-range of mobile devices. Most of the conventional approaches are not introduced to support the smaller number of mobile cloud users because many resources are required, making these approaches unsuccessful in real situations. Our SEEQoSA consumes 34.67 out of 50 Joules of energy after completing 4500 rounds for a maximum of 18 handover processes. On the other hand, other competing approaches consume 35.22–42.46 Joules with same number of handovers and rounds. The location update server is deployed with our approach to determine the location of the mobile device and to initiate the re-registration after the handover. As a result, the IPMS acquires the updated request from the top layer (application layer), which could save additional time and lead to a lower energy consumption.

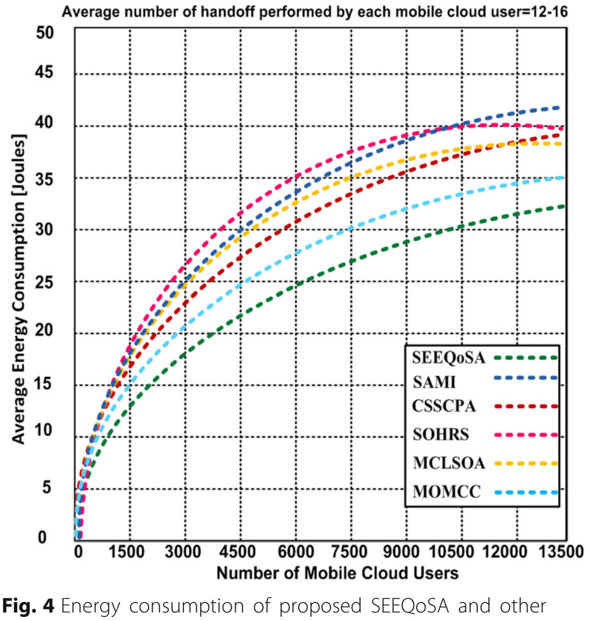

Fig. 4 Energy consumption of proposed SEEQoSA and other competing approaches

Malicious detection probability

Recently, the security of mobile cloud computing has been subjected to a high level of threat, leading to security cracks. Therefore, the probability of detecting malicious intent should be determined. We demonstrate the performance of our proposed SEEQoSA and its comparison with other competing approaches for malicious probability detection in Fig. 5. When the number of malicious mobile cloud users increased in this experiment, the malicious detection probability began to drop. However, our SEEQoSA approach had an edge over other contending approaches. The malicious detection probability decreased by only 5.36% with 108 malicious mobile cloud devices, whereas the malicious detection probability decreased by 10.86–18.24% for contending approaches. Therefore, these results indicate that our approach is superior to other approaches for detecting

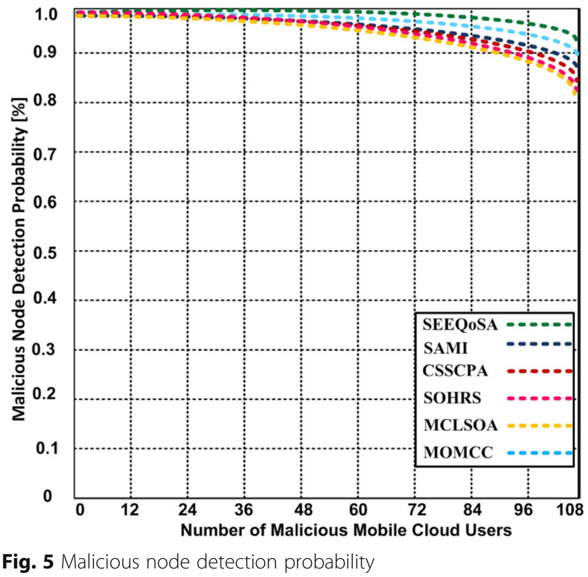

Fig. 5 Malicious node detection probability

malicious users. The secure and strong authentication algorithm in our approach provides privacy protection because the keys are fragmented and stored on different servers. Hence, it is more difficult for an adversary to gain access to all of the cloud servers. If any adversary tries to exploit the mobile cloud servers, then an adversary is recognized as an illegitimate user, and as a result, it is not permitted by the role manager. Therefore, the SSA helped to identify the probability of the malicious mobile device, whereas the contending approaches either deploy no proper secure authentication or apply fragile authentication mechanisms that can only secure the traditional networks but are not appropriate for mobile cloud computing [37, 38].

Reliable data delivery

There is a large probability of data loss when the mobile device initiates the handover process. The delivery of reliable data is of high significance because the performance of the architecture depends on how much data can be reliably delivered to the end user. The trends in the reliable data delivery for our proposed algorithm and other contending approaches are plotted in Fig. 6. The trend shows that the reliable data delivery of the SEEQoSA steadily evolves and ranges between 99.08 and 99.68% with 9000 mobile cloud devices and a maximum of 16 handovers. A lower reliable data delivery rate is observed for the competing approaches and ranges between 97.64 and 99.16%. In Fig. 7, we increased the number of mobile cloud devices up to 13,500; the data delivery rate is slightly reduced in our case to values of 98.74–99.45%, whereas the contending approaches have a rate of 95.23–99.17% in the same scenario with similar parameters. The results prove that our SEEQoSA outperforms other contending approaches in terms of the reliability of data transfer when the number of the mobile cloud devices increases.

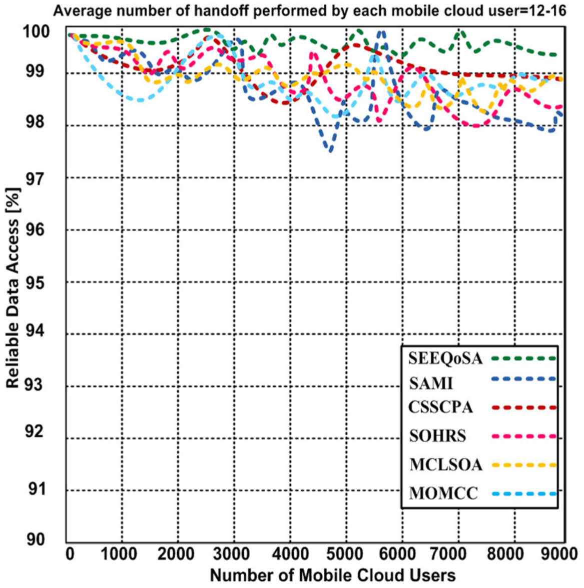

Fig. 6 Reliable data delivery of proposed SEEQoSA and other competing approaches with 9000 mobile cloud users

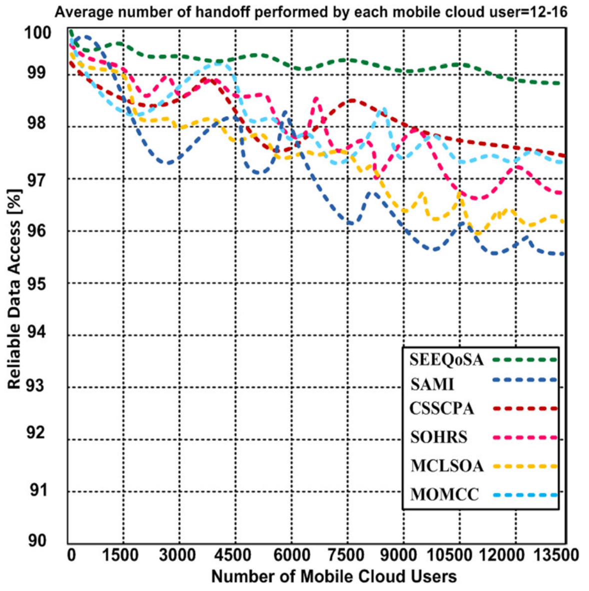

Fig. 7 Reliable data delivery of proposed SEEQoSA and other competing approaches with 13,500 mobile cloud users

Bandwidth consumption

We determined the bandwidth utilization of the SEEQoSA and compared it with those of the SAMI, CSSCPA, SOHRS, MCLSOA and MOMCC in Fig. 8. The SEEQoSA

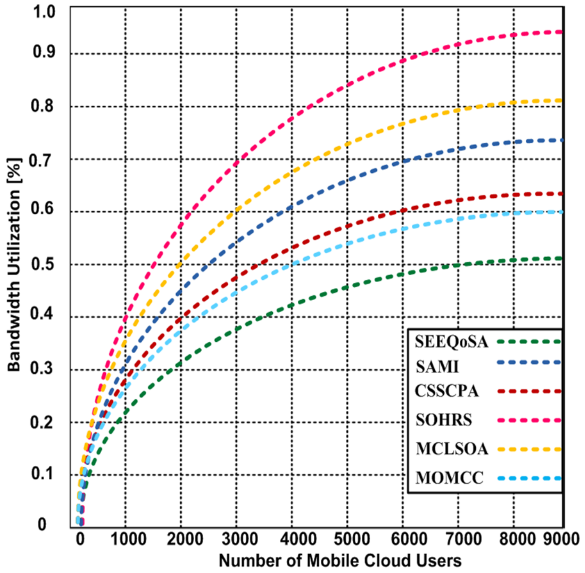

Fig. 8 Bandwidth utilization of proposed SEEQoSA and other contending approaches with 9000 mobile cloud users

consumes less bandwidth than the contending approaches during the mobile cloud handover initialization process. The results show that the bandwidth consumption increases with increases in the number of the mobile cloud devices. The bandwidth consumption of the other approaches depends on the number of available mobile cloud devices that attempt to initiate the handover and re-registration processes. The results confirm that the SEEQoSA approach consumes 53.07% of the total assigned bandwidth with 9,000 mobile cloud devices, whereas the competing approaches consume 59.8–94.37% of the entire assigned bandwidth. When we increase the number of mobile cloud devices to 13,500, the SEEQoSA consumes 56.3% of the bandwidth, whereas the contending approaches consume 73.98–99.24%, as shown in Fig. 9. The SOHRS had the greatest bandwidth consumption compared to the other approaches, and the SEEQoSA, which uses the simple registration process, had the lowest bandwidth consumption. The significance of the SEEQoSA is to incorporate the PEM, which assigns priority to the mobile cloud device when initiating handover based on the nature of the network traffic.

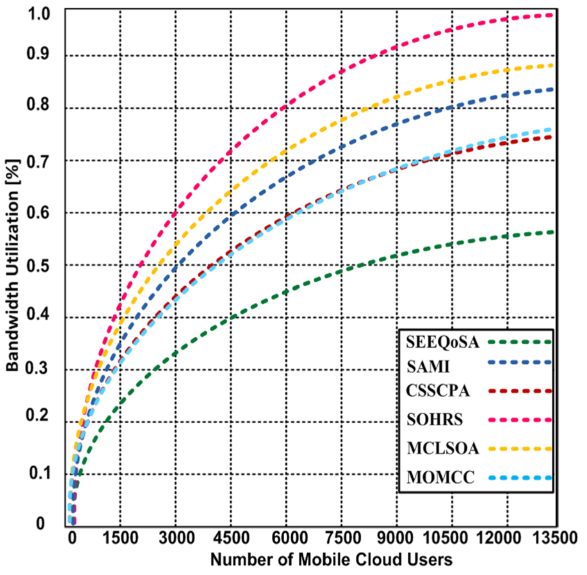

Fig. 9 Bandwidth utilization of proposed SEEQoSA and other contending approaches with 13,500 mobile cloud users

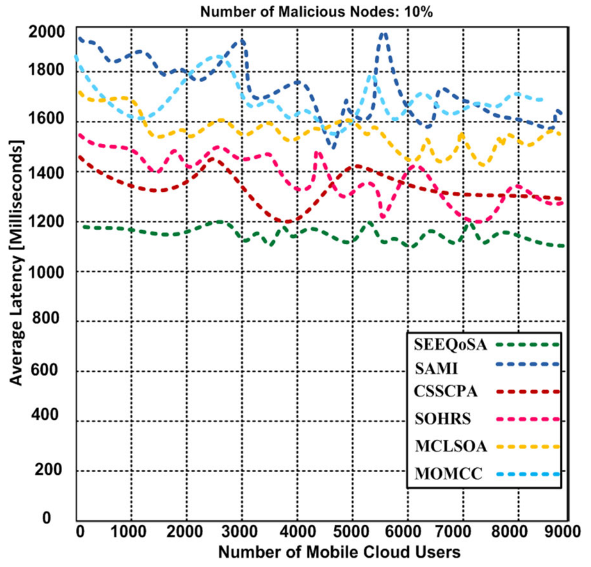

Fig. 10 Latency of our proposed SEEQoSA and other competing approaches: SAMI, CSSCPA, SOHRS, MCLSOA and MOMCC in presence of 10% malicious nodes

Latency in the presence of a malicious node

Cloud latency specifies the delay between a response of the cloud service provider and a client request and significantly affects the communication performance (which can be particularly susceptible to the latency for several reasons). The latency is less predictable but is difficult to determine in cloud computing. In Fig. 10, the latency of our proposed SEEQoSA is compared to those of other competing approaches (SAMI, CSSCPA, SOHRS, MCLSOA and MOMCC) with 10% of the nodes being malicious and attempting to affect the hops in the router. The simulation results indicated that our proposed SEEQoSA has a minimum latency of 1,150 ms (which is nearly stable for the cloud users), whereas the other competing approaches have a higher latency of 1,254–1,834 ms. Factors affecting the latency include the number of the hops in the router or ground-to-satellite communication hops that target the server. Thus, the latency can cause serious damage for multiple cloud services. Our approach is supported by the priority enforcement module and communication module, which help handle the flow of the packets and detect the malicious nodes available on each hop.

Average throughput

The key measurement of the network performance is the throughput. The throughput indicates the average amount of bandwidth data that can be transmitted through the network per unit time. Throughput is not always considered as a critical factor for cloud-based software applications [39]. The average throughput performance is shown in Fig. 11, illustrating that our proposed SEEQoSA has an advantage over other competing approaches. The SEEQoSA has a throughput of 3.9 MB/s, whereas the other approaches have throughputs of 3.01-3.46 MB/s. The SOHRS produced the minimum throughput among all the approaches. The improved throughput in our approach is due to the fast and seamless handoff based on the dynamic host configuration protocol (DHCP), which involves the new priority

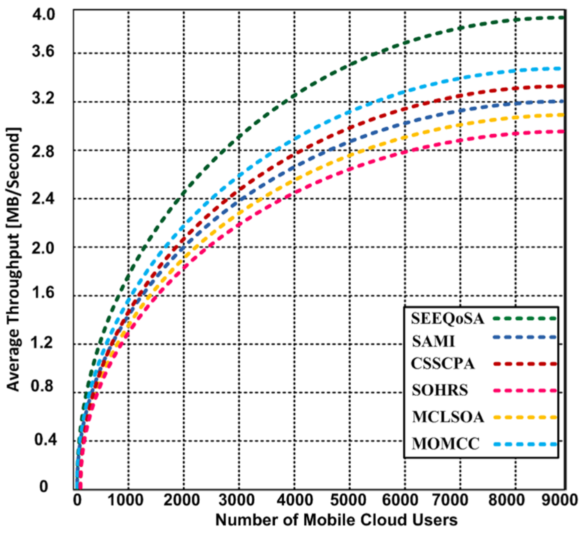

Fig. 11 An average throughput performance of our proposed SEEQoSA and other competing approaches: SAMI, CSSCPA, SOHRS, MCLSOA and MOMCC

enforcement module that allows only legitimate users to complete the re-registration process after initiating the handoff. This approach enables reliable data access and content delivery with a higher throughput.

Conclusion

This study introduced the SEEQoSA to achieve an efficient handover process in mobile cloud computing. The proposed paradigm consists of four layers: application, IPMS, communication and media with connectivity. The application layer serves as the enterprise server to control the operations of the other three layers. The IPMS provides different services, such as web, videoconferencing, and video-on-demand. The communication layer handles the faster re-registration process to avoid unexpected delays and data loss. Furthermore, the communication layer involves an energy-efficient detection model to determine the energy of each node when initiating the handoff process. The media with connectivity layer consists of the priority-based module, which allows only legitimate users to complete the re-registration process after initiating the handover and reduces the occurrence of extended delays during the handover. The architecture is implemented using C++, and the code is converted to the object tool command language (OTCL) run on the CloudSim platform. The results confirm the validity of our proposed architecture and comply with the QoS and energy-efficiency parameters. The architecture aims to facilitate energy-efficient and QoS-supported handoff processes. The simulation results validate that the SEEQoSA achieves a 5.5–12.8% higher malicious node detection probability with an 8.2–42.2% lower bandwidth consumption compared to other known approaches. The SEEQoSA consumes 0.67–7.87% less energy with 12–16 handover processes over 5,000 rounds. Furthermore, it has also a 0.7–1.4% higher data delivery rate compared to other service-oriented architectures.

The results confirm that the SEEQoSA is a more suitable choice for mobile phones when initiating the handover process in a cloud computing environment. In the future, we will determine possible malicious attacks on the SEEQoSA and will propose appropriate solutions.

Acknowledgements
We are also thankful to anonymous reviewers for their valuable feedback and comments for improving the quality of the manuscript.

Authors' contributions
This research work is part of QBH. dissertation work. The work has been primarily conducted by QBH under the supervision of JPD. Extensive discussions about the algorithms and techniques presented in this paper were carried between the two authors over the past year. Both authors read and approved the final manuscript.

About the Authors
Qassim Bani Hani is pursuing towards his Ph.D., Department of Computer Science and Engineering University of Bridgeport, Bridgeport, at the CT. Qassim's interests are in Cloud computing, Cloud computing mobility, and Cloud localization. He has authored and coauthored several technical refereed papers in various conferences, and journal articles. He is IEEE member.
Julius Dichter is an Associate Professor in the department of Computer Science and Engineering at the University of Bridgeport in Connecticut. He received his M.S. degree from the University of New Haven and the Ph.D. from the University of Connecticut in the area of parallel computing optimization. He has authored and coauthored several technical refereed and non-refereed papers in various conferences, journal articles, and book chapters in research and pedagogical techniques. His research interests include parallel and distributed system performance, security of the cloud computing, algorithms and object-oriented systems. Dr. Dichter is a member of IEEE, ACM, and ISCA.

Competing interests
The authors declare that they have no competing interests.

Publisher's Note
Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Received: 20 July 2016 Accepted: 28 March 2017
Published online: 18 April 2017

References
1. Yuan H, Kuo C-CJ, Ishfaq A (2010) Energy efficiency in data centers and cloud-based multimedia services: An overview and future directions. In: Green Computing Conference, 2010 International., pp 375–382
2. Shiraz M, Abdullah G, Rashid Hafeez K, Rajkumar B (2013) A review on distributed application processing frameworks in smart mobile devices for mobile cloud computing. Communications Surveys & Tutorials, IEEE 15 3:1294–1313
3. Rizvi S, Razaque A, Katie C (2015) Third-Party Auditor (TPA): A Potential Solution for Securing a Cloud Environment. In: Cyber Security and Cloud Computing (CSCloud), 2015 IEEE 2nd International Conference., pp 31–36
4. Razaque, Abdul, Syed S. Rizvi, Meer J. Khan, Hani QB, Dichter JP, Parizi RM (2017) "Secure and quality-of-service-supported service-oriented architecture for mobile cloud handoff process." Computers & Security 66:169-184
5. Othman M, Sajjad Ahmad M, Samee Ullah K (2014) A survey of mobile cloud computing application models. IEEE Communications Surveys & Tutorials 16 1:393–413

6. Wang S, Dey S (2013) Adaptive mobile cloud computing to enable rich mobile multimedia applications. IEEE Transactions on Multimedia 15(4):870–883
7. Shekhar S, Viswanath G, Michael RE, KwangSoo Y (2012) Spatial big-data challenges intersecting mobility and cloud computing. In: Proceedings of the Eleventh ACM International Workshop on Data Engineering for Wireless and Mobile Access., pp 1–6
8. Sanaei Z, Abolfazli S, Gani A, Buyya R (2014) Heterogeneity in mobile cloud computing: taxonomy and open challenges. IEEE Communications Surveys & Tutorials 16(1):369–392
9. Zhang H, Chunxiao J, Julian C, Victor CM L (2015) Cooperative interference mitigation and handover management for heterogeneous cloud small cell networks. IEEE Wireless Communications 22 3:92–99
10. Gani A, Nayeem GM, Shiraz M, Sookhak M, Whaiduzzaman M, Khan S (2014) A review on interworking and mobility techniques for seamless connectivity in mobile cloud computing. J Netw Comput Appl 43:84–102
11. Chiu K-L, Yuh-Shyan C, Ren-Hung H (2011) Seamless session mobility scheme in heterogeneous wireless networks. International Journal of Communication Systems 24 6:789–809
12. Ferretti S, Vittorio G, Fabio P, Elisa T (2010) Seamless support of multimedia distributed applications through a cloud. In: Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference., pp 548–549
13. Chen Y-S, Kun-Lin W (2011) A cross-layer partner-assisted handoff scheme for hierarchical mobile IPv6 in IEEE 802.16 esystems. Wireless Communications and Mobile Computing 11 4:522–541
14. Razaque A, Rizvi SS (2017) Privacy preserving model: a new scheme for auditing cloud stakeholders. J Cloud Comput 6:1–7.
15. Ryu S, Lee K, Mun Y (2012) Optimized fast handover scheme in Mobile IPv6 networks to support mobile users for cloud computing. J Supercomput 59(2):658–675
16. Keke G, Qiu M, Zhao H, Tao L, Zong Z (2016) Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing. J Netw Comput Appl 5:46–54
17. Rakpong K, Niyato D, Wang P, Hossain E (2013) "A framework for cooperative resource management in mobile cloud computing." IEEE J Sel Areas Commun 31;(12):2685–2700.
18. Lee D, Lee H, Park D, Jeong Y-S (2013) Proxy based seamless connection management method in mobile cloud computing. Clust Comput 16(4):733–744
19. Qi Q, Liao J, Cao Y (2014) Cloud service-aware location update in mobile cloud computing. Communications, IET 8(8):1417–1424
20. Qi H, Abdullah G (2012) Research on mobile cloud computing: Review, trend and perspectives. In: Digital Information and Communication Technology and it's Applications (DICTAP), 2012 Second International Conference., pp 195–202
21. Mayuri K, Ranjith KS (2014) A Novel secure handover mechansim in PMIPV6 networks. International Journal of Information Technology Convergence and Services 4(4):1
22. Razaque A, Saty Siva Varma N, Suharsha V, Dinesh Kumar A, Dammannagari Nayani R, Poojitha A, Divya V, Vamsee Sai M (2016) Secure data sharing in multi-clouds. In: Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference., pp 1909–1913
23. Rizvi S, Razaque A, Cover K (2015) Cloud Data Integrity Using a Designated Public Verifier. In: High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conferen on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference., pp 1361–1366
24. Suo H, Zhuohua L, Jiafu W, Keliang Z (2013) Security and privacy in mobile cloud computing. In: Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International., pp 655–659
25. Abolfazli S, Sanaei Z, Ahmed E, Gani A, Buyya R (2014) Cloud-based augmentation for mobile devices: motivation, taxonomies, and open challenges. IEEE Communications Surveys & Tutorials 16(1):337–368
26. Jiang Y, Hu X, Sen W (2014) Transformation Matrix for Time Discretization Based on Tustin's Method. Math Probl Eng 2014:9
27. Márquez-Barja J, Calafate CT, Cano J-C, Manzoni P (2011) An overview of vertical handover techniques:Algorithms, protocols and tools. Comput Commun 34(8):985–997
28. Abolfazli S, Zohreh S, Muhammad S, Abdullah G (2012) MOMCC: market-oriented architecture for mobile cloud computing based on service oriented architecture. In: Communications in China Workshops (ICCC), 2012 1st IEEE International Conference., pp 8–13
29. Gutierrez M, Andres F, Neco V (2011) Mobile Cloud Computing based on service oriented architecture: Embracing network as a service for 3 RD party application service providers. In: Kaleidoscope 2011: The Fully Networked Human?-Innovations for Future Networks and Services (K-2011), Proceedings of ITU., pp 1–7
30. Nishio T, Ryoichi S, Tatsuro T, NarayanB M (2013) Service-oriented heterogeneous resource sharing for optimizing service latency in mobile cloud. In: Proceedings of the first international workshop on Mobile cloud computing & networking., pp 19–26
31. Yee KY, Yilun C, Flora ST, Ang Wee T, Rajaraman K (2011) Cloud-based semantic service-oriented content provisioning architecture for mobile learning. Journal of Internet Services and Information Security 1 1:59–69
32. Sanaei Z, Saeid A, Abdullah G, Muhammad S (2012) SAMI: Service-based arbitrated multi-tier infrastructure for Mobile Cloud Computing. In: Communications in China Workshops (ICCC), 2012 1st IEEE International Conference., pp 14–19
33. Rizvi S, Karpinski K, Razaque A (2015) Novel architecture of self-organized mobile wireless sensor networks. J Comput Sci Eng 9(4):163–176
34. Razaque A, Elleithy KM (2014) Energy-efficient boarder node medium access control protocol for wireless sensor networks. Sensors 14(3):5074–5117
35. Guan L, Xu K, Meina S, Junde S (2011) A survey of research on mobile cloud computing. In: Computer and Information Science (ICIS), 2011 IEEE/ACIS 10th International Conference., pp 387–392
36. Kumar K, Yung-Hsiang L (2010) Cloud computing for mobile users: Can offloading computation save energy? Computer 43(4):51–56
37. Alizadeh M, Saeid A, Mazdak Z, Sabariah B, Kouichi S (2016) Authentication in mobile cloud computing: A survey. J Netw Comput Appl 61:59–80
38. Chow R, Markus J, Ryusuke M, Jesus M, Yuan N, Elaine S, Zhexuan S (2010) Authentication in the clouds: a framework and its application to mobile users. In: Proceedings of the 2010 ACM workshop on Cloud computing security workshop., pp 1–6
39. Razaque A, Rizvi SS (2016) Triangular data privacy-preserving model for authenticating all key stakeholders in a cloud environment. Computers & Security 62:328–347