# A Review Paper on Security Issues in Mobile Devices- Cryptographic approach and Security Measures

Urvil Ashokkumar Patel (1131703)
Lakehead University
upatel19@lakeheadu.ca

## I. ABSTRACT

In today's era, the internet and technologies play a significant role in our lives and growing explosively during the past several decades. Moreover, smartphones and other mobile devices have become essential in every person's life. Because they mainly offered numerous applications which make human life very easy. The rapid growth of the smartphone and the use of these devices for email, online banking, and accessing other forms of sensitive data has led to the emergence of a new and ever-changing threat landscape [1]. Concerning desktop computers, growth in mobile devices has been massive in recent years. The significant progression and development in mobile phone and equipment innovations bring a few difficulties like Data security. It might open the vast scope for hackers to take some essential information and performs different sorts of attacks on cell phones. In this paper, the primary security concerns in mobile applications are discussed. This paper introduced the basic overview of mobile computing, its challenges, significant security concerns in mobile applications, provides data encryption methods using cryptography and security tips to keep the mobile device safe from the various malicious code and hackers.

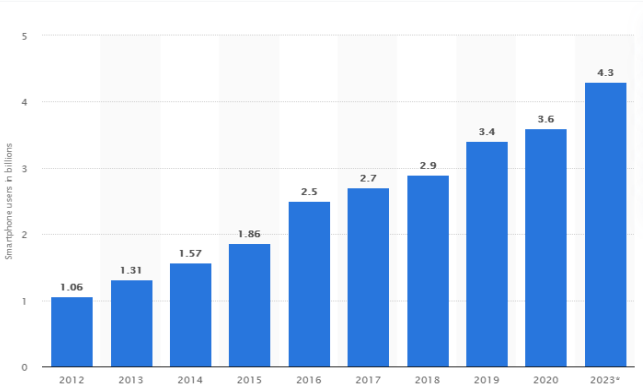
## II. KEYWORDS

Data security, Mobile computing, Mobile applications, Cryptography, Encryption, Decryption, Malicious code, Malware

## III. INTRODUCTION AND BACKGROUND

Nowadays, smartphones will become an essential part of our lives. Almost all people are carrying on or more smartphones with them for their daily usage. Because they have offered the same facilities that desktop workstations have provided [2]. Mobiles are helpful to perform messaging, E-mails, bank transactions, online shopping, etc. With the use of mobile devices, people can connect with their family and friends through social media. In a few years, the world coverage of mobile phone subscriptions has raised from 12% of the world population in 2000 up to 96% in 2014 - 6.8 billion subscribers – Corresponding to penetration of 128% in the developed world and 90% in developing countries [3].

There are many operating systems used in mobile devices, but the most popular ones are Android and iOS. Also, there are various versions of Android operating systems such as Lollipop, Marshmallow, Nougat, Oreo, etc. Similarly, the multiple versions of iOS are iOS8, iOS9, etc. The number of smartphone users worldwide today surpasses three billion and is further grow by several hundred million in the next few years [4].




Number of smartphone users worldwide from 2012 to 2023 [5]

Advance use of mobile phones for both personal and business purposes has increased significantly, which leads to big challenges like the security of user's data. Mobile device security is a developing security area of rising significance and cumulative needs, but it is a comparatively weak area for protecting a user's data privacy [6]. People can use various applications from different platforms, and the use of applications on the Internet creates complex problems with respect to the handling of threats and vulnerabilities in securing a user's data privacy. For instance, mobile applications like E-wallet, banking application, various social media applications, etc. exposes essential data of the users, which are always prone to much vulnerability. The value of data is far more important than the value of the device [7].

As wireless communication works mainly through the radio channels, so it is somehow easier to intercept on the communication channels. Nowadays, the number of attackers and malicious programs has increased rapidly. Although the mobile companies are working hard to provide security in the phones, according to the threats predictions report, 2015 will the turning point for threats to mobile devices in which the total number of mobile malware samples exceeded 5 million in Q3 2014 [8]. These threats can slow down the operation of the smartphone and transmit or modify user data. Therefore, it is important to provide security from threats.

## IV. LITERATURE REVIEW

Sardasht, Bakhtiar, Rebwar [2] studied various Mobile Application security in their paper. In which they initially started by giving an overview about how people can become dependent on mobile devices in their daily lives. They also discuss various security problems in mobile devices or mobile applications. Moreover, they mentioned various types of mobile malware and different types of attacks on mobile devices. They have also done the analysis on the various operating system regarding the security issues in mobile devices in the year 2012-2015.

Nagarjun and Shakeel Ahamad [22] analyzed the various mobile attacks like securing data storage, securing communication, and Malware attacks. They also provided security measures for developers, users, and for app hosting providers.

Jalaluddin, Haider, Jalal [6] analyzed the four various mobile threats like a physical threat, Application-based threat, Network-based threat, and web-based threat. They gave detailed information about mobile vulnerabilities which make the mobile phones slow or sometimes it may don't work properly. And in the last, they gave a defensive mechanism for users to keep their mobile phones safe.

Srikanth Pullela [24] analyzed the five fundamental goals of security in information systems like Confidentiality, Integrity, Availability, Legitimate and Accountability. Also discuss the symmetric, asymmetric algorithm and security protocols.

## V. SECURITY ISSUES IN MOBILE COMPUTING

Many authors have presented security issues in their papers but there are five fundamental goals of security in mobile computing are [17]:

- **Confidentially:** Prevent unauthorised users from gaining access to confidential information about a single person.
- **Integrity:** Ensure that unauthorized alteration, elimination or formation of data cannot occur.
- **Availability:** Ensure that authorized user getting right access when it's required.
- **Legitimate:** Ensure that only authorized users can access to services.
- **Accountability:** Ensuring that the users are kept accountable for their security-related actions.

## VI. MOBILE THREATS

Mobile device applications make a person's life even easier than it would be ever before. At any location, any mobile user can use applications to fulfil their daily needs, including communicating, buying, searching, making payments, selling, entertainment, and finding general information [6]. In addition, the threats can be done by


Various Security Threats [9]

using the internet and most of this mobile application can be work by using the internet. So, there are mainly four basic types of mobile device threats which include application-based, web-based, network-based, and physical threats.

### 1) Downloadable Application Threats:

The downloadable application can present many types of security issues for mobile devices. Application-based threats happen when individuals download an application that looks genuine (Malicious apps) however its stole data from their device. Application-based threats generally occur from one or more of the following categories:

- **Malware:** Malicious software, most commonly known as malware, is a threat to our devices. Cybercriminals create malicious software that is installed on someone else's device without their knowledge to gain access to that particular user's personal and financial information or to damage the device. It occurs in all types of the operating system.

- **Spyware:** Spyware describes software with malicious behavior that aims to gather information about a person or organization and send such information to another entity in a way

that harms the user [11]. It is basically designed to collect the user's private data without their knowledge. Spyware targets the user's phone call, location, text message, E-mail, browser history, private photos, etc. This stolen information can be used for financial fraud as well.

- **Privacy:** Privacy threats can be caused by using malicious applications. Almost all websites and applications collect some information about users and that information is at risk of loss [12]. Hackers can steal those user's information and their identity, which can cause serious problems.

- **Vulnerable Applications:** Vulnerable applications are those apps that give an attacker permission to perform unwanted actions like access sensitive information, stop other applications or services which may work correctly, download unwanted apps in user's device without their knowledge [13].

### 2) General Cyber security threats or Web based threats:

Due to the nature of mobile use, we carry a smartphone with us everywhere we go and also do browsing over the internet. Furthermore, we also use web-based applications over the internet which may cause some serious issues.

- **Phishing Scam:** Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It starts with a fraudulent email, link, or any other communication that attracts the user or victim. The message is made as it comes from the trusted sender. So, it fools the user, and if the user clicks on any particular link, then it will automatically download malware onto the target's computer [14].

- **Drive by Downloads:** If a user can visit any malicious website or web address, then it will automatically download an application on the user's device whether the user wants that application or not. Then in some cases application can run automatically, or the user can click on that downloaded item, which causes the mobile device, and it may become unstable [13].

- **Browser Exploits:** Browser Exploits are malicious code that allows attackers to abuse flaws and vulnerabilities in browser software or other programs used by it, such as Flash Player, PDF reader, and image viewer. This threat is somehow similar to the drive-by downloads [15].

### 3) Network and WiFi Security Threats:

The mobile device typically supports a cellular network as well as a local wireless network such as WiFi and Bluetooth. Which has different types of threats for the user. Some network-based threats are described below:

- **Denial-of-service attack:** A DoS is a cyber-attack in which hackers are meant to shut down a machine or network by overwhelming or flooding requests and to make them inaccessible to the intended user.

- **Network Exploits:** Network exploits particularly damage the mobile operating system or other application that operates on a wireless or cellular network. Bluetooth is especially vulnerable. Hackers can run the program and find the nearest all Bluetooth connections and connect to them. Once it is connected, they can install malware on the user's phone without their knowledge [12].

- **WiFi sniffing:** Wi-Fi sniffing means intercepting data between the mobile devices and Wi-Fi access points from the air [6]. It is also known as a packet sniffer. Many applications and web pages do not use proper security measures; they can send information or data into the unencrypted form, which can be easily accessed by hackers.

### 4) Physical Threat:

The mobile device becomes an integral part of human's daily life and physical security is an important issue. Some of the physical threats are described below:

- **Bluetooth:** Bluetooth is a short-range wireless technology standard used for exchanging data between fixed and mobile devices over short distances [16]. Bluetooth might result in exploits and data loss from the device through malware.

- **Loss or theft mobile devices:** The loss or theft of mobile devices is also a major issue because the device can be sold on the secondary market. And once it is sold out, then the information or data inside that device will be no longer be safe.

## VII. VARIOUS MALWARE ATTACKS

Mobile vulnerabilities are the biggest reason to slow down the performance of mobile devices, and it will also crash the running application as well. Malware can spread through the internet or unauthorized or unsecured applications. Once the malware is spread in the mobile devices, then it will become easy for the attacker to

access the sensitive information of the users. The most common mobile malware is listed below:

- **Worm:** A worm is a program code that will replicate itself and spread to other mobile devices. It can damage the security of the mobile device. The mobile worm can spread through SMS or any other communication source without user interaction [22].

- **Trojan Horse:** A Trojan horse is a type of malware that is often disguised as legitimate software. So, when the user clicks on that particular link and executes the file, then Trojan will be activated. It is also used in a phishing attack. It can steal both the personal and professional information of a particular user.

- **Rootkit:** A rootkit is designed in such a way that it can remain hidden on the user device. It may basically attack the operating system of the particular device. It will contain the number of tools and other programs that allows the hackers to steal the user information like credit card number or online banking information [23].

- **Botnet:** A botnet is a collection of internet-connection devices that allows the hacker to remotely control the user device. m. It represents a serious money-related security threat around the world and also responsible for sending spam mail to commit DoS attacks [6].

## VIII. CRYPTOGRAPHIC APPROACH IN MOBILE APPLICATIONS

### Use of cryptography in data protection:

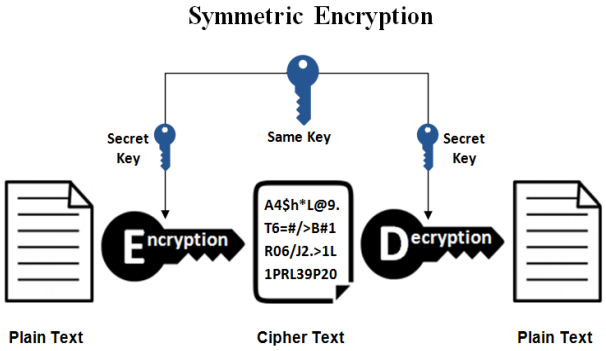
Nowadays, cryptography is used extensively in mobile devices to provide security and keep user phones from the various types of threats. To connect securely and quickly through electronic data transfer by using the web, the data should be encrypted. So, the primary aim of cryptography is to keep the user information safe during transmission. Cryptography is the best way of sending vital information secretly.

Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services [18]. Cryptography is the process of changing data or secure data so that they are not readable by an unauthorized person. Moreover, an unauthorized person might see that there are data communicated but cannot understand them. Cryptography converts data or information into an unreadable format for an unauthorized user and that information cannot be read without a key to decrypt it.

Encryption can help us to protect the data that we sent through the web. Basically, encryption is the process of taking plain text, like a text message or email, and convert it into an unreadable format -called “ciphertext.” There are various algorithms and methods which provide a high level of security. Cryptography can be defined as techniques of cipher data, and using a particular algorithm makes sure that the messages and data are secured from the other elements. Decryption is generally a reverse process of encryption. It decodes the encrypted information into the original information but while decryption requires a key. Any mathematical function that works in combination with a key, used for a cryptographic algorithm. The two types of cryptography algorithms are Symmetric cryptography and Asymmetric cryptography.

### Symmetric-key encryption algorithm:

Symmetric encryption is also known as private key cryptography. This algorithm uses the same key for both encryption and decryption. As shown in the image below, the secret key is shared between the communicating users in advance via a secure channel. So, the security of symmetric-key cryptography depends on keeping the secret key safe. So, this method requires careful key management. Examples of symmetric key cryptography include AES (Advanced Encryption Standard), DES (Data Encryption Standard), RC5 (Rivest Cipher 5), RC6 (Rivest Cipher 6), and Blowfish [19].

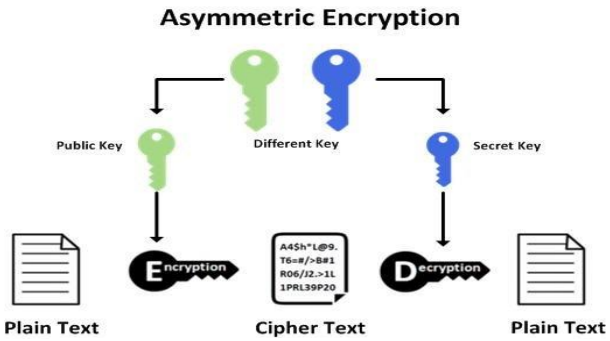



Symmetric Key Encryption [19]

### Asymmetric-key encryption algorithm:

Asymmetric encryption is also known as public-key cryptography. As shown in the image below, Asymmetric encryption uses two keys to encrypt plain text: the public key and the private key. The public key is distributed to anyone but the private key exchange over the internet or a large network. With the help of the Secure Socket Layer protocol, a secure connection is established with the users. It ensures that the malicious person does not misuse the key. Anyone who has a secret key or private key should decrypt the message and read the information in it. Examples of asymmetric key cryptography include

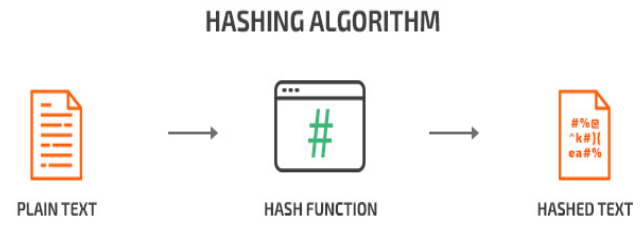
RSA (Rivest Shamir Adleman), DSA (Digital Signature Algorithm), and Diffie Hellman [19].




Asymmetric Key Encryption [19]

## Hashing:

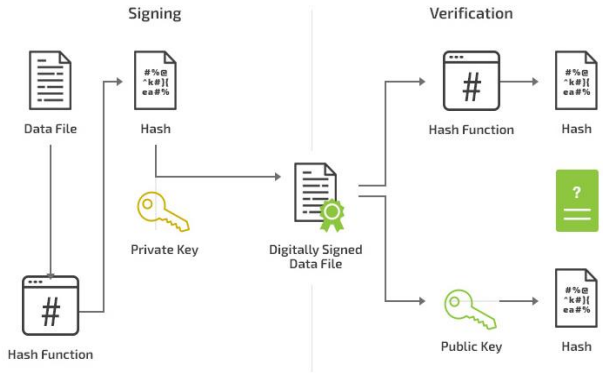
Hashing is not a form of encryption, but it does use cryptography. Hashing basically generates a unique, fixed-length string or signature for a message. The message generates by applying a hash algorithm with the same length, only with a different character sequence.
It is easy to generate a hash function from the plain text or message but very difficult to determine the original output from the hash [20].




Hashing [20]

## Digital Signature:

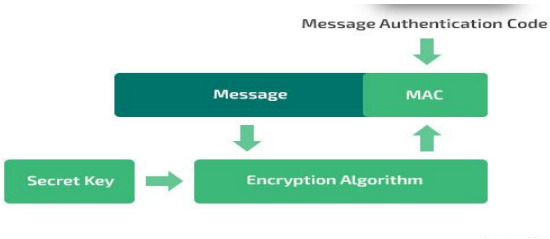
A digital signature algorithm is considered one of the best encryption algorithms for mobile applications. It is a combination of asymmetric cryptography with hashing to provide integrity and authenticity by encrypting the hash of the message with the private key [21].




Digital Signature [21]

## Hash based Message Authentication Codes (HMAC):

HMAC is a type of message authentication code that combines other cryptographic mechanisms (such as symmetric encryption or hashes) with the private key. The key is only known by server and endpoint. The endpoint applies a hash algorithm to the data and sends it to the server. The server decrypt that message by using the private key and compares the hashed data with the original message [20].




HMAC [20]

## IX. TIPS TO PROTECT MOBILE DEVICE FROM MALWARE OR SECURITY MEASURES

- Always install the mobile application from a trusted or well-known app development companies, for instance: Google Play App Store or the iTunes App Store, because they check the application thoroughly for malicious before making them public. Moreover, users can verify the application's trustworthiness by checking reviews from other users. Download applications from the internet or third-party app stores like APKPure may contain the application with malicious code [22].

- Protect all mobile applications and devices with a strong password. Use advanced features of passwords like fingerprint or face recognition, which makes the user's phone even stronger, and it becomes difficult to steal data from the locked phone.

- Use robust anti-virus software or download anti-malware on mobile devices. The anti-virus software will help the user to protect their device from various malware applications that sometimes get downloaded automatically.

- Always read the terms and privacy policy because the user can get information like how to use that particular application and where the data has been shared.

- It is good to turn off Bluetooth when not using it. It may reduce the chances of hackers getting the data through Bluetooth, and it will also cut down your battery usage.

- Instead of using public WiFi, stick to using a virtual private network (VPN) to encrypt all data transfer so that hackers cannot access them.

- Use up to date operating system in the device. Sometimes developers provide more security patches in the updated version, which makes the application stronger than before.

## X. CONCLUSION

Mobile computing is a very vast field, and it is very challenging to handle security threats. This paper surveys various security threats like downloadable application threats, web-based threats, Network security threats, and physical threats. Furthermore, this paper presented a cryptographic approach in mobile applications and how someone can keep their phones safe using cryptographic techniques. Also, this paper discussed security measures to keep the mobile device safe from the various malware software and also keep it safe from hackers.

## XI. REFERENCES


[1] Ryan Farmer, “A brief guide to android security”

[2] Sardasht, M., M. Bakhtiar, and M. Rebwar. "Mobile Application Security Platforms Survey." International Journal of Computer Applications 133.2 (2016): 40-46.

[3] Blondel, Vincent D., Adeline Decuyper, and Gautier Krings. "A survey of results on mobile phone datasets analysis." EPJ data science 4.1 (2015): 10.

[4] S. O’Dea, “Smartphone users worldwide 2016-2023”

[5] Statista. “Number of smartphone users worldwide from 2016 to 2023” [Online] Available at: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

[6] Khan, Jalaluddin, Haider Abbas, and Jalal Al-Muhtadi. "Survey on mobile user's data privacy threats and defense mechanisms." Procedia Computer Science 56 (2015): 376-383

[7] Sujithra, M., G. Padmavathi, and Sathya Narayanan. "Mobile device data security: a cryptographic approach by outsourcing mobile data to cloud." Procedia Computer Science 47 (2015): 480-485.

[8] Mcafee (2015), —Threats Predictionsǁ, [online]. Available at: http://www.mcafee.com/es/resources/misc/infographicthreats-predictions-2015.pdf

[9] “Various Security Threats” [Online] Available at: https://www.le-vpn.com/wp-content/uploads/2017/03/Smart-Phone-Security-Threats1200x628.jpg

[10] Norton. “Malware attacks” [Online]. Available at: https://us.norton.com/internetsecurity-malware-malware-101-how-do-i-get-malware-complex-attacks.html

[11] Spyware. Wikipedia.org [Online]. Available at: https://en.wikipedia.org/wiki/Spyware

[12] LE VPN. “SECURITY CHALLENGES ON MOBILE DEVICES” [Online]. Available at: https://www.le-vpn.com/security-challenges-on-mobile-devices/

[13] Lookout. “What is mobile threat?” [Online]. Available at: What is a mobile threat? (lookout.com)

[14] Imperva. “Phishing attacks” [Online]. Available at: https://www.imperva.com/learn/application-security/phishing-attack-scam/#:~:text=What%20is%20a%20phishing%20attack,instant%20message%2C%20or%20text%20message

[15] Cynet. “BROWSER EXPLOITS – LEGITIMATE WEB SURFING TURNED DEATH TRAP” [Online]. Available at: https://www.cynet.com/blog/browser-exploits-legitimate-web-surfing-turned-death-trap/

[16] Bluetooth. Wikipedia.org [Online]. Available at: https://en.wikipedia.org/wiki/Bluetooth

[17] [Online]. Available at: http://ijsrcseit.com/CSEIT1833315

[18] Tutorials Point. “Cryptography just for beginners.” [online] Available: cryptography_tutorial.pdf (tutorialspoint.com), pg.11

[19] “Symmetric vs. Asymmetric Encryption – What are differences?” [Online] Available at: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

[20] Apriorit. “Top 7 Methods of Data Encryption in Android Applications” [Online] Available at: https://www.apriorit.com/dev-blog/612-mobile-cybersecurity-encryption-in-android

[21] “Cryptography in Mobile Apps” [Online] Available at: https://mobile-security.gitbook.io/mobile-security-testing-guide/general-mobile-app-testing-guide/0x04g-testing-cryptography#:~:text=Symmetric%2Dkey%20encryption

%20algorithms%20use,method%20requires%20careful%20key%20management.

[22] Nagarjun, P. M. D., and S. A. Shaik. "Review of Mobile Security Problems and Defensive Methods." International Journal of Applied Engineering Research 13.12 (2018): 10256-10259.

[23] Norton. “What is rootkit? And how to stop them” [Online] Available at: https://us.norton.com/internetsecurity-malware-what-is-a-rootkit-and-how-to-stop-them.html#:~:text=Rootkits%20are%20a%20type%20of,to%20remotely%20control%20your%20computer.

[24] Pullela, Srikanth. "Security issues in mobile computing." Department of Computer Science, University of Texas at Arlington (2002).