Go Mobile

With the increasing popularity of smart phones the use of cloud services for mobile applications has also increased by many folds. There are some issues and challenges with respect to privacy and security of your data stored and the way we handle our mobiles. Living in the world of smart phones, we need to be cautious while handling our data and using various features, thus this section highlights on certain security measures for smart phones.

---------- *Keeping your Mobile Apps Secure*

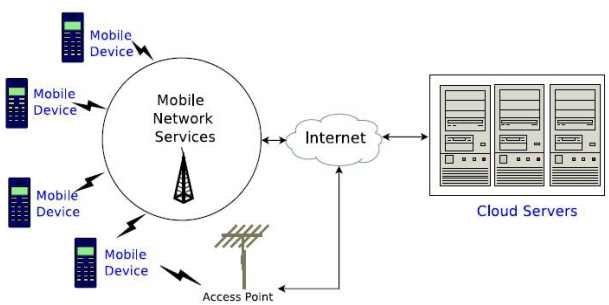
Secure Mobile Data Computation Offloading

Manoj Singh Gaur
Director, Indian Institute of Technology Jammu Jagti, PO Nagrota, Jammu

Vijay Laxmi
Professor, Department of Computer Science and Engineering Malaviya National Institute of Technology, JLN Marg, Jaipur

Shweta Saharan
Ph.D. Scholar, Department of Computer Science and Engineering , Malaviya National Institute of Technology, JLN Marg, Jaipur

Mobile Cloud Computing (MCC) provides a scalable solution for both storage and computation of data over the Cloud. MCC provides a huge pool of stor-age which can be accessed online by the mobile users. However, it aggravates the user data privacy issues. Secure data storage is based on cryptographic solutions, but when it comes to computation cryptographic solutions are not useful, as data is rst decrypted then the computation is performed. However, homomorphic techniques support computation on encrypted data and generate an encrypted result, are compute intensive and not advisable due to resource constraint nature of mobile devices. Privacy leakage risks prevent users from sharing their private data with third-party services. Now a days, large number of image and document processing apps, process the data on the cloud, instead of mobile device. Basic cryptographic solutions cannot provide secure computation in mobile cloud, which raises the requirement of light-weight secure offloading methods. This article gives a brief description about increasing use of mobile cloud apps and suggests some measures to securely make use of mobile cloud computing via apps.



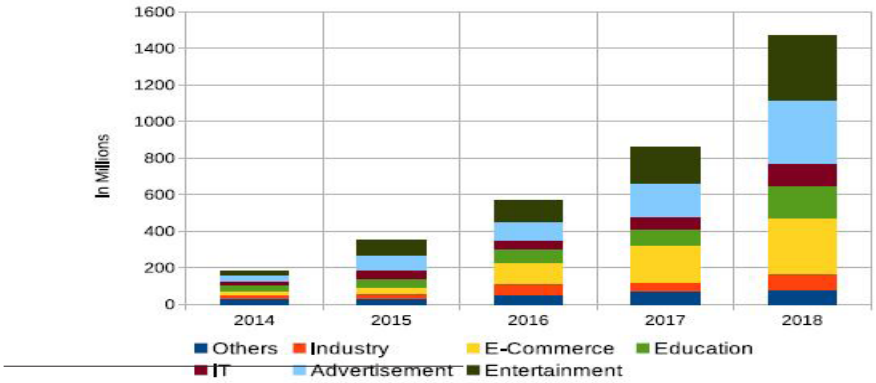


Figure 2: Growth of Mobile Cloud Apps from 2014-2018

Introduction

Mobile Cloud Computing (MCC) combines cloud computing, mobile computing and wireless networks in order to provide rich computational resources to mobile users. MCC brings together the fastest growing cloud technology with the ubiquitous smart-phone. Need of MCC as mobile devices have

- Limited Processing Capabilities
- Limited Storage
- Limited Battery Power

Figure 1 shows the architecture of MCC, where mobile devices ooad both data and computation to the mobile cloud via network service provides. For supporting intensive computations on resource-restricted mobile devices, ooads the computation to the mobile cloud. This mechanism helps in achieving eciency in performing the mobile task, whereas along with this, it raises many security and privacy concerns. With the use of Mobile Cloud Computing, private data of the mobile user is processed at the cloud side. This leads to exposure of both mobile data and computation to the cloud. A malicious cloud service provider can misuse this data.

Services Oered and Usage of MCC

There are many existing approaches which preserve the privacy of the data stored on the cloud. Most of them are heavy cryptographic techniques, which are capable of preserving the privacy of data stored over the cloud. When any computation is carried on the encrypted data stored on the cloud, it is rst required to decrypt it and thus make it vulnerable again, then computation is performed. As a solution to this, Homomorphic Encryption was introduced, which is capable of performing computation on the encrypted data and generate the result in encrypted form which can be later decrypted. Homomorphic encryption is too complex and compute intensive for battery and resource-constraint mobile devices.

As per a survey by Appypie [1], the usage of mobile cloud apps is increasing rapidly in various domains as shown in Figure 2. Services offered by Mobile Cloud Computing are

Data Storage:
It is storing data like photos, videos, document les on mobile cloud in order to overcome storage shortcomings. Example: Mi Cloud, Google drive, Dropbox etc.,

Computation offloading:
It is transfer of certain computing tasks to an external platform i.e. mobile cloud due to hardware limtations of the mobile device.

- Image processing: PIXLR, Pics Art
- File conversion: Covert.les
- Language processing: Siri (Apple), Alexa (Amazon), Ok Google (Android)

Securing Cloud-based Mobile Data and Computation

- For ensuring the security of sensitive mobile data which is offloaded, user should prefer encryption mechanism.
- For performing computation on mobile cloud,non-sensitive data should be offloaded, sensitive photos and other content should be processed on mobile device itself.
- Instead of offloading complete application, only non-sensitive operations should be offloaded.
- Download apps from legitimate source only, for processing documents and images.
- Always check for the third party policy declared by Cloud Service Providers.
- Avoid using newly added apps for processing your personal documents and photographs.
- Check for app policy, whether its processing data oine or using cloud.

References:

- *Snigdha https://www.appypie.com/basics-of-mobile-cloud-computing-and- mobile-cloud-applications*

QR Code can be Malicious!

Mrs K Indraveni
Principal Technical Officer
Centre for Development of Advanced Computing (C-DAC), Hyderabad

With the increasing use of smartphones, QR codes are becoming popular. QR Code or Quick Response Code, is a matrix bar code which can be read by camera and then processed to read its data. It was initially developed for the automotive industry in Japan, but now it is being used by many companies. You will be surprised to know that the QR code was invented back in 1994 by Denso Wave.

Let us first see few instances where QR codes are seen and used.

The auto or cab drivers are tagging the QR code which contain the driver information in the vehicle so that passengers can easily scan the QR code, save or share the driver details, as part of safety. The whatsapp which is the most popular mobile application these days, have a web.whatsapp.com which can be connected using the QR code from the mobile application and start using the web version of whatsapp. We also see the QR code for performing digital transactions at various places like shopping malls, delivery boys, street food vehicles and many more.

So, many people now know what QR code is, but still many are unaware. It is similar to the bar code which we see on products, but unless like a bar code reader, QR code reader do not require any specific reader. Our smartphone camera can read it. The application which is reading the QR code , should be able to understand the content of the QR code, other than which there is no dependency to process the QR code. Due to fast readability, it is now widely accepted and the use of QR codes is increasing. The scan of the QR code replaced efforts required to perform various tasks like writing down the web url, information on a paper, typing etc.,. We can quickly open a website by scanning a QR code rathar than typing the URL. The QR code can be generated for a piece of information like business card details, web address, paragraph or around 300 characters or even more. The smaller the content the better is the QR code.

QR code for web address https://infosecawareness.in

Do not fall prey to the phishing websites through QR codes

In this article, we will see the risks coming up with QR codes and how they are becoming malicious to us in our day to day lifes.

QR Code Generation

For generating QR code , there are many online resources using which we can create the QR code for a text which can be url, web address, vcard, email, phone number etc., A few QR code generator tools are :

- https://www.the-qrcode-generator.com
- http://goqr.me/
- http://www.qr-code-generator.com/
- http://www.qrstuff.com/
- https://scan.me/qr-code-generator

These generator tools will accept your text information and generate an image which can be downloaded for later usage.

The programming languages have also in-built libraries to support QR code generation. Thus the web applications can, also dynamically generate QR codes for important easy to transmit data like online certificates generated, to access online reports etc.,

The QR Code once generated, it will contain the information for unlimited time and thus QR code do not have any expiry or lifespan.

Is it possible to hack the QR Code

By now, you might have got an overview that QR is just an image which contain the text inside. However there are chances that you see a different QR code for same piece of text when generator using different methods. The reason for this is that, There are 40 Versions (sizes) of QR Codes, 4 error correction levels and 8 masking possibilities giving a total of 1280 possible QR codes for any given input. For more details on types of QR codes, storage, error correction and many more technical details, visit, https://en.wikipedia.org/wiki/QR_code.

Though same piece of information can have various QR codes, the QR code once generated cannot be tampered or hacked. Hacking a QR code means manipulation of the action without modifying the QR code. This is not possible. QR codes can be malicious and can trigger malicious action. But that QR code will not be the same as the legitimate QR code. Two QR codes with different actions will never be the same. We will certainly see different patterns in both QR codes. So, QR codes cannot be hacked. But It can be malicious and hackers can use a QR code for various malicious purposes.

Security risks involved in using QR Codes

As discussed earlier, QR codes can be malicious, so there are various risks involved with QR codes. Let us see those risks.

QRishing Attacks

Phishing is a popular way of hacking web accounts. Attackers send a fake web page with forms to collect credit card / debit card details, login details etc., which pretend to be the original one. The attackers used various means to send the phishing web urls to the victim like, email, chat messages etc., and when awareness about phishing websites increased, people started taking precautions by verifying the web url, by not clicking the links received through emails etc., later to which the attackers started performing tabnapping attack through which an idle tab is forced to redirect to the phishing website. This is driven to be another mode of taking victim to phishing website. Today, the QR code has become another medium for the attackers to reachout with phishing website to the victim's browser. It is also described as QRishing by some security researchers.

Its very simple, due to the flexibility and easiness in adopting the QR codes, the public posters and advertisements, started using the QR code which when scanned will take us to the advertisers website or show us relevant information. The attackers can create malicious QR code which contains web url of the phishing website and print the posters and advertisements with this malicious QR code. Also, the attackers can just paste the malicious QR code over the original public posters displayed across without even printing the entire poster. Unknowingly, the person who scans these QR codes will be landed up into the phishing website. Due to limited space in mobile, browsers do not show the full address in the URL thus the victim ends up sharing the details in the phishing website.

There are cases where survey forms related web urls were phished and shared through QR Code.

Drive-by download of Malicious apps

Malicious software distribution are also done through QR codes. A QR Code with web url of malicious websites to distribute malware via drive by download attack. Drive by download attacks are attacks in which a website forcefully downloads software in the device when we visit the website. It does not need any action from the user's side. Visiting the website is enough to trigger the download action. The downloads can be of malicious apps like capturing screen, recording camera and mic, sending SMS, collect your data or anything which can perform potential harm.

In Russia, a malicious QR code on scanning sent SMS to premium numbers costing $5 USD per SMS. Most of these kinds of attacks have been seen against Android devices.

Digital Transactions

So far, I haven't seen any UPI digital transactions related attacks through QR codes. However, by understanding the QR codes usage and various attacks done using QR codes, I presume that the following UPI based attacks using QR codes may be the future attack vector.

Here is how it can be done. We come across in many shopping areas the QR Codes are displayed over the walls for digital transaction. It can be paytm, phonepe, upi, bhim etc., Customers just scan the QR code and process the payment. I have seen in many busy shops where customers purchase the items and just scan the code available in the display area , finish the payment and very rarely customers show the transaction tick mark to the shop person as well. Not sure how much attention the shop owner paid on the details above the tick mark. Someone can change the displayed QR code when the shop owner is inattentive with another QR code. The shop owner may notice that payment have not been received , but by that time, already few transactions might have been missed.

Same is the case with cabs, autos who also are displaying the QR codes for digital transactions. There are chances for travelling passengers to change the QR code with another code with different account details. Thus your payment may not reach the intended person. And if you are one of the user who display the QR code, beware of such manipulations.

Protect yourself from Malicious QR codes

Choose the right QR Code reader and review the QR code

- Before installing the QR code reader in your smartphone, check its features. Look for an option if it allows you to inspect the decoded code before opening up the code in browser or other targeted application. If it doesn't do that, change your choice and go for another QR code reader app which supports such feature.
- When the QR code reader decodes the text embedded in the QR code, verify the url or the content for its correctness.

Inspect the QR code to make sure its not a sticker

When you see a QR code over a public poster, newspaper or any such places, make sure that its not a sticker. Touch with your hand to feel the difference between the QR code and the rest of the paper, or try to peel and check. If such incident is observed, report it to the owner.

Reconfirm the payee name

While performing digital transaction by scanning the QR code, the apps usually display the name of the person who owns the account before the amount is entered. Read out the name or show it to the concerned to verify if its the correct address to which the transactions is supposed to be done by you.

Mitigation against Mobile Application and Operating System Attacks

- *Consider installing security software from a reputable provider and update them regularly.*
- *Always check the features before downloading an application. Some applications may use your personal data.*
- *Do a good research about the application and the developer when you are downloading the application from third party.*

Mobile Security :
Bringing up children along with technology

Hemant Tyagi
Principal
Doon Valley International School

Learning starts by birth 98% of the human brain gets developed by the age of 6 years, so if we want to foster and motivate our child to understand good and safe learning then technology needs to be a part of their experience in early years.

Technology as well needs to be dealt in a positive and secured manner. Internet has become a necessary tool for the family. Back in the year 2000, when phones came to India like a boom, no one ever thought of India to be the leading user in the world. The very nature of mobile phones that helps in connecting people and resources which has some risk of people intruding into your system. When everyone carries their personal phones almost everywhere, yes everywhere, we have to be very cautious in performing our actions.

Take a pledge to grant your children that much required exposure of mobile usage and embrace the technology

Most People check their phones almost 250 times in a day but one thing they never checked, how secured their mobile apps. Since mobile technology becomes more advanced so do the security attacks of those who want to exploit mobile technology creating a multitude of troubling scenarios.

Some important measures to keep our children aware of pros and cons of technology :

- No mobile phone screen before age of 2, if you are unable to avoid it then keep it on flight mode.
- Make a schedule of using mobile phones or other devices for children
- Give them in Safe Mode
- Consider common place for mobile phones to children.
- Set family rules for accusing Internet.
- Remind them regularly that people we met online can be stalkers, fake Id users, and cyber criminals etc. to avoid any mis-happening in future.
- Create strong, unique and easy to remember passwords.
- Guide your children not to post your personal photos and videos on social sites without informing family to avoid Hacking. Your ignorance is power of hackers.
- *Install firewall, Antivirus etc , visit www.cdac.in to download free tools & software for your mobile phones and PCs.

When you teach children in your classroom to keep screens away during playtime or story time and ensure that there is a timetable to be followed while using mobile phones, then kids learn that mobile phones cannot be used all the time. This is the same that parents need to be taught to do at home too, children learn by imitation, so if they see adults using mobile phones all the time then they will learn the same bad habits.

Solution to all the problems is be with children during mobile phone viewing time and chat with them during the show. Mobile phones are a one way process and so children don't learn important skills like waiting for the other person to speak. So face to face conversation are a must in the early years to build the foundation of social skills.

So, if children grow up seeing and experiencing the wise and safe use of technology then they will make best use of it, rather than being a slave of technology. The future is all about technology and we cannot prepare children for this future by keeping them away from it or by giving them incorrect habits of using it

MOBILE APPLICATION SECURITY

Do good research about apps and their developers by reading the reviews

Use only official stores for downloading Apps

Check for spelling mistakes in the title or description

Reset your phone to factory settings to remove any malware

Beware of apps that promise shopping discounts

Make sure you review and manage permissions for each app you download

Avoid installing apps by clicking on links in emails, social media etc.,

Uninstall apps when you no longer use

Look at the publish date. A fake app will have a recent publish date

Always keep an updated anti virus security solution installed

For more details / queries on Cyber Security visit or call us to our Toll free number

Information Security Education & Awareness
Ministry of Electronics and Information Technology
Government of India

www.InfoSecawareness.in

1800 425 6235

For Virus Alerts,Incident & Vulnerability Reporting
certin Handling Computer Security Incidents
http://cert-in.org.in/

www.cyberswachhtakendra.gov.in