Security and privacy issues in mobile cloud computing

SAURABH DEY
SRINIVAS SAMPALLI
Dalhousie University, Halifax, Canada

QIANG YE
University of Prince Edward Island, Charlottetown, Canada

Abstract
Mobile cloud computing facilitates "anytime, anywhere" remote accessibility to users with a plethora of services, such as PaaS (platform as a service), SaaS (software as a service), and IaaS (infrastructure as a service). Ease of use, mobility and the absence of globally accepted standard data access/security protocols make the mobile cloud susceptible to different types of attacks. The advent of smartphones and the widespread use of other mobile devices such as tablets have introduced a new dimension to cloud computing, offering a higher degree of flexibility in data access, and with it has increased the need for security standards. Unlike other issues, security and privacy are crucial when associated with business requirements, financial transactions, and health care. Studies indicate that existing cloud services can suffer from numerous security and privacy issues, such as MITM (man-in-the-middle), DDoS (distributed denial of service), data theft, data compatibility, and information leakage. The objective of this paper is three-fold. Firstly, we highlight the importance of security and privacy issues in cloud computing in general, and in mobile cloud computing in particular and survey the literature in this area. Secondly, we outline and discuss four strategies, namely, refined policy, compatible software and interfaces, authentication and security audit, as means to mitigate threats to the mobile cloud platform. Thirdly, we present a novel authentication scheme called MDLA (message digest and location based authentication) for mobile cloud computing, which ensures secure mutual authentication between a registered mobile device and a cloud server. The technique is lightweight and is independent of device-specific properties.

Keywords
Cloud computing, vulnerability, authentication, mobile, privacy, security, threat mitigation

1. Introduction

Let us begin with a small fictitious story that serves as an introduction to mobile cloud computing. Emily is a budding entrepreneur who has recently started a small data analytics company to provide financial insights and financial data management to other companies. Emily has to process large sets of sensitive data that help in understanding business trends and growth of a particular business establishment or product over a specific period of time. Since Emily is a new entrepreneur with limited capital, she cannot afford to purchase large storage servers, application servers, analytics tools, platforms and other necessary hardware to perform the data processing. An attractive solution for Emily is cloud computing. She rents an operating system, data analytics and visualization tools, and processing power from a cloud service provider and starts to deliver financial solutions to her clients. Her company receives requests

from clients to process huge amounts of data frequently, for which she uses cloud resources to analyze data and generate reports. However, renting resources from a cloud service provider and processing data alone is not enough to serve her clients. Her clients need full control on the entire analytics process and a mobile solution with which their employees can perform analytics any time anywhere. Therefore, Emily wants to provide her clients direct access through personal computers, tablets, smartphones, and other mobile devices to cloud resources. In short, her company needs to design and develop a mobile cloud computing platform.

Cloud computing provides numerous customized services, such as PaaS (platform as a service), SaaS (software as a service), and IaaS (infrastructure as a service) (Yoo et al. 2012, Yandong et al. 2012). These services have helped many small and mod size business organizations in reducing their infrastructure costs as the pay per use model is less expensive than purchasing new hardware or storage devices. Mobile cloud computing can be defined as a computing environment where mobile devices communicate with cloud services for data processing. The aforesaid services are crucial for a mobile user who accesses cloud infrastructure for data (e.g., big data) analytics and visualization. Since mobile devices lack sufficient computational power and battery life, it is desirable to perform much of the resource intensive tasks at the cloud server. The mobile device can then be used mainly as a medium for transferring data or as a viewer for visualizing the final results. Mobile cloud computing can help a user perform a complicated task, such as big data analytics remotely irrespective of the geographical location.

IDG enterprise's recent study on cloud usage (IDG Enterprise Marketing 2015) indicates that 72% of the organizations have at least one cloud application running or they are utilizing some portions of the cloud infrastructure. The market of cloud usage is growing and many business players are leaning towards cloud computing.

International Data Corporation (IDC 2016) has released a quarterly data of the cloud revenue for private and public clouds based on the data available from IDC's Worldwide Quarterly Cloud IT Infrastructure Tracker. This tracker provides information about the number of servers, storage disks and Ethernet switches that are deployed in the cloud environment. According to IDC, the vendor revenue of sales of cloud IT infrastructure products grew 21.9% year over year to $29.0 billion in 2015. Table 1 highlights the cloud IT infrastructure vendor revenue and market share growth for the fourth quarters of 2014 and 2015.

The overall growth of revenue indicates the increased usage of cloud resources. In addition, the usage of mobile devices, such as smartphones, tablets, and sensors is increasing every year. Fig. 1 (Statista.com 2016) shows the total number (in millions) of smartphone users and projected smartphone users worldwide from 2014 to 2019. The increased usage of smartphones and cloud resources has triggered the use of mobile cloud computing. Online gaming, audio-video streaming, online storage, web browsing, social networking are various forms of mobile cloud computing that are performed by smartphones or tablets. According to a study conducted by Cisco (2016), by 2020 the mobile data traffic is expected to reach 30.6 Exabytes (one Exabyte = 10^{18} bytes) per month at a CAGR (compound annual growth rate) of 53% from 2015 to 2020.

Table 1: IDC, April 2016 fourth quarter revenue data for 2014 and 2015

Top 5 Corporate Family, Worldwide Cloud IT Infrastructure Vendor Revenue, Q4 2015 (Revenues are in Millions, Excludes double counting of storage and servers)					
Vendor	4Q15 Revenue (US$M)	4Q15 Market Share	4Q14 Revenue (US$M)	4Q14 Market Share	4Q15/4Q14 Revenue Growth
1. Hewlett Packard Enterprise	$1,304	15.80%	$1,112	15.60%	17.20%
2. Dell*	$845	10.20%	$667	9.40%	26.70%
2. Cisco*	$802	9.70%	$591	8.30%	35.50%
4. EMC	$759	9.20%	$634	8.90%	19.70%
5. IBM	$352	4.30%	$345	4.80%	2.10%
ODM Direct	$1,927	23.40%	$2,138	30.00%	-9.90%
Others	$1,328	27.40%	$1,640	23.00%	37.80%
Total	$8,248	100%	$7,126	100%	15.70%
IDC's Worldwide Quarterly Cloud IT Infrastructure Tracker, April 2016					

Security and privacy stand out as critical issues in the design and deployment of mobile cloud computing. These are especially important in mobile commerce and healthcare applications that are characterized by sensitive and time-critical information transfers, thereby requiring not only guaranteed information transfer security but also data and user privacy. This design challenge stems from a number of factors. Firstly, a common characteristic of mobile devices is their severe resource constraint, since such devices may consist of small sensors or chips with limited computational power and bandwidth. This makes the deployment of sophisticated and advanced cryptographic algorithms infeasible. Secondly, deploying security has always been a bigger challenge in mobile devices as compared to their wired counterparts, due to their inherent free space and broadcast transmission, as well as protocol vulnerabilities. Secondly, non-uniform traffic, unpredictable topology changes, differing node densities, high degree of mobility, and high bit-error rates dictate communication between mobile devices and the cloud. Thirdly, the misplacement of a mobile device by a client who uses cloud infrastructure for sensitive and economic data processing can lead to a high probability of theft of data downloaded from the cloud on to the mobile device.

The objective of this paper is three-fold. Firstly, we highlight the importance of security and privacy issues in cloud computing in general, and in mobile cloud computing in particular and survey the literature in this area. Secondly, we outline and discuss four strategies, namely, refined policy, compatible software and interfaces, authentication and security audit, as a means to mitigate threats to the mobile cloud platform. Thirdly, we present a novel authentication scheme called MDLA (message digest and location based authentication) for mobile cloud computing, which ensures secure mutual authentication between a registered mobile device and a cloud server. The technique is lightweight and is independent of device-specific properties.

This paper is organized as follows. Section 2 explores literature related to security and privacy issues that can affect a mobile cloud computing environment, and Section 3 describes

the various ways of mitigating intrusions. Section 4 describes a lightweight authentication scheme for mobile cloud computing for end-to-end security. Section 5 provides a discussion of the proposed scheme in the context of mobile cloud security. Section 6 concludes the paper.

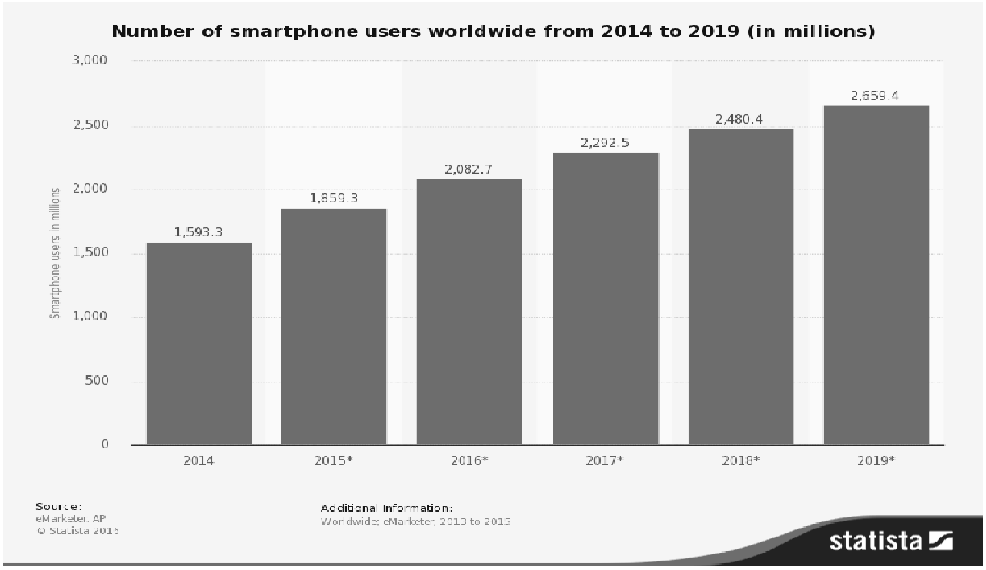

Fig. 1: Smartphone users (in millions) worldwide from 2014 to 2019 (Statista.com 2016)

2. Security and Privacy Issues

Numerous research indicates various security and privacy issues that are related to cloud computing. These issues are applicable for mobile cloud computing as well. Furthermore, mobile cloud computing has additional security and privacy issues.

The study done by Popovic et al (Popovic et al 2010) outlines the security and privacy issues faced by cloud service providers. Cloud resources run on remote locations, and clients access resources through virtual machines. Although each client runs an individual virtualized environment, sharing the same physical resources can impose a security threat. In addition, each cloud service provider uses different storage structures, which may prevent the clients from switching from one vendor to the other. There is no data integrity standard followed by the cloud service providers and the ownership of control for encryption/decryption is not standardized.

Cloud service providers do not disclose the location of data or storage, and the physical security of the data is not managed by the clients (Behl 2011). The paper by Behl identifies a number of security and privacy threats that are present in various layers in a cloud computing environment. Often an absence of hiring standard for cloud employees may lead to insider threats and intrusions. Dishonest employees can leak clients' data to rival companies, which causes violations of privacy. Section 55(1) of The UK Data Protection Act (1998) states that gaining access to personal data without the permission or knowledge of the data controller is a

violation of privacy and is an offense. However, in subsection (2) of the Data Protection Act 1998, it is mentioned that the personal data could be obtained without the knowledge of a data controller, only if it is required to prevent crime. A cloud employee who is not a data controller or who is not appointed by a court of law should not access personal data under any circumstances.

Multi-tenancy issue is another security threat, which is discussed in numerous studies. Since clients access cloud resources through virtual machines (VM), there is a possibility of launching repetitive VM-to-VM attacks. In addition, cloud servers are susceptible to outside attacks, such as man-in-the-middle attacks (MITM). Cloud computing provides more interfaces to provide efficient data access, and this leads to MITM attacks. Furthermore, in mobile cloud computing, wireless communications and heterogeneous networks maximize the chance of MITM attacks. Data loss is another major issue found in cloud computing. A cloud server is a multitenant system with access control different from client's premises. Weak authentication techniques, accounting controls and inconsistent use of encryption keys can lead to data loss.

Applications that use cloud resources are equally vulnerable to threats. An important research in this area (Al-Aqrabi et al. 2013) indicates security challenges associated with BI (business intelligence) systems that run on clouds. Business strategy data is highly sensitive. Generally, in BI systems, data extraction is performed based on SQL query and loaded to the temporary data marts. At this stage, the data is accessed by expert data modelers and ensured that the data is transformed as per rules. Transformed data is then loaded to the warehouse. Multiple OLAP (online analytical processing) queries access the data from the data warehouses. Human intervention and automatic processes, reading and writing are required in the entire BI process at multiple stages, which impose a security and privacy threat to the entire process. Although different layers have safety measures (securing database objects, application files, and servers etc.), there is a requirement for unified threat management (UTM) to reduce the security risks as well as overhead.

Furthermore, there are threats that are specific to mobile cloud computing. Kim et al. (2012) describe the mobile cloud security issues related to malicious programs that are injected in a mobile cloud virtualization environment. These malicious programs can affect one virtualized machine, and spread to the other. An affected VM can cause information leakage and data loss, which is a serious problem for any cloud user.

User authentication is an issue in a mobile cloud computing environment. If cryptographic keys used for encryption and authentication are stored at the cloud premises, it is difficult to access the resources when the key is compromised or lost. Therefore, there is a need of effective key management in mobile cloud computing. Choi et al. (2012) describe authentication using profiling. This includes the user information and the service information. However, implementing complex security algorithms and protocols remain a challenge considering the limited resources of mobile devices, such as basic smartphones or sensors. High-end smartphones have good processing power and memory, which could support complex security mechanisms.

3. Threat Mitigation Strategies

Implementing a security and privacy mechanism for a mobile cloud computing environment is important. However, the heterogeneous architecture, multi layered functional components, and various modes of communications prevent implementation and deployment of a single security standard and a unique privacy policy. Therefore, a threat mitigation strategy is required, which can help in minimizing the security and privacy issues. In this section, we identify four threat mitigation strategies.

a. Refined policy

Cloud policies should be refined to address issues related to data privacy (Khan et al. 2012), ownership, transparency, and cloud administration etc. Clients should know the location of the cloud storage, and they should be able to partially or fully control the encryption/decryption of their data. The policy should define the data ownership and maintain privacy of the data. Only trusted employee should administer the cloud services. In order to determine the trustworthiness of an employee, background verification should be performed by a third party to ensure an unbiased evaluation. The policy must be refined periodically and notified to the mobile client through a simple interactive interface.

b. Compatible software and interfaces

Cloud service providers use different software and interfaces, which are incompatible and cause complications in the data migration (Opara-Martins et al. 2014). If all the cloud service providers, such as Google, Amazon, Microsoft use a specific well-defined access mechanism and storage structure then clients can switch between different vendors without any obstacle. This compatible software and the mechanism should support multiple mobile devices for any registered client in order to provide seamless transition between devices.

c. Strong authentication

A strong authentication mechanism ensures authorized access of sensitive data. Therefore, it is important to deploy an authentication scheme that can validate the mobile client and the cloud server. Although smartphones have good processing power and memory, other mobile devices, such as wearable devices have very limited resources. Therefore, a light-weight mutual authentication scheme should be deployed, such as CA-based (cellular automata) OTP (one-time password) authentication (Yoo et al. 2012) or light-weight message digest and location based authentication, such as the one presented in this paper.

d. Security audit

Selection of a cloud service is difficult considering various factors, such as security, privacy, cost, and policy etc. Many business organizations feel hesitant to adopt a cloud service primarily for security reasons. Therefore, there is a requirement of security audit. Han et al. (2015) proposes a hierarchical method for security audit, which consists of two levels. One level measures overall security of the cloud stack and another level accesses each different service. A periodic security audit ensures safety of all internal functionalities of a cloud environment, and the overall security of the mobile cloud computing environment. However, it is equally

important to educate the mobile cloud users to safeguard their data against latest threats or nefarious activities, such as ransomware, spyware, scareware etc.

4. Light-weight Authentication Scheme

In this section, we present a Message Digest and Location based Authentication (MDLA) for end-to-end security in a mobile cloud computing environment. The seed for the idea for this scheme and a very preliminary version of this scheme was presented as a conference poster (Dey et al. 2014). In this following, we expand upon the idea presented in the poster publication and provide a full description of the technique's individual phases. MDLA is a novel authentication scheme, which validates a mobile client and a cloud server participating in a mobile cloud computing. This scheme is independent of device specific properties, such as USIM (universal subscriber identity module) or MAC (media access control) address. Three key phases - registration, authentication and update constitute the operation of MDLA scheme. The registration phase stores mobile client's credentials to the cloud server and generates a seed key and a message digest for the initiation of the authentication phase. The authentication phase is the core phase of MDLA. The steps in the authentication phase run each time when a mobile client wants to establish a session with the cloud server. This phase ensures that data transmission is possible, if and only if both parties are legitimate and if the mobile client is registered with the cloud server. There are three different types of updates performed by the proposed scheme to ensure confidentiality and access control– updating the client registration: re-registration, updating the authentication: re-authentication, and updating the keys: key generation.

Table 2: Notations used in the MDLA scheme

Notation	Definition
cid	Client id that uniquely defines each mobile client
pwd	Password that is secret to each mobile client
h	Specifies a hash operation
δt	Timestamp of the mobile device client
δh	Hash function choice parameter, which defines the type of hash function used by both parties. E.g. SHA1, MD5 etc.
δp	Indicates the choice of pseudo random number generator. E.g. Blum Blum Shub etc.
ε	Defines expiry period chosen by the cloud server for each client. It is a counter which decrements to "0" from a preset value
$prim_{key}$	Primary key used by mobile client and server as one of the symmetric key
$auth_{key}$	Authentication key used by mobile client during authentication request
sec_{key}	Secret key chosen by the cloud server during registration and authentication phase
ϕ	Indicates location vector of the mobile device. It is a logical OR of the latitude and longitude
md_{client}	Message digest or hashed message of each mobile client's certificate generated by the cloud server
ref	Column reference in big table at the cloud server, where each client's information is stored

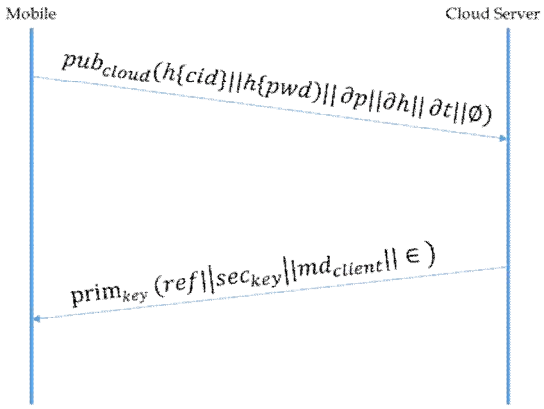

Fig 2: Registration Phase

a. Registration phase

The registration phase (Fig. 2) is an account setup phase, where a mobile client registers with a cloud server and exchanges setup information such as client id, password, contact information etc. Typically, a certification authority certifies a cloud server, therefore MDLA focuses on certifying the registered mobile client. During the registration phase, the cloud server obtains $m_{reg\text{-}req}$ from the mobile client and stores in the big table residing at the cloud server, which contains hashed client id, hashed password, timestamp, location information, etc. The mobile client sends a registration request message encrypted with the cloud's public key pub_{cloud} (Equation 1).

$$m_{reg-req} = E_{pub_{cloud}}(h\{cid\}||h\{pwd\}||\partial p||\partial h||\partial t||\emptyset) \quad (1)$$

$h\{cid\}$, $h\{pwd\}$ are the hashed client id and hashed password, respectively. ∂p defines the choice of PRNG (pseudo random number generator), ∂h defines the type of hash function the mobile device is running. ∂t defines the current time-stamp of the mobile device at the time of registration, and ∂ indicates the geographical location (latitude and longitude) of the mobile device at the time of registration. Upon receiving the encrypted message, the cloud server decrypts it with the cloud's private key prv_{cloud}. Then the server stores the received parameters in the server's big table specific for each of the mobile clients. After storing the parameters, the cloud server creates a client certificate with the client's account credentials and generates a message digest md_{client} of the client's certificate. In addition, it generates a random number as secret key sec_{key}, which is used during the authentication phase for the cloud server validation. The $h\{cid\}$, $h\{pwd\}$ are XOR-ed and used as the seed for the PRNG in order to generate a symmetric key termed as primary key $prim_{key}$ (Equation 2). During the registration phase, the location of the mobile client (∂) sent from the mobile device, is used as the state identifier for the PRNG to identify a stream sequence as $prim_{key}$. For all the subsequent primary keys $prim_{key}$, previous location of the mobile device ∂_{prev} is used as the state identifier for the PRNG.

$$h\{cid\} \oplus h\{pwd\} \xrightarrow{\substack{PRNG \\ \emptyset_{prev}}} prim_{key_i} \quad (2)$$

In addition, the cloud server creates a registration expiry period □ for the mobile client, which forces a re-registration. The cloud server decrements the expiry period, which becomes true when the value reaches "0". The re-registration helps in updating password, expiry period, and re-generation of client's certificate. Upon completion of key generation (sec_{key}, $prim_{key}$), message digest (md_{client}), and expiry period (□) the cloud server sends a response back to the mobile client encrypting with primary key $prim_{key}$ (Equation 3). This response $m_{reg\text{-}res}$ includes the big table column reference (*ref*) for efficient lookup.

$$m_{reg-res} = E_{prim_{key}}(ref || sec_{key} || md_{client} || \in) \quad (3)$$

The mobile client generates the primary key $prim_{key}$ using the client's *h{cid}*, *h{pwd}*, □ (Equation 2) and decrypts the received message. The mobile client then stores the four received parameters for the authentication phase.

b. Authentication phase

The authentication phase must satisfy the following conditions to execute the MDLA scheme between a mobile device and a cloud server.

- The mobile client is registered with the cloud server and received message digest md_{client} from the cloud server during registration.
- The mobile client knows his/her *cid* and *pwd* to access the cloud services.
- The cloud server is synchronized with the mobile client, which means the cloud server has □*p*, □*h*, □*t*, □, *h{cid}*, and *h{pwd}* for each registered mobile client.
- The mobile client has received *ref*, and sec_{key} from the cloud sever.

For sending the authentication request, each time the mobile device generates the primary key $prim_{key_i}$(Equation 2), and a fresh key known as authentication key, $auth_{key_i}$ (Equation 4) by using mobile client's current timestamp □t_{new} as the seed, and mobile client's current location □$_{new}$ as the state identifier for the PRNG. The state identifier is used to specify a PRNG stream sequence as the $auth_{key_i}$. The mobile client sends an authentication request to the cloud server by sending the authentication message $m_{auth\text{-}req}$ (Equation 5).

$$\partial t_{new} \xrightarrow{\substack{PRNG \\ \emptyset_{new}}} auth_{key_i} \quad (4)$$

$$m_{auth-req} = E_{prim_{key_i}}(E_{auth_{key_i}}(md_{client}) || \partial t_{new} || \emptyset_{new}) || ref \quad (5)$$

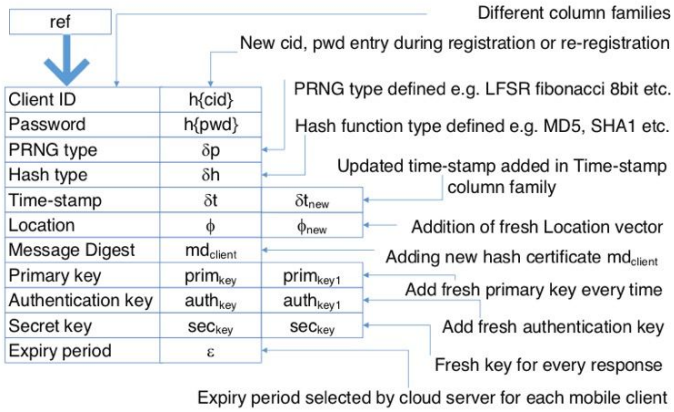

Fig 3: Security parameters' entry to the cloud server big table

As soon as the cloud server receives $m_{auth\text{-}req}$ from the mobile client, it reads the column reference *ref* and locates the mobile client's information in the server's big table (Fig. 3) to get the $prim_{key}$, and □. The job of the column reference is to perform efficient lookup at the big table.

If *ref* is modified or removed during transmission the cloud server decrypts the encrypted portion of the message by performing a trial and error method with all the stored primary keys. The cloud server first verifies with server's table if the registration is still valid for the client's entry by checking the expiry period, □. If the value for □ is "0", the cloud server rejects the authentication request and sends a re-registration (described in the update phase) notification to the mobile client. For a valid registration, the cloud server decrypts the encrypted portion of the authentication message $m_{auth\text{-}req}$ using $prim_{key}$ to obtain □$_{new}$, and □t_{new} used in generating the $auth_{key_i}$ (Equation 4). The $auth_{key_i}$ decrypts the rest of the encrypted message and obtains md_{client}, which is verified with the stored message digest. A successful match indicates that the mobile client is legitimate. Once the mobile client is authenticated by the cloud server, it is time for the cloud server to be authenticated by the mobile client. The cloud server sends an authentication response message $m_{auth\text{-}res}$ (Equation 6).

$$m_{auth-res} = E_{sec_{key}}(md_{client} || sec_{key_{new}}) \quad (6)$$

The response message contains md_{client}, which is encrypted with the pre-shared key sec_{key}. In addition, the cloud server picks up another random number as new secret key and sends it to the mobile client to use it for the next authentication request. The mobile client receives the response message $m_{auth\text{-}res}$ from the cloud server and decrypts it using the stored sec_{key}. The received md_{client} is matched with the stored message digest. The successful match ensures the cloud server is legitimate. During this process the old sec_{key} stored in the mobile device is replaced with the new one received from the cloud server.

c. Update phase

For a specific mobile client, re-registration takes place when the expiry period □ becomes "0". During the reregistration process the cloud server sends $m_{re\text{-}reg\text{-}req}$ (Equation 7) to the mobile

client, which contains a registration request encrypted with sec_{key}. Once the mobile client receives the $m_{re\text{-}reg\text{-}req}$ from the cloud server, it decrypts the message with the stored sec_{key} and retrieves the md_{client}, and registration request. At first, the mobile client validates the cloud server by matching the message digest received with the stored message digest. If the cloud server is legitimate, the mobile client reads the re-registration request and sends $m_{reg\text{-}req}$ (Equation 1) to the cloud server. A re-registration process expects the mobile device to fetch a new $h\{pwd\}$, and a new timestamp Δt. The cloud server re generates a fresh client certificate, message digest md_{client}, and a new expiry period Δ during re-registration. The cid, Δp, and Δh, remain unchanged.

$$m_{re-reg-req} = E_{sec_{key}}(md_{client} || re - registration - request) \quad (7)$$

Updating the authentication refers to a re-authentication process, which is triggered if there is a sudden connection loss after the session establishment. The reason for connection loss could be a network error, value of Δ becoming "0" during an ongoing session, or some type of forced termination of the connection. The re-authentication is same as the authentication process, and is initiated by sending the $m_{auth\text{-}req}$ (Equation 5) to the cloud server in order to prevent any rogue client to access the cloud server during a session re-establishment. Updating keys refers to the key generation process. Keys are updated frequently to make sure even if a key is compromised, the subsequent messages are still secure. We use three major keys in our authentication scheme termed as primary key - $prim_{key}$, authentication key - $auth_{key}$, and secret key sec_{key}. The primary key generation (Equation 2) accepts the $h\{cid\}$ XOR-ed with the $h\{pwd\}$ as the seed to the PRNG. The variability of the $prim_{key}$ is introduced by using the previous location Δ_{prev} of the mobile device as state identifier to the PRNG. The $auth_{key_i}$ generation (Equation 4) accepts the current timestamp Δt_{new} as the seed to the PRNG and current location of the mobile device Δ_{new} as the state identifier. The $auth_{key}$ is fresh for every authentication request due to the use of two variables, the current time-stamp and the current location. The secret key sec_{key} is a random number chosen by the cloud server during the registration phase and sent to the mobile client. An old key is replaced with a newer key $sec_{key_{new}}$ during every authentication response that is sent from the cloud server to the mobile client. Every authentication request ensures a sec_{key} update.

5. Discussion and Conclusion

In developed or developing nations, there is an increase in demand of IT (information technology) and ITES (information technology enabled services), which has fueled the growth of cloud technologies and mobile enabled services. Substantial usage of mobile devices brings in the concept of mobile cloud computing to offload computing power to cloud servers. This is a versatile technology where large ranges of mobile devices utilize virtualized cloud resources.

As technology of this kind grows, it draws the attention of business organizations and attracts more people and that includes adversaries, which impose a serious threat to any kind of sensitive information. Security and privacy are critical issues in mobile cloud computing, especially when they are deployed for sensitive information transfers, such as health care records, financial transactions and business strategies. A mobile cloud computing environment

could be affected if there is a service disruption or security breach in mobile device, cloud premises or in the communication media. A large corpus of literature indicates various types of security and privacy issues that are present in the cloud computing and mobile cloud computing environment. However, there is no unique or standard solution, which could be applied to the system.

Cloud computing is a combination of heterogeneous technologies and services, which makes it difficult to implement a standard security protocol or scheme. The absence of security standard for cloud computing makes cloud resources vulnerable to different types of security and privacy threats, such as VM-to-VM attacks, injection of malicious codes, unauthorized access, data loss, and information theft. In addition, mobile cloud computing suffers from data ownership problem and jurisdiction, which are policy issues. Interoperability between cloud service providers is a major issue, which restricts user to switch between cloud service providers. Cloud service providers need to use compatible software and storage structure in order to prevent data loss or integrity issues. Regular security audit is required to assess the threat level and security features. A threat mitigation strategy could be employed to safeguard the mobile cloud computing. Furthermore, there is a need of lightweight authentication scheme, which can support resource constrained mobile devices, such as wearable devices.

One such lightweight scheme that we presented in this paper is MDLA. In order to run MDLA, a mobile client and a cloud server need to be synchronized, which is performed using a secured registration phase. During this phase, important parameters such as location vector, timestamp, password, client id, choice of PRNG, choice of hash function, message digest of client's certificate, secret key, and expiry period are exchanged between a mobile client and the cloud server. Registration is a one-time process and is performed at the very first time when a mobile device registers with a cloud server. However, a re-registration phase could be triggered when expiry period, becomes "0". Use of location vector and timestamp during key generation increases the intensity of unpredictability, and thereby makes MDLA secure.

References

Akhil Behl 2011, 'Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation', *2011 World Congress on Information and Communication Technologies*, pp. 217-222, December.

Cindy Liu 2015, 'Worldwide Internet and Mobile Users', *eMarketer's Updated Estimates for 2015*, viewed Jun 2016, https://insights.ap.org/uploads/images/eMarketer_Estimates_2015.pdf

Cisco 2016, 'Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020', *Cisco Systems*, pp. 5. viewed Jun 2016, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html

Data Protection Act 1998. Chapter 29. London: HMSO, viewed Jul 2016, http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf

H. Al-Aqrabi, L. Liu, R. Hill, Z. Ding and N. Antonopoulos 2013, 'Business Intelligence

Security on the Clouds: Challenges, Solutions and Future Directions', *Service Oriented System Engineering (SOSE), 2013 IEEE 7th International Symposium on*, Redwood City, 2013, pp. 137-144

IDC 2016, 'Worldwide Cloud IT Infrastructure Spend Grew 21.9% to $29.0 Billion in 2015', *Press release*, Framingham, viewed May 2016, http://www.idc.com/getdoc.jsp?containerId=prUS41176716

IDG Enterprise Marketing 2015,'IDG Enterprise Cloud Computing Survey – Insight into the Advancement of Enterprise Cloud Adoption', *IDG Enterprise*, viewed May 2016, http://www.idgenterprise.com/resource/research/2015-cloud-computing-study

J. Opara-Martins, R. Sahandi and F. Tian 2014, 'Critical review of vendor lock-in and its impact on adoption of cloud computing', *Information Society (i-Society), 2014 International Conference on*, London, pp. 92-97

K. Popovic and v. Hocenski 2010, 'Cloud computing security issues and challenges', *MIPRO, 2010 Proceedings of the 33rd International Convention*, pp. 344-349, Opatija, Croatia.

S. Dey, S. Sampalli and Q. Ye 2014, 'A light-weight authentication scheme based on message digest and location for mobile cloud computing', *2014 IEEE 33rd International Performance Computing and Communications Conference (IPCCC)*, Austin, TX, 2014, pp. 1-2

Sang-Ho Shin, Dong-Hyun Kim and K. Y. Yoo 2012, 'A lightweight multi-user authentication scheme based on cellular automata in cloud environment', *Cloud Networking (CLOUDNET), 2012 IEEE 1st International Conference on*, Paris, France, pp. 176-178

Statista.com 2016, 'Smartphone users worldwide 2014-2019', viewed Jun 2016, http://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

T. Kim et al. 2012, 'Monitoring and detecting abnormal behavior in mobile cloud infrastructure', *2012 IEEE Network Operations and Management Symposium*, Maui, HI, 2012, pp. 1303-1310.

Wei Deng, Hoon Jeong, Euiin Choi 2012, 'User Authentication using Profiling in Mobile Cloud Computing', *AASRI Conference on Power and Energy Systems, AASRI Procedia*, Volume 2, 2012, pp. 262-267

Z. Yandong and Z. Yongsheng 2012, 'Cloud computing and cloud security challenges', *International Symposium on Information Technology in Medicine and Education,* pp. 1084-1088.