ISSN (e): 2250 – 3005 || Volume, 09 || Issue, 6 || June– 2019 ||
International Journal of Computational Engineering Research (IJCER)

Android User Level Security

[1]Jyothy Joseph, [2]Dr.K.Nirmala
Research Scholar Quaid-E-Millath College for Women, Chennai - 600 002, Tamilnadu,India.
Assoc. Professor,Dept. of Computer Science, Quaid-E-Millath College for Women, Chennai - 600 002, Tamilnadu,India
Corresponding Author: Jyothy Joseph

ABSTRACT

Android operating system provides multiple user-level security options, which helps in protecting mobile devices and its contained data. This paper explains about various user-level security features available in Android OS and briefs how to enable the respective security options. This Analysis has been done based on the Android 9 (Pie) version. Most of these security features are disabled by default, need basis users can enable each one. The key advantages of these security options are find the device or wipe-out the device if its physically lost, setup application level security, manage and control user notifications, provide safe browsing configuration, lock the device to protect from unauthorized access, enable biometric security features, enable safe mobile app downloads, provide secure notification messages, restrict unauthorized application access, etc.

KEYWORDS: Android, Operating system, User level security, Mobile Device,Biometric Security

Date of Submission: 05-06-2019 Date of acceptance:20-06-2019

I. INTRODUCTION

Android, though a widely used open source mobile device platform, its security is always a hot topic. This operating system provides a lot of powerful security features. Few of its security features come along with the OS and few others need to be configured based on a need basis. This operating system is packed with multiple software and hardware-based security options. Android integrates themobile device industry prominent security features and meticulously work with device owners to keepthe OS safety up-to-date. Android OS is used on a wide range of devices like smartphones, tablets, wearable devices, smart TVs, gaming boxes, and set-top-boxes. Android operating system is built on top of the Linux kernel. All device resources, like camera functions, GPS data, Bluetooth functions, telephony functions, network connections, etc. are accessible through the operating system. A set of pre-installed applications are available on the Android platform and these applications manage the primary functionalities of the mobile device. A huge set of third-party applications are also available to configure in the Android OS. Android is designed with multi-layered security features and is capable to support all the latest and industry-leading security features.

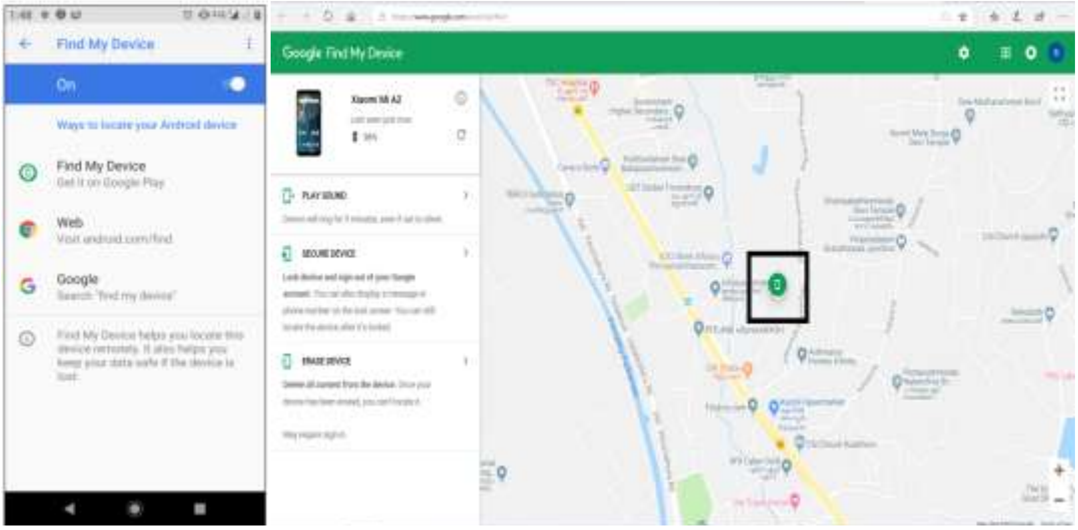
All available user-level security features are not mandatory to protect the device and its data. In most of the cases, device owners enable the required features based on the need basis. Below are the key user-level security features:

1. Find my Device
2. App permission
3. Notification Permission
4. Safe Browser settings
5. Screen Lock
6. Biometric Security
7. Smart lock
8. Google Play Protect
9. Emergency contact
10. Lock Screen Message
11. Lock Screen Notifications
12. Screen pinning
13. Enable Lockdown mode

1. Find my Device: This option helps to remotely track your android device. In addition to locating your phone, Find My Device lets you ring your device, remotely lock it, or even erase the data if the device goes missing or stolen. By default, this option would be enabled. If the device is misplaced or lost, this option helps to detect the phone location through https://www.google.com/android/findURL and perform the following actions.
Figure-1 gives the mobile application view and the webpage view for this option.

- Play Sound: This option can play a sound so that the devicerings for around five minutes (even if the device is on silent mode). This feature is helpful if the map indicates that the phone is within earshot but can't see it.
- Secure Device: This option helps to lock the device and send a custom notification/ message in the device. Also,this option can be used to remotely sign out from the current login account.
- Erase Device: This option helps in wiping out all the data remotely from the device.

Feature Path: Settings → Security & location → Find My Device



Find My Device

On

Ways to locate your Android device

Find My Device
Get it on Google Play

Web
Visit android.com/find

Google
Search "find my device"

Google Find My Device

Xiaomi Mi A2

PLAY SOUND

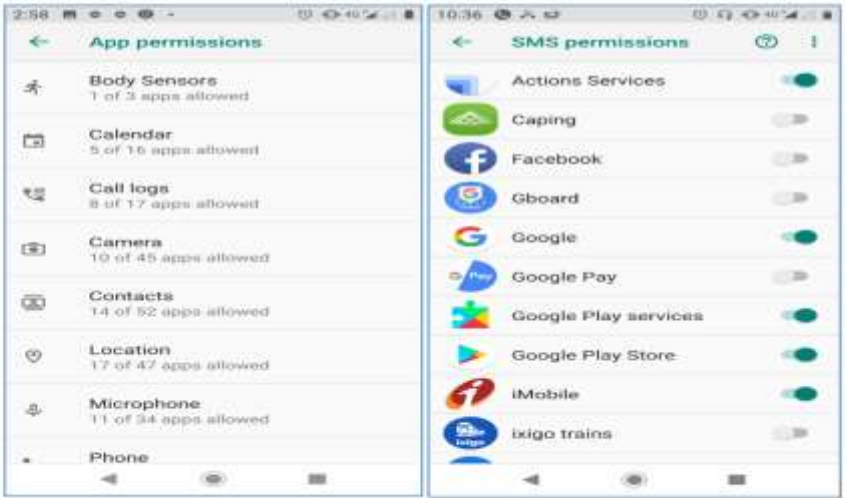
SECURE DEVICE

ERASE DEVICE

Figure-1 Find my Device

2. App Permissions: App permission feature helps in protecting the sensitive user datacontained in the device. Using this option, users can configure the permissions that installed applications can access.A common instance is usage of SMS (Short message service) which is unsecured data. In many scenarios, this option is used to communicate secured information like OTP (one-time password). Consequently, unauthorised access to SMS application is a big threat. By using the app permission feature, devices users can restrict the data access in a more secured way.

Feature Path: Settings → Apps & Notifications → App Permissions



App permissions

Body Sensors
1 of 3 apps allowed

Calendar
5 of 16 apps allowed

Call logs
8 of 17 apps allowed

Camera
10 of 45 apps allowed

Contacts
14 of 52 apps allowed

Location
17 of 47 apps allowed

Microphone
11 of 34 apps allowed

Phone

SMS permissions

Actions Services ●

Caping ○

Facebook ○

Gboard ○

Google ●

Google Pay ○

Google Play services ●

Google Play Store ●

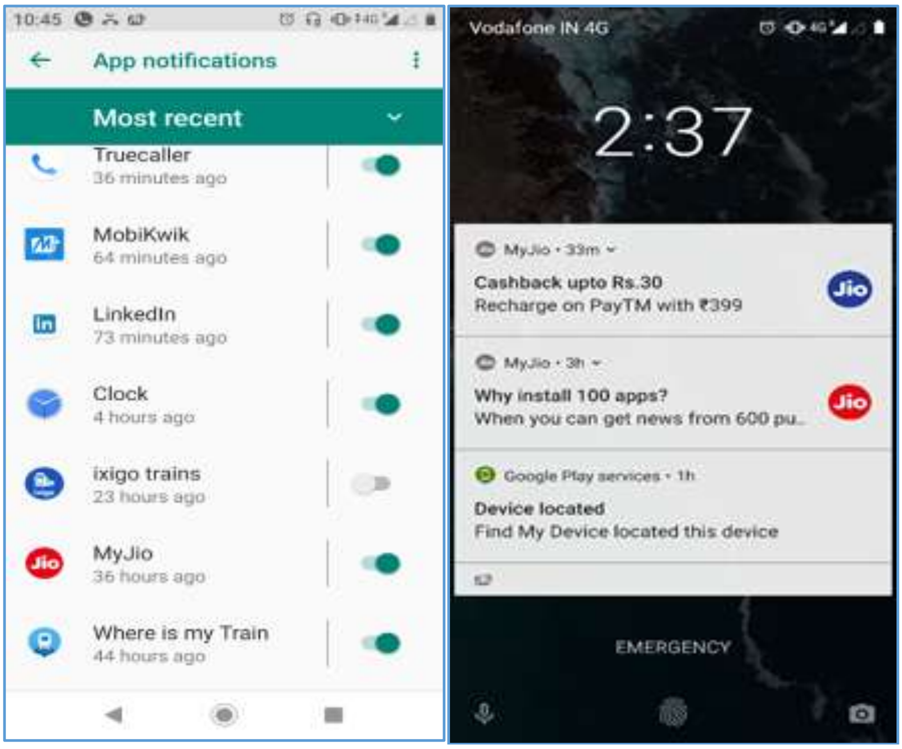
iMobile ●

ixigo trains ○

Figure-2 App Permissions

3. Notification Permissions:Notification overview is one of the attractive features of Android OS. This feature if overlooked, exposesthe user data or secure messages to others, even if the device is locked. Using proper configuration, users can make use of the system settings to choose the level of details visible in the lock screen notifications, including the option to disable all lock screen notifications.

Feature Path: Settings → Apps & Notifications → Notifications



10:45

App notifications

Most recent

Truecaller
36 minutes ago

MobiKwik
64 minutes ago

LinkedIn
73 minutes ago

Clock
4 hours ago

ixigo trains
23 hours ago

MyJio
36 hours ago

Where is my Train
44 hours ago

Vodafone IN 4G

2:37

MyJio • 33m
Cashback upto Rs.30
Recharge on PayTM with ₹399

MyJio • 3h
Why install 100 apps?
When you can get news from 600 pu...

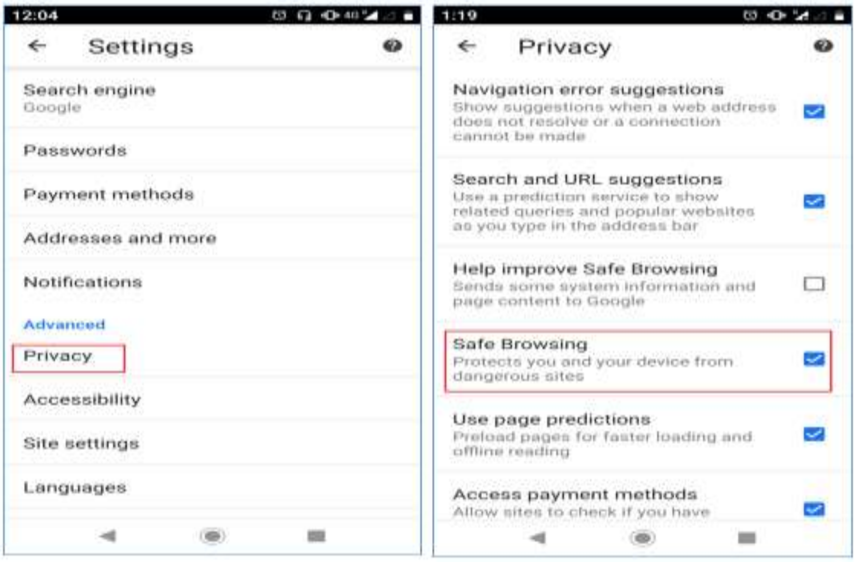
Google Play services • 1h
Device located
Find My Device located this device

EMERGENCY

Figure-3 Notification Permissions

4. Safe Browser settings: GoogleChrome is the default browser set for Android OS. Chrome has a secure browsing feature called Safe Browsing mode. With Safe Browsing mode enabled, users are given warningswhen they attempt to enter or load any suspicious web URL or download dangerous files. In addition to phishing or malware attacks, it will also warnthe user about sites that prompt to install unwanted software. This feature helps to protect the device from malwares to gets load from malicious websites.

Feature Path: Chrome → Settings → Privacy → Safe Browsing



12:04

Settings

Search engine
Google

Passwords

Payment methods

Addresses and more

Notifications

Advanced

Privacy

Accessibility

Site settings

Languages

1:19

Privacy

Navigation error suggestions
Show suggestions when a web address does not resolve or a connection cannot be made ☑

Search and URL suggestions
Use a prediction service to show related queries and popular websites as you type in the address bar ☑

Help improve Safe Browsing
Sends some system information and page content to Google ☐

Safe Browsing
Protects you and your device from dangerous sites ☑

Use page predictions
Preload pages for faster loading and offline reading ☑

Access payment methods
Allow sites to check if you have ☑

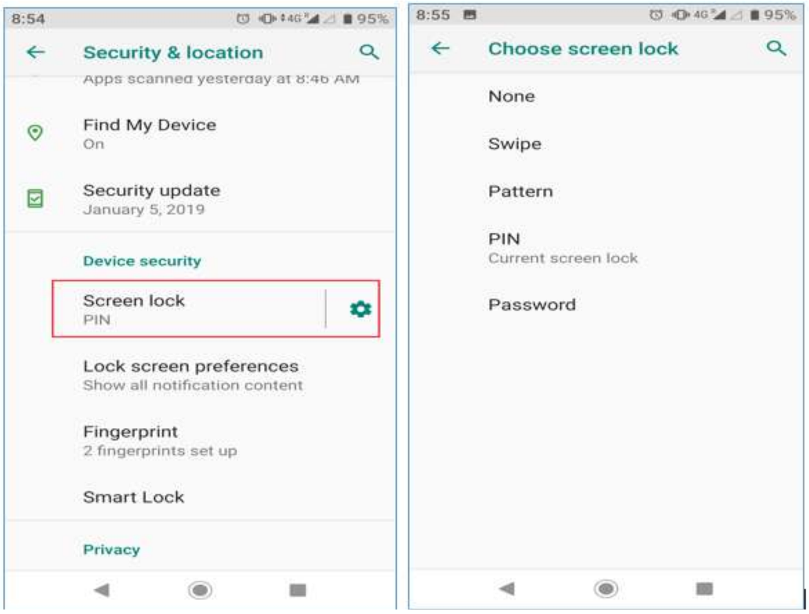
Figure-4 Safe Browsing

5. Screen Lock: This is one of the simplest and most effective security features to protect device contents via physical access. This feature helps the usertoprotect the device with any of feature mentioned below.

- Swipe Lock
- Number lock
- Pattern lock
- PIN lock
- Password lock

If the Swipe lock is enabled, the user has to follow a particular swipe motion to access the device. For the Number lock feature, the user can seta particular number to enable the device. If pattern lock is enabled, user has to draw that particular pattern to enable the device. PIN lock helps to set a particular PIN to enable the device. Password lock helps to set a password consisting of numbers and alphabets for device enabling.

Feature Path: Settings → Security & location → Screen lock



8:54 95%

Security & location

Apps scanned yesterday at 8:46 AM

Find My Device
On

Security update
January 5, 2019

Device security

Screen lock
PIN

Lock screen preferences
Show all notification content

Fingerprint
2 fingerprints set up

Smart Lock

Privacy

8:55 95%

Choose screen lock

None

Swipe

Pattern

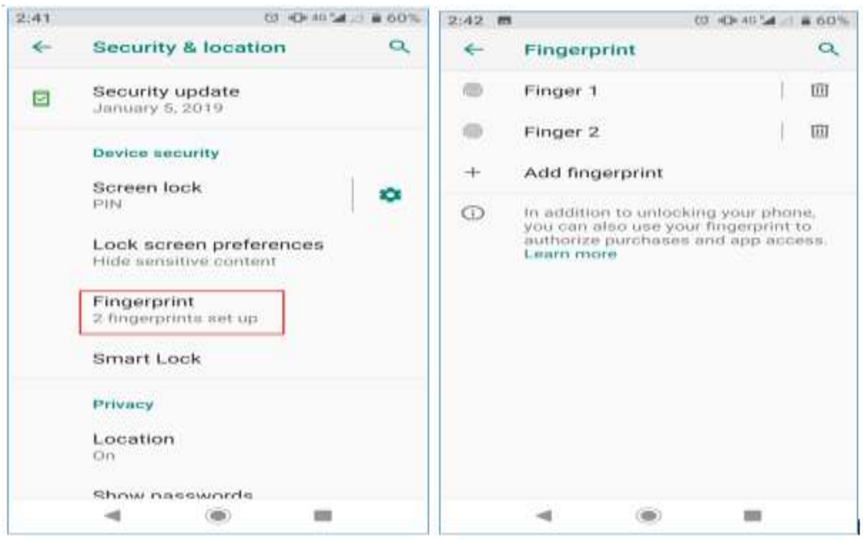
PIN
Current screen lock

Password

Figure-5 Screen Lock

6. Biometric Security: Android 9 currently supports only fingerprint scanning. Other biometric feature supports are forthcoming or are being developed. Fingerprint biometrics helps to enable the mobile device based on fingerprint validation. The device owner can add multiple fingerprints for validation purposes.

Feature Path: Settings → Security & location → Fingerprint



2:41 60%

Security & location

Security update
January 5, 2019

Device security

Screen lock
PIN

Lock screen preferences
Hide sensitive content

Fingerprint
2 fingerprints set up

Smart Lock

Privacy

Location
On

Show passwords

2:42 60%

Fingerprint

Finger 1

Finger 2

Add fingerprint

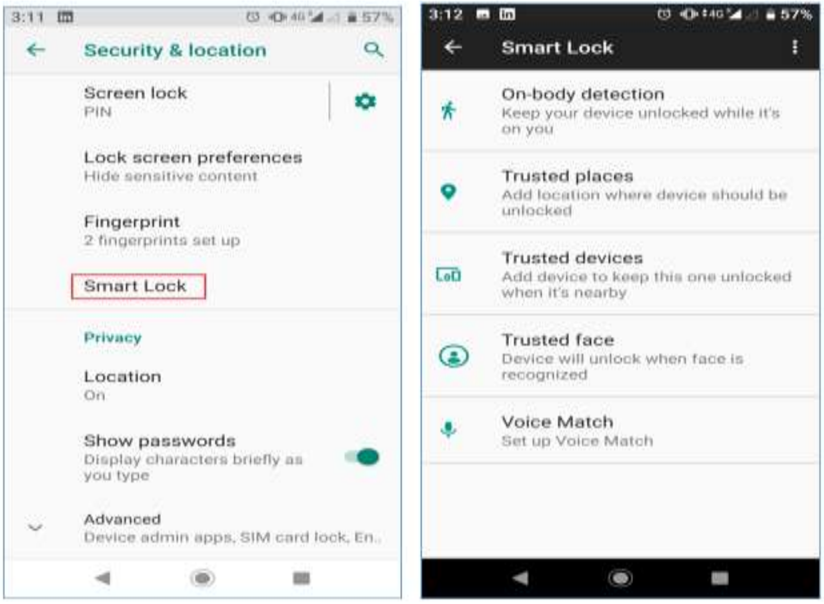
In addition to unlocking your phone, you can also use your fingerprint to authorize purchases and app access. Learn more

Figure-6 Biometric Security

7. Smart Lock: This functionality helps in unlocking the device without prompting it to do any specific task. Below are the five options to enable the smart lock. All these features might not be supported on all devices.

- **On-body Detection**: This smart lock feature can detect and thus unlock when the device is on the user's body (in the hand or in the pocket).
- **Trusted Places**: Users can add trusted locations (home or office) to enable the device. The device gets automatically unlocked upon reaching the added locations. This feature working is based on the GPS in the device.
- **Trusted Devices**: Users can set up trusted devices like Bluetooth watch, car stereo etc. When the added device gets connected to a mobile device, it will get automatically unlocked.
- **Trusted Faces**: This functionality lets users unlock the phone through facial recognition. User can add trusted faces through a camera and when theadded face comes in front of the camera, the device gets automatically unlocked.
- **Voice match**: Users can set up voice detection in their devices and can add different voices too.The device can unlock itself when the it detects a voice match.

Feature Path: Settings → Security & location → Smart Lock



3:11 57%

Security & location

Screen lock
PIN

Lock screen preferences
Hide sensitive content

Fingerprint
2 fingerprints set up

Smart Lock

Privacy

Location
On

Show passwords
Display characters briefly as you type

Advanced
Device admin apps, SIM card lock, En..

3:12 57%

Smart Lock

On-body detection
Keep your device unlocked while it's on you

Trusted places
Add location where device should be unlocked

Trusted devices
Add device to keep this one unlocked when it's nearby

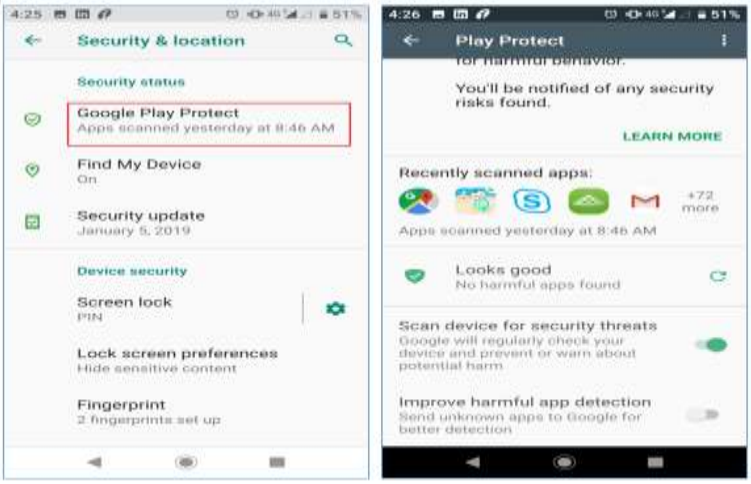
Trusted face
Device will unlock when face is recognized

Voice Match
Set up Voice Match

Figure-7 Smart Lock

8. Google Play Protect: This is Android's internal security system. By default, this feature is enabled in all the Android mobile devices. This feature helps to continuously scan the device and warn or identify if any potentially harmful applications are present and remove them.

Feature Path: Settings → Security & location → Google Play Protect



4:25 51%

Security & location

Security status

Google Play Protect
Apps scanned yesterday at 8:46 AM

Find My Device
On

Security update
January 5, 2019

Device security

Screen lock
PIN

Lock screen preferences
Hide sensitive content

Fingerprint
2 fingerprints set up

4:26 51%

Play Protect

for harmful behavior.

You'll be notified of any security risks found.

LEARN MORE

Recently scanned apps:

+72 more

Apps scanned yesterday at 8:46 AM

Looks good
No harmful apps found

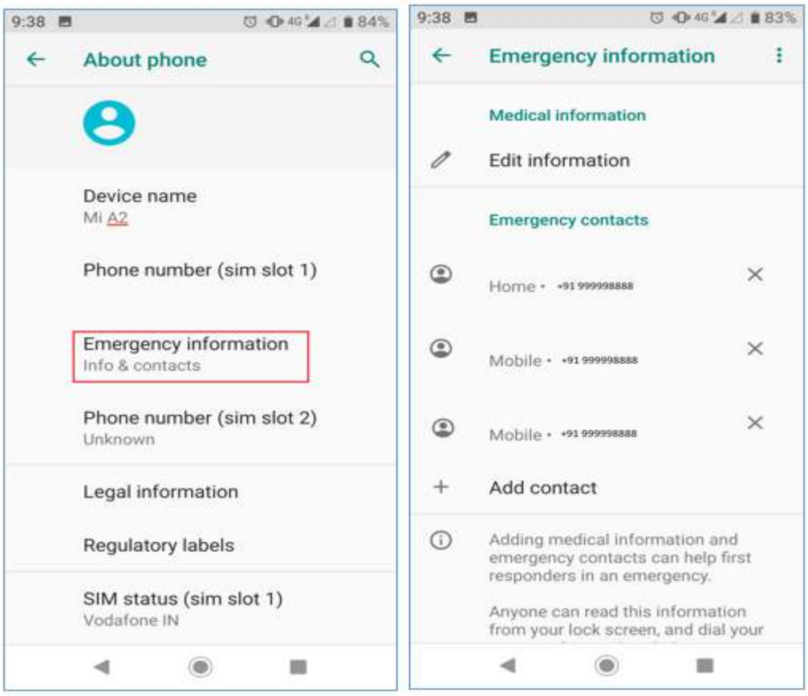
Scan device for security threats
Google will regularly check your device and prevent or warn about potential harm

Improve harmful app detection
Send unknown apps to Google for better detection

Figure-8 Google Play Protect

9. Emergency contact: This feature can be used for multiple purposes. One usage is for physical emergency or security. In case of any emergency, this feature helps to access the contacts that are added as emergency contacts even when the phone is locked. This can also be used to add owner information and therefore identify the owner in case the device is lost and is found by someone. This feature wouldn't require unlocking the phone by an unknown person.

Feature Path: Settings →About Phone → Emergency Information → Emergency Contacts



9:38

About phone

Device name
Mi A2

Phone number (sim slot 1)

Emergency information
Info & contacts

Phone number (sim slot 2)
Unknown

Legal information

Regulatory labels

SIM status (sim slot 1)
Vodafone IN

9:38

Emergency information

Medical information

Edit information

Emergency contacts

Home • +91 9999988888

Mobile • +91 9999988888

Mobile • +91 9999988888

Add contact

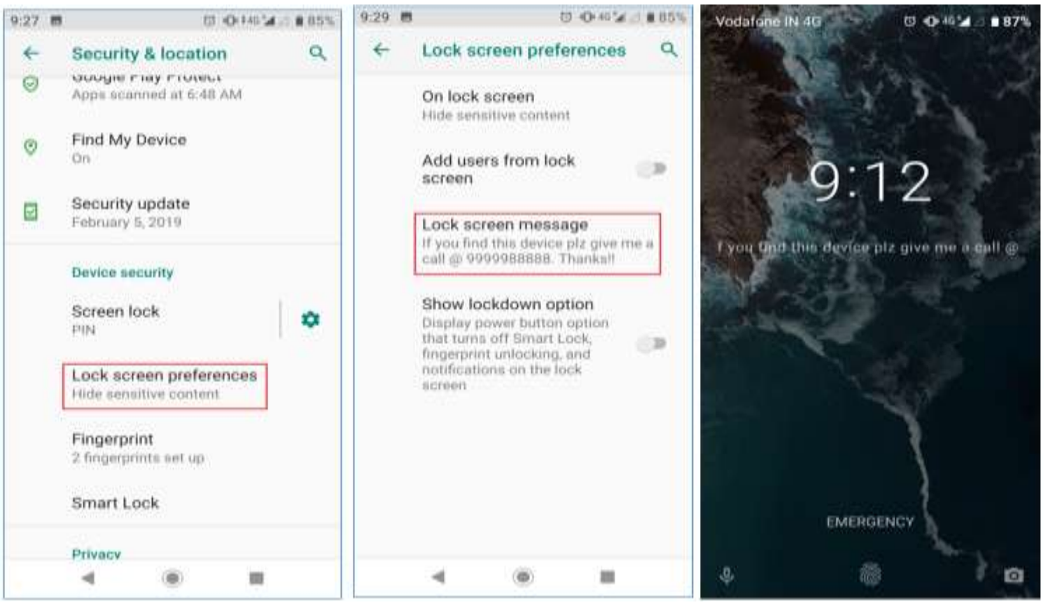
Adding medical information and emergency contacts can help first responders in an emergency.

Anyone can read this information from your lock screen, and dial your

Figure-9 Emergency Contact

10. Lock Screen Message: This feature can be used for physical emergency similarly like Emergency contacts. User can provide a Lock screen message containing owner information etc. to display when the device is in Lock screen mode. This option helps to reach or identify the owner in case the device is misplaced or lost.

Feature Path: Settings →Security & location → Lock screen preferences → Lock screen Messages



9:27

Security & location

Google Play Protect
Apps scanned at 6:48 AM

Find My Device
On

Security update
February 5, 2019

Device security

Screen lock
PIN

Lock screen preferences
Hide sensitive content

Fingerprint
2 fingerprints set up

Smart Lock

Privacy

9:29

Lock screen preferences

On lock screen
Hide sensitive content

Add users from lock screen

Lock screen message
If you find this device plz give me a call @ 9999988888. Thanks!!

Show lockdown option
Display power button option that turns off Smart Lock, fingerprint unlocking, and notifications on the lock screen

Vodafone IN 4G

9:12

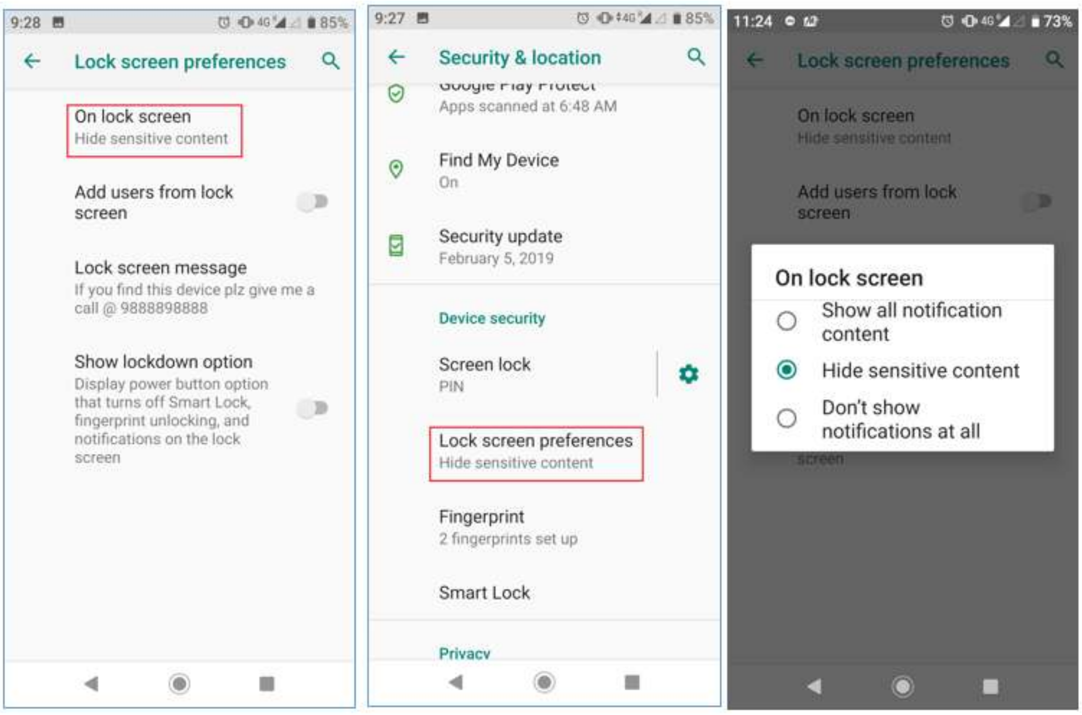
f you find this device plz give me a call @

EMERGENCY

Figure-10 Lock Screen Message

11. Lock Screen Notification: This feature helps to manage the notifications displayed on the device lock screen. Secured messages like one-time passwords (OTP), security keys, etc. which are displayedon the screen may not always be secured. This feature helps to manage these messages in a more securedmode. Lock screen notifications can be customized only to specific applications and sensitive contents also. This feature would show the notifications on the lock screen but the sensitive content would be locked.

Path: Settings →Security & location → Lock screen preferences →On lock screen



9:28

Lock screen preferences

On lock screen
Hide sensitive content

Add users from lock screen

Lock screen message
If you find this device plz give me a call @ 9888898888

Show lockdown option
Display power button option that turns off Smart Lock, fingerprint unlocking, and notifications on the lock screen

9:27

Security & location

Google Play Protect
Apps scanned at 6:48 AM

Find My Device
On

Security update
February 5, 2019

Device security

Screen lock
PIN

Lock screen preferences
Hide sensitive content

Fingerprint
2 fingerprints set up

Smart Lock

Privacy

11:24

Lock screen preferences

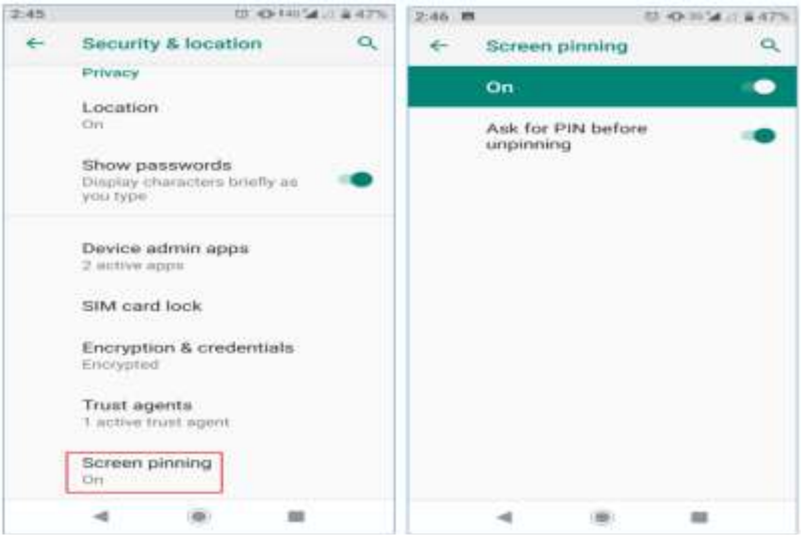
On lock screen

○ Show all notification content
● Hide sensitive content
○ Don't show notifications at all

Figure-11 Lock Screen Notifications

12. Screen Pinning: This security feature enables the device and limits access to only a specific pinned application. All the other applications or features of the device would be disabled or locked. This security feature is helpful in situations whenthe device is borrowed by someone. For example, the user wants to give the device to an untrusted person for short time to use any application. In this scenario the user can pin the required app and can give it to that person.

Path: Settings →Security & location →Screen pinning



2:45

Security & location

Privacy

Location
On

Show passwords
Display characters briefly as you type

Device admin apps
2 active apps

SIM card lock

Encryption & credentials
Encrypted

Trust agents
1 active trust agent

Screen pinning
On

2:46

Screen pinning

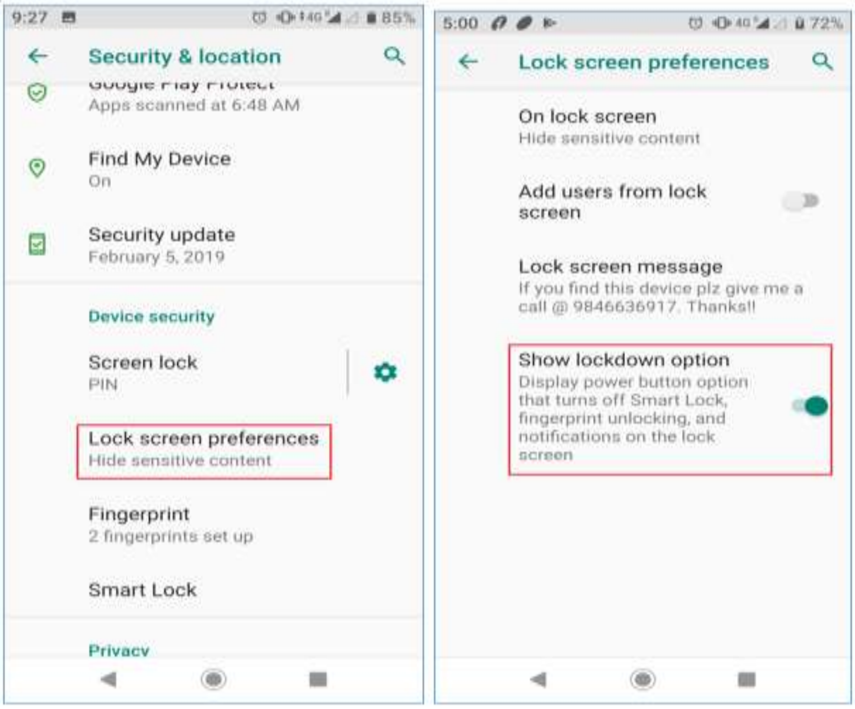
On

Ask for PIN before unpinning

Figure-12 Screen Pinning

13. Enable Lockdown Mode: This feature helps to protect the device from unauthorized usage bydisabling biometric authentication (fingerprint scanner, facial and voice recognition) temporarily. This mode helps to protect the device and the contained private data from unauthorized access while the owner is not watching. Once this feature is enabled, the only way to enable the device is by entering the PIN code, password or pattern lock to use the device. This feature can be used for dual authentication on secured apps.

Path: Settings →Security & location →Lock screen preferences → Show lockdown option



9:27 85%

Security & location

Google Play Protect
Apps scanned at 6:48 AM

Find My Device
On

Security update
February 5, 2019

Device security

Screen lock
PIN

Lock screen preferences
Hide sensitive content

Fingerprint
2 fingerprints set up

Smart Lock

Privacy

5:00 72%

Lock screen preferences

On lock screen
Hide sensitive content

Add users from lock screen

Lock screen message
If you find this device plz give me a call @ 9846636917. Thanks!!

Show lockdown option
Display power button option that turns off Smart Lock, fingerprint unlocking, and notifications on the lock screen

Figure-13 Lockdown Mode

II. CONCLUSION

Android is the most popular open source mobile operating system. On the contrary, Android is also the most attractive platform for malicious hacking activities nowadays If the device users do not make proper and effective useof the security features installed in Android devices, there is a highchance of the device gettingvulnerable to malware and phishing attacks. In majority of the cases,the user’s ignorance paved the way in making secured content accessible to outsiders and hackers.Also, many of the mobile applications are collecting a lot ofdata from the device without proper consent from the device owner. Android OS provides multiple user-level security options to device users. The users must be entirely aware of all these features and enable it to keep the device and data secure. Android majorly gives the following type of security features to device users: Application level security, Data level security, Access level security, Physical security, Notification securities, Browser level security, Biometric security, Screen level access security, Secure application downloads, Emergency contact security, Security messages management, etc. Device users can use these security features on a need basis to keep safe the mobile device and its contained data.

REFERENCES

[1]. https://source.android.com/security

[2]. International Journal of Trend in Research and Development, Volume 2(5), ISSN 2394-9333 www.ijtrd.com

[3]. Shubhankar Mukherjee et al, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.3, March- 2015

[4]. Android Security: A Survey of Security Issues AndDefensesPersin Kaur Granthi1, Mrs. S. M. Bansode2International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 04 Issue: 07 | July -2017 www.irjet.net p-ISSN: 2395-0072

[5]. Android Security Issues and Solutions International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2017)

Jyothy Joseph" Android User Level Security" International Journal of Computational Engineering Research (IJCER), vol. 09, no. 6, 2019, pp 48-55