

Study on Security Ensuring Tools and Techniques for Mobile Devices

BY

MAHTABUR RAHMAN SOBUJ

ID: 211-25-015

This Report Presented in Partial Fulfillment of the Requirements for the
Degree of Masters of Science in Computer Science and Engineering

Supervised By

Dr. Sheak Rashed Haider Noori

Associate Professor and Associate Head

Department of CSE

Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

Dhaka, Bangladesh

January 2022

APPROVAL

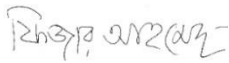
This Thesis report titled “Study on Security Ensuring Tools and Techniques for Mobile Devices” submitted by “Mahtabur Rahman Sobuj” ID: “211-25-015” to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of M.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 19-01-2021.

BOARD OF EXAMINERS



Dr. Touhid Bhuiyan
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Chairman



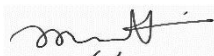
Dr. Fizar Ahmed
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Naznin Sultana
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Dr. Mohammad Shorif Uddin
Professor
Department of Computer Science and Engineering
Jahangirnagar University

External Examiner

DECLARATION

I hereby declare that, this Thesis report paper has been done by me under the supervision of Dr. **Sheak Rashed Haider Noori, Associate Professor and Associate Head, Department of CSE** Daffodil International University. I also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:



Dr. Sheak Rashed Haider Noori
Associate Professor and Associate Head
Department of CSE
Daffodil International University

Submitted by:



Mahtabur Rahman Sobuj
ID: 211-25-015
Department of CSE
Daffodil International University

ACKNOWLEDGMENT

Firstly I express our heartiest thanks and gratefulness to **Almighty Allah** for his divine blessing makes us possible to complete the final year Thesis successfully.

I am really grateful and wish profound indebtedness to **Dr. Sheak Rashed Haider Noori, Associate Professor and Associate Head**, Department of CSE, Daffodil International University, Dhaka. Deep Knowledge & keen interest of supervisor in the field of “*Study on Security Ensuring Tools and Techniques for Mobile Devices*” to carry out this Thesis. Her endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stage have made it possible to complete my Thesis.

I would like to express heartiest gratitude to **Professor Dr. Touhid Bhuiyan, Professor and Head**, Department of CSE, for her kind help to finish my Thesis and also to other faculty member and the staff of CSE department of Daffodil International University.

I would like to thank entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, I must acknowledge with due respect the constant support and patients of parents.

ABSTRACT

This project is on the study of security ensuring techniques and tools for mobile devices. Mobile devices are now very essential in our daily life. We cannot imagine a day without mobile devices and particularly mobile phones. Its functions are also increasing. The use of mobile devices is increasing in every sector day by day. Our important and personal data are stored on the mobile phones. We need to secure this data. Data can be theft by cyber criminals. Data can be missing used by the cyber criminals. An overview of various techniques and tools are presented in this project report. The use of some mobile security tools is explored to show how mobile data can be secured. The tools can be used to detect malicious apps and vulnerabilities. A comparison of the mobile security tools and techniques is also presented.

TABLE OF CONTENTS

CONTENTS	Page No
Approval	i
Declaration	ii
Acknowledgement	iii
Abstract	iv
CHAPTER1: INTRODUCTION	1-2
1.1 Introduction	1
1.2 Motivation	1
1.3 Objectives	1-2
1.4 Outline	2
CHAPTER 2: BACKGROUND	3-4
2.1 Introduction	3
2.2 Related work	3-4
CHAPTER 3: TECHNICAL TERMS	5-8
3.1 Techniques for ensuring mobile security	5-6
3.2 Mobile device security tools	6-7
CHAPTER 4: RESEARCH METHODOLOGY	8-24
4.1 Various Mobile Devices	8
4.2 Mobile application	9
4.3 Mobile Platforms	9
4.4 Mobile App Architecture Design	10-11
4.5 Mobile Application Component	11-12
4.6 Mobile Security Types	12-14
4.7 Threats To Mobile Devices	14-16
4.8 Mobile security threats	16-19

4.9 Misuses And Cyber Attack On Mobile Devices	19-20
4.10 Vulnerabilities Of Mobile Devices Software And Hardware	20-21
4.11 Mobile Viruses	21-23
4.12 Mobile Data Theft	23-24
CHAPTER 5: RESULT AND PREDICTION	25-29
5.1 Comparative Analysis	25
5.2 Discussion	25-26
5.3 Screenshots of Mobile Security Software	27-29
CHAPTER 6: FUTURE WORK &CONCLUSION	30
6.1 Future Work	30
6.2 Conclusion	30
REFERENCES	31

LIST OF FIGURES

FIGURES	PAGE NO
Figure 4.2 : Mobile application architecture design	9
Figure 4.8 : The anatomy of viruses	22

LIST OF TABLE

FIGURES	PAGE NO
Table 5.2.1 : Comparison of different software	26-27
Table 5.2.2 : Security level	27

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

Security is freedom from, or resilience against, ability harm (or other undesirable coercive change) as a result of others. Beneficiaries of security may be of persons and social groups, objects and institutions, ecosystems or any other entity or phenomenon vulnerable to unwanted change [1].

Security basically refers to safety from adversarial forces, but it has an extensive variety of different senses: for example, as the absence of harm, as the presence of a crucial good, as resilience against capacity damage or harm, as secrecy as containment and as a state of mind.

mobile device security refers to the measures designed to protect touchy information stored on and transmitted by laptops, smart phones, tablets, wearable's, and other portable devices. At the foundation of mobile tool security is the goal of retaining unauthorized users from getting access to the company network.

1.2 MOTIVATION

Mobile device is now an essential part of our life. Its security is important for all of us. Unsecure devices mobile data may steal by theft. Many people don't know about the importance of mobile security. They even don't know that their personal data can be stealing from mobile. Mobile devices, such as smart phones and tablets, have been widely used for personal and business purposes [2]. Peoples need to introduce more and more about this. If people more conscious about this mobile security then cybercriminal cannot be harm their mobile. Cybercrime can also be reducing day by day. So I decided to represent about this topics. Here we will discuss about mobile security and mobile security tools.

1.3 OBJECTIVES

The objectives of this project report are making people aware of-

- The mobile technology

- How this technology works
- The mobile security
- The reliability issues of mobile security
- The necessary steps that can be taken to prevent such threats

1.4 OUTLINE

Here is the outline of this research project paper-

Chapter 1 contains the Introduction with a short discussion about the mobile device security & motivation of this report is discussed. Also, the objectives are pointed out along & Chapter 2 contains the background for introduction and related work. Chapter 3 contains the Technical terms for ensuring mobile security. Chapter 4 Research Methodology for contains-

- Mobile platforms
- Mobile App Architecture Design
- Mobile application component
- Mobile security types
- Threats to mobile devices
- Misuses and Cyber Attack on Mobile Devices
- Vulnerabilities of mobile devices software and hardware
- Mobile viruses

Chapter 5 it's provide about Result and prediction on full research base review. Finally Chapter 6 ends with Future Work and Conclusion.

CHAPTER 2

BACKGROUND

2.1 INTRODUCTION

Now a day's uses of mobile device are increasing day by day for personal use and business purposes. Today 67.03% of the world's population has mobile devices. In mobile devices may have once personal data, password etc. While these devices provide more features and functionality, they also introduce new risks and threats [8]. Thus, mobile devices are easy targets for cyber criminals [1]. Cyber criminals can attack it easily. They can misuse your data and also can theft bank balance. So it's important to ensure mobile security. Using tools we can ensure our mobile security. Security tools can detect vulnerability and malicious attack on mobile devices.

Many people don't know about mobile viruses and how to protect from them. So it's must be include on educational activities. Mobile attacks are increasing day by day. First mobile virus founded in June 2004. It's written in C++. Mobile is a multiple entrance open system. Its uses central data management. A mobile have many unique functions. Its uniqueness makes challenges to develop mobile security.

In this research study work we will see different types of security threats and four testing approaches for mobile security. Here we will compare security tools by installing them on mobile. We also investigate future changes of mobile security tools.

2.2 RELATED WORK

In [1] the authors tell about the mobile security testing approaches. Mobile devices data are sensitive. Its can carry personal information. Mobile devices have different more components then common personal computers [3]. Mobile device security is very much important.

In this paper, for mobile security they present four testing approaches. Those are mobile forensic, penetration test, static analysis, and dynamic analysis [1]. Their testing result indicates that mobile security testing tools needs update. They are still in early ages.

Here [12] the author's purpose is to determine outgoing mobile security risk. And they provide mobile device security suggestion for practical small and medium size enterprise (SMEs). The SME mobile device invests in more expensive maximum

security technologies. In order to protect enterprise and customer data and information invest in less expensive minimum security technologies with increased risk, or postpone the business mobility strategy [12].

In “A location based mechanism for mobile device security” the author said they describe about a location based authentication process. That takes action servers called policy beacons. Location data and control device behavior are provides it. Mobile devices are vulnerable to theft and loss due to their small size. For mobiles characteristics they can use in common usage environment [4]. They also pose new risks [5]. To available policy beacons mobile devices determine their proximity and upon validation assume the designated organizational policy [5]. Take advantages of Bluetooth this process is designed to.

In [6] mobile device widely uses for business and personal purposes. Sensitive data are stored on mobile devices [7]. In this paper, they propose a framework on mobile devices, Mobile Guardian for security policy enforcement [6]. They said the frame work is secure and can adopt any mobile platform.

In Mobile Malware and Smart Device Security: Trends, Challenges and Solutions author discussed about the malware. Malware challenges and future trends they identified.

In smart devices to tackle the issue they propose and discuss an integrated security solution for cyber security [8].

In [9] their purpose is to focus on Google play store and their downloads. Some vulnerability was founded. They analyzed about the device to device (D2D) network.

They identified that most data transfer over mobile D2D network is unencrypted [9]. They provided security lessons and some suggestion of possible solution.

In [10] from a loyal and secure existence a lightweight process to isolate one or more android user land instances. This entity the Android instances are controls and manage. Its software provides an interface for remote administration and management of the device [10]. For secure network access they included several security extensions.

CHAPTER 3

TECHNICAL TERMS

3.1 TECHNIQUES FOR ENSURING MOBILE SECURITY

- **Use strong passwords/biometrics**

Robust passwords with fingerprint authenticator, make unauthorized get right of entry is almost not possible. If we need strong password then it should be over 8 characters. You can also add factor authentication. For unforeseen attacks don't always want a subject [21]. If your device stealing. Then they can access to it. Regularly change your password.

- **Ensure public or free Wi-Fi is protected**

Maximum of the free wifi points aren't encrypted. These free networks permit also malicious people. That's why they can find your data easily. We can use packages which tell us the about the wifi. WPA is extra easy in comparison to WEP. Whilst you aren't the use of them you have to also turn off wireless connectivity. It's not only avoid your automated connection it will safe your battery also.

- **Utilize VPN**

If you don't trust your network where you connected, you can use vpn. A vpn will securely connect to your network. In public wifi they can save your data. It's also useful when you enter less secure website. In terms of combating cybercrime you actually need to have a new mind-set.

- **Encrypt your device**

With a built-in encryption feature most mobile devices are bundled. Data unreadable happen when encryption occurs. Decryption converts into normal data. It can stop unauthorized access. For this you need this feature then you can encrypt your device [21]. Depending on your data size this process may take some time. Bigger data will

take more time. If the wrong encryption password is entered after a number of times mobile devices will automatically erase everything.

- **Install an antivirus application**

If you download any apps or file it can be packed malicious code. If you install this file your information can be leaked. So that you're private message can be insecure. To safe from this problem you can install antivirus application. Some antivirus programs provide greater functionalities. It will erase your data and block harmful callers also. And it also tells that which application is insecure. It also said to delete cookies.

- **Update to the latest software**

For vulnerability your device your firmware need also be vulnerable. Every time update latest software in your device. Google android and apples ios are Fundamental mobile tool firmware organizations. Roll out new updates occasionally on your mobile. To acknowledged vulnerabilities for your device maximum of those updates act as a safety patch. You might set up updates.

- ✓ Prevent auto fill – some website provides auto fills that why you don't need login every time. You must be avoiding this. And stop it from your browser.
- ✓ Log out – Applications, you have to log off each time you are done using them. Some are linked to one another. You must off it specially.
- ✓ Use only trusted stores – From secure stores download your apps.

3.2 MOBILE DEVICE SECURITY TOOLS

Mobile device security tools are:

- **Mobile device management (MDM)**

The first is called to mobile device management (MDM). Across all enterprise-owned devices MDM can be used to enforce a regular, authorized security model. Adjustments to the policy can mechanically be pushed to the devices remotely. There are a diffusion of MDM products to be had for phone systems. Protection group must consider MDM technology. To block the installation of new apps, which mitigates the threat related to malware brought through malicious apps MDM may even be used.

- **Sandboxing**

The second tool is sandboxing. The mobile device is separated into two sections with sandboxing [22]. Through sandbox all corporate data is stored in and accessed via one of the sections. It calls for the consumer to login. Safety crew explicitly controlled and get right of entry to can be granted and revoked at will. That's why if the device is said stolen, the relaxed login can be disabled and the sandboxed area of the tool is safe.

- **Secure browsers**

Secure browsers are the third tool. On mobile gadgets a secure browser can be set up to update the default browser. Every time a website is asked a secure browser can test in opposition to a blacklist of recognized malicious websites. Towards social engineering and malware set up this will be a defense. That is simplest as powerful as the blacklist in use. Vendors consisting of Symantec, McAfee, trend Micro, F-secure, Lookout and Webfoot, provide comfy browsers plus blacklists for diverse phone platforms.

CHAPTER 4

RESEARCH METHODOLOGY

4.1 Various Mobile Devices

Now a day we can't imagine a day without mobile. It was not that long when stationary hardware is ruled in the industry. A mobile device is an electronic device which is portable in hand. We have many types of mobile devices like:

- Smartphones
- Tablets
- Laptop computers
- Smart watches
- E-readers
- Handheld gaming consoles

Smartphones are the most popular device now a day. Easily portable and fit in pocket. Through this they can be connected all the time with the help of a wireless network. This device has many options. Anyone can choose as their needs.

Tablets are same as smartphone's with better display and large battery.

Laptop computer are also popular device. It can give same functionality as desktop computer. They also have keyboard option. Same input output port also have.

Smart watches are new. We can use it to check notification. We can take and receive phone calls.

E-readers have for many years. It has similarity with tablet. But its primary purpose is to read. People who enjoy to reading they choose this digital format of reading.

Handheld gaming consoles are popular for gaming. Now a days gaming is most popular for entertainment.

4.2 Mobile application

Mobile application is also called an app. It's a software design to run on mobile device. It provides services same as pc. Apps are may be small and limited functions also have. Mobile application also may know as an app, web app or mobile app. Mobile applications are game, calculator etc. in mobile devices multitasking are not available because hardware resources are limited.

Apps are divided into two broad categories. Those are native apps and web apps. Native apps are built for specific mobile like android etc. native app gives better performance. In HTML or CSS web apps are used. it requires minimum device memory. Web apps need a better connection. Several types of apps are here. Like

Gaming apps: its an equivalent of video games. Now a days many games are available.

Productive apps: this apps are use for business purposes like sending email and tracking work progress etc.

Life style and entertainment apps: its popularity are increasing day by day.those are social media, facebook etc.

Other app types are mobile commerce .that are use to purchase, travel etc.

4.3 MOBILE PLATFORMS

Through mobile platform everyone can engage with lots of content. A mobile device has lot of functions like messaging services, social media and various apps [3]. Customers love that content. The Android platform uses a modified Linux kernel. Maximum applications are written within the Java programming language.

4.4 MOBILE APP ARCHITECTURE DESIGN

3-layer architecture is famous multilayer architecture. This three-layer architecture is important for creating mobile app architecture. Three essential layers of mobile architecture design is given below:

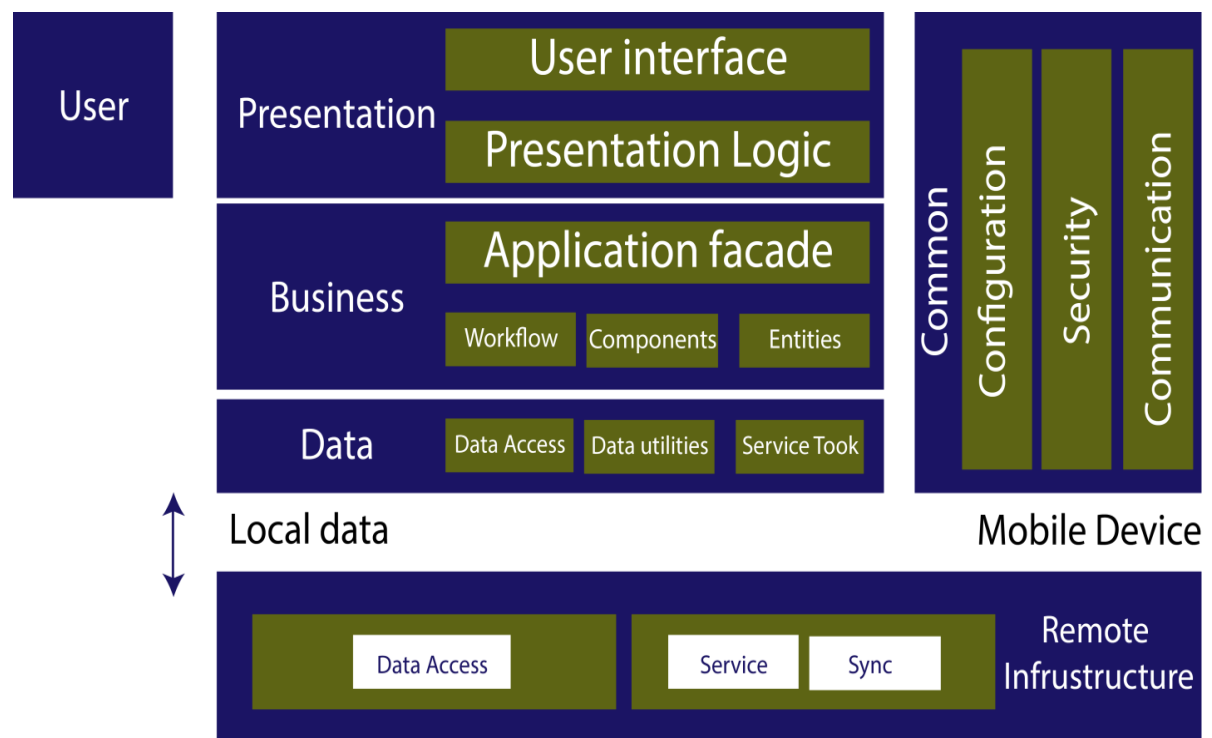


Figure 4.2: Mobile application architecture design.

- **Presentation Layer**

The presentation layer consists of additives. These layer consist the user Interface and UI system. Here the primary cognizance is the mobile application’s presentation of end users. The cellular application builders need to know the customer type. In the presentation layer level, you need to determine on many crucial matters. Themes, fonts, shades and shadings are one of them. The developers keep on mind the customer’s deployment limit and mobile app architecture designs. Choose the perfect information format is the difficult part of this layer.

- **Business Layer**

The business layer is factors for business front. This layer determines how the application will present the business to the end-users. Enterprise additives, workflow, and entities are included there. Those layers' are very much complex than others. It handles too many problems like caching and logging. The exception control and safety challenges are also uploaded. To reduce the complexity they have some layer. Service layer and domain model are including those. Commonplace application feature units are the service layer.

- **Data Access Layer**

The application wishes meet through data access layer. They provide efficient and secure facts transactions. For this motive, this layer designs a developer. It combines exclusive elements consisting of information utilities, information access additives, and service marketers. The choice of the proper facts layout is crucial. Additionally, having a sturdy validation method is any other issue that makes it crucial to layout this layer. Maintenance of the records must not forget through cellular application builders.

4.5 MOBILE APPLICATION COMPONENT

Four different types of app components are here

- **Activities**

An activity will be the entry point. User interface provide a single screen [17]. As an instance, an email application has one activity a list of latest emails that suggest, every other activity to compose an electronic mail, and for reading emails. Among system and application an activity helps the subsequent key interactions:

- ✓ Ensure that the system running continuously the hosting activity technique.
- ✓ The user can go back to activities with their previous state restored helping the application take care of having its technique killed.
- ✓ Coordinating user flows provide a way for apps.

- **Services**

Keep running an app inside the background a service is general point. It runs within the background to perform lengthy-running operations. A service now not provides a user interface. When customer busy with an app music plays in the background. When playing music in background some varieties are happened that handles by:

- ✓ Music playback is directly aware of. A notification tells the user to foreground it [17].
- ✓ An everyday background service isn't so much important to immediately conscious as running; to dealing with the system has greater freedom in dealing with its system. It permitted to be killed if it wishes RAM.

- **Content providers**

A content material provider manages a shared set of application data in the file system that can save, In a SQLite database, your application can get entry to at the internet, or on any other chronic storage region. To the system, for publishing named data items a content company is an entry point into an application. This permits the device to do in dealing with an app there are a few specific things:

- ✓ Does not require that the application remain strolling assigning a URI, so after their owning apps have exited URIs can persist. Apps record must be retrieved from corresponding URL [17].
- ✓ It provides a good security model.

4.6 MOBILE SECURITY TYPES

Organizations have become increasingly reliant on mobile security vendors to protect devices. There are four different types of mobile security models used by vendors.

- i. Traditional signature file antivirus approach
- ii. Hybrid-AI cloud security
- iii. Intermediary cloud approach
- iv. Mobile behavioral analysis

i. Traditional signature files antivirus approach

For comparing all apps and files the conventional signature document antivirus version creates a signature report at the. This doesn't work very well for cellular devices. For mobile devices this doesn't work very well, however. Today, many organizations service the hybrid-AI approach [18].

ii. Hybrid-AI cloud security

Device studies the documents users download and set up on their gadgets. It's similar to search engines like Google wherein the community contributes samples that enhance the general experience. Inside the cloud analyzing these files and applications helps security tools perceive the caution signs of malicious rationale. It prevents customers from downloading and starting them As soon as AI identifies any malicious files. About the protection of documents the tools enforce those guidelines via a neighborhood app that updates with the latest information. This cloud-based evaluation approach works very well for mobile devices. However, at finding zero-day assaults this sort of cell safety approach isn't always great due to the time lag inherent with collecting facts, testing and returning intelligence to the on-device agent. Protection versions the subsequent form uses the cloud and essentially acts as an intermediary carrier.

iii. Intermediary cloud approach

In this model, if they may be malware or protection threats any documents a user gets or downloads to the device are automatically uploaded to the cloud service for trying out and assessment to determine. If these documents are accredited then the documents are loaded to the device only. For mobile devices this intermediary approach also works well. However if the mobile devices are on a gradual network it can sometimes cause a lag in performance. Fortunately, fast 4G, 5G and LTEs general availability makes this less of an issue.

For mobile safety vendors, this method means methods on high-powered cloud servers, removing the regulations of on-device resources. They could run very fast and significant

iv. Mobile behavioral analysis

With this technique, by way of flagging suspicious conduct an AI-based totally preloaded app prevents malicious interest. To this technique there may be nonetheless a cloud-based factor. To flag on the device agent every now and then downloads new suspicious behaviors. However, locally most of the work is accomplished. Locate zero-day exploits mobile behavioral evaluation is the nice way. To gain and check documents this method uses crowd sourcing,

4.5 THREATS TO MOBILE DEVICES

Mobile safety threats are attacks which are supposed to compromise or steal data from mobile gadgets like smart phones and tablets. those threats regularly take the shape of malware or spyware, giving awful actors unauthorized get entry to to a device; in lots of instances, customers aren't even conscious that an attack has took place

- **Data Leakage**

Unintentional data leakages cause are often mobile application. For example, for mobile users who grant them broad permissions “risk ware” apps pose a real problem [19]. Those are free apps. Those cellular malware packages use distribution code. To keep away from those problems, best give apps the permissions for correctly function. The September 2019 updates for to make users more aware about it Android and Apple iOS both introduced protocols.

- **Unsecured Wi-Fi**

Free Wi-Fi is too much risky. It must be unsecure. According to V3, in fact, 3 technology specialists who promise free Wi-Fi are safe they also hacked. Their data are also stolen. So don't use free Wi-Fi it must be stolen our data

- **Network Spoofing**

Hacker sets a fake access point connection. It acts like a wi-fi networks that is called network spoofing. It's just a trap. They use just a common location like coffeshop. They use common name for this. Sometime its need to create account with password. Please stay safe from this network spoofing.

- **Phishing Attacks**

Most of the time phishing attacks happened on mobile phone because mobile gadgets are constantly powered-on. Cellular tool apps show less information to deal with the smaller screen sizes that's why it's most susceptible.

- **Spyware**

Malware sending data streams back to cybercriminals that's why many cell users are worried about it, there's a key threat closer to home: spyware. They keep track their purpose and activity. For the have some co employer. To detection this need a special technique. And keep away from this.

- **Broken Cryptography**

In line with InfoSec Institute training materials, whilst app builders use weak encryption algorithms to force strong encryption cryptography can happen. As an end result, to crack passwords and advantage get entry to any attacker can take advantage of the vulnerabilities. Within the second example, builders use highly secures algorithms. They add flaws in code. Hacker doesn't crack this password. That need modify high-level application. Before apps are deployed the onus implements encryption requirements on developers and organizations.

- **Improper Session Handling**

Many apps make use of “tokens to facilitate ease-of-access for cellular device transactions. Without being forced to re-authenticate their identity they permit customers to carry out multiple movements. Like passwords for customers. Generated by means of apps to discover and validate devices tokens. With each access attempt, or “session secure apps generate new tokens. It must be need to remain confidential. In case from your tablet you logged into a corporation intranet website online and omitted to sign off while you completed the task. If it keeps open then a cyber criminal can attack it. Also explore different connected elements of your employer’s community.

4.7 Mobile security threats

Now a days mobiles are top priority for organization. Beacouse research shows that it can improve operations and productivity. For this popularity mobile device are increasing day by day. For this security issues are also creating. 4 types of security threats are given below:

Mobile application security threats: application based security threats are happen when people downloads an app that looks real but it’s a scam. Examples are spyware and malware. It can steal information

Web-Based Mobile Security Threats: People visit a website which is affected. But it looks fine and autometicaly download malicious content

Mobile Network Security Threats: It’s very common and dangerous. When people use public wifi hackers can steal unencrypted data

Mobile Device Security Threats: Physical threats are very dangerous. When thief steal your device where private data are stored. Theft can easily get your private information. Hackers have direct access to it.

Common example of those threats are given below.

Social engineering: social engineering attacks happen when fake emails are sent. And your employee clicks on it then your organization's information may be at risk.

To avoid this your employees need to know about this and be very much careful for this.

How The Bad Guys Attack



2. Data Leakage via Malicious Apps

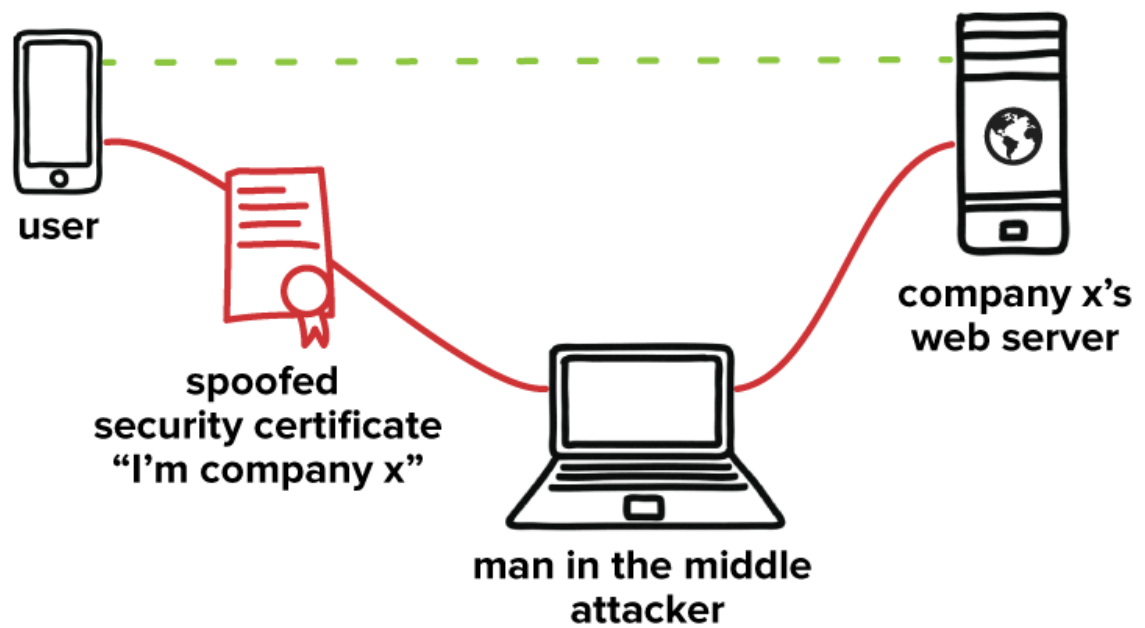
Today 85% apps are unsecured. Hackers can easily find an unsecured app. And very easily collect information's. For example suppose your employee goes an app store and install an app. And this app request to access any folder and your employee gives permission on it without fully knowing about it. Then your organization may in danger. They can steal any information.

To secure from this it admin needs to manage corporate data without disrupting employee's information.

3. Unsecured Public WiFi

Public wifi are generally unsecured. Because its really hard to know who set this up. Its secure or not no one really knows that. In this situation if you give your employee an

immediate task .and he or she doing it through public wifi then your information can be steal. Your organization may be loss. Some times it looks like an wifi network but it's a scam to stall your information. To secure this employee needs to use vpn.



4. End-to-End Encryption Gaps

If you encrypt your data but it's a hole then your information may at risk. You must be sure about this that your data are fully encricted.

Fig. 1a: Encryption in transit

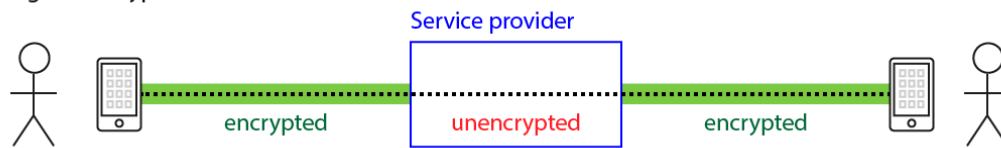


Fig. 1b: End-to-end encryption

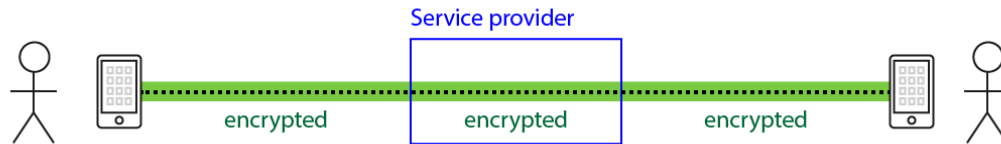


Fig. 1c: End-to-end encryption (no service provider)



4.8 MISUSES AND CYBER ATTACK ON MOBILE DEVICES

Misuses of mobile phones are Corruption, Terrorism, and Misusing of facebook, Misuse in the examination, Data hacking, Chatting and wastage of time.

Recently, check point (renowned security firm) published its mobile safety report 2021.

The record said that 40% of all mobile devices are vulnerable to cyber-attacks [13].

Furthermore, it changed into introduced up that approximately 97% of businesses global dealt with mobile threats that utilized several attack vectors. No longer to forget about that as a minimum one worker in 46% of the corporations reportedly downloaded a malicious application on their phone. With the upward thrust of COVID-19 and the enlargement of the work-from-domestic lifestyle, the attacks on human being's private devices were increasing considerably. The identical document also said that nearly every employer witnessed as a minimum one phone malware attack remaining year. 93% of the stated attacks stemmed from the mobile's network. It changed into noted above that approximately 40% of all mobile devices are at the risk of becoming a target of cyber-attacks. If the above-mentioned findings didn't sound alarming enough, it turned into additionally stated that a 15% surge in banking Trojan activity turned into witnessed last year. These activities made it easier for the attackers to steal touchy facts

consisting of person users' banking credentials. It's been predicted that over the following 3 years, about 6 out of 10 employees may be operating from domestic. So, expect cybercriminals to take full advantage of this reality. Also, check factor located out that malicious actors have come up with a new assault in which they take advantage of a main organization's mobile device management (MDM) machine to unfold malware to over 3 out of 4 gadgets it manages.

4.9 VULNERABILITIES OF MOBILE DEVICES SOFTWARE AND HARDWARE

There are four vulnerabilities of mobile devices software and hardware. They are

- **App vulnerabilities**

Mobile apps data transmission security is progressed. Program improvement cooperation provides some security apps. But vulnerabilities come from short software development life cycle. Organization employees download those apps. We can say that many apps are not reviewed. Most of them have vulnerabilities. It management can't manage it.

- **Device vulnerabilities**

Google and Apple both frequently post security announcements. Organization can measure danger by "vulnerability window".

Longer vulnerability windows have on android devices than iOS. Android's most critical protection problem is many producers and providers. For example, in modern running system Oreo have only 0.2 percent of Android customers are presently, according to Google.

- **Networks vulnerabilities**

Mobile network vulnerabilities may happen on software and hardware [14]. Heart bleed, FREAK, and POODLE are example. Heart bleed turned into an SSL vulnerability from the lively memory of affected systems. Browser handles network traffic encryption from smaller. More vulnerable version is the POODLE. That forced the browser.

At the same time as to detection/safety solution almost every endpoint safety suite on the grounds that windows XP have protected a firewall and host-based intrusion. Don't have the identical degree of safety on mobile devices.

- **Web and content vulnerabilities**

To gain unauthorized access they use web content like videos, photos etc [14]. Example of that is Stage fright, inside the Android media processing element software program vulnerability. Through pressing this content they get entry to the android device. Much large story of mobile chance vulnerabilities are just one factor. Enterprise data can effected by mobile device configuration.

4.10 MOBILE VIRUSES

Some mobile virus name is adware, ransom ware, spyware, Trojan horses, and worms. Behind legitimate applications, faux emails, or inflamed attachments viruses may be hidden. For avoiding detection hackers continuously fine tune their craft.



Figure 4.8: The anatomy of viruses

- **Adware**

Influx is signal of adware. It's not tolerable while some pop-u.s. is a predicted part of advertising and marketing promotions. It could track activities of you device. For theft your data it will root you device.

- **Ransom ware**

It's found on desktop first. Ransom ware encrypts users personal data. So that user can't access to it. Then they demanded a ransom for this [15].

- **Spyware**

Spyware is attached in some applications. Its then track your activity. You also don't know that you installed a risky app.

- **Trojan horse**

As a text message a computer virus in your mobile phone will typically seem. They send premium messages and increase your phone bill.

- **Worm**

Any other virus unfolds by means of texts. To wreak havoc A bug doesn't need consumer interaction. It unfold many devices as it can. These way hackers can load malware. And they take your data.

4.11 MOBILE DATA THEFT

If you download some apps on your mobile your mobile already is in danger. Maximum people are very casual with his smart phones that carry a lot of digital identity. Within half an hour identification thieves may alternate the password to all my email and social networking offerings.

There is a 4 way you can prevent data theft.

- **Set up a lock screen**

Use a screen lock Step one to blocking off access to the data. On few phones have lock screen & password. Here you can select any of these options from pattern, PIN, Password and Fingerprint. I recommend both password and fingerprint to unlock. It will be too much tougher to crack. As soon as you have activated your tool's display lock it will be harder for whom who is trying to access your phone without permission.

- **Encrypt your device data**

We can use encrypt feature for secure our devices. In settings this features have in security. But sometimes it is in privacy. Your information will be protected if you use encryption. If your phone stolen then your information still will be secure for using pin. Encrypt your data when your phone fully charged. Otherwise it will interrupt and lose your data

- **Set up Android Device Manager**

Activate your Android device manager. This feature is in settings security. It can also be found settings privacy. When you activate Android tool manager then you have to ensure that it's running well [20].

If it's not found net dashboard will show your location. Its ringing option also can on remotely. You can lock your screen and delete files or anything remotely.

- **Set up remote access**

If the thief change your sim card and also give new setting manager than is an app called Cerberus anti theft [20]. From the lock screen this paid application prevents everybody from powering down your phone. Even after a SIM card exchange that send SMS indicators. You can activate your phone's cameras through internet dashboard or with an SMS command. Then you can snap the culprit. On your Google drive and Dropbox account remotely the application also can be configured to lower back up data.

CHAPTER 5

RESULT AND PREDICTION

5.1 COMPARATIVE ANALYSIS

Uses approach for digital signature and cryptography for secure authentication and data security. Provides multiple security levels to cloud services and supports switching among them for enhanced security. Provision for distributed, one time access key sharing mechanism (multi key division based authentication and access control with distributed access key distribution). Option for service barring in unauthorized attempts. Choice based security provisions for sensitive and non - sensitive data. Protection for critical and highly confidential or sensitive data. Securing confidential data from database hijacking attacks (making data of no use to hijacker using honey pots), faking identity of data for basic guessing attacks. Prevention man in middle attack using distributed key distribution model, prevention of malicious insider attack (helps to maintain Security of data maintained over a cloud with third party).

5.2 DISCUSSION

Figure 5.2.1: Comparison of different software

Antivirus	Price per year	Minimum android support	Ads	Maximum user size
Avast mobile security	Free\$12\$ 24	5.0 lollipop	Free version	Free version 10
Bit defender Mobile Security	\$15	5.0 lollipop	No	10
Google Play Protect	Free	4.4Kit Kat	No	Free version
Kaspersky Mobile Antivirus	Free\$15	5.0 lollipop	No	Free version 5
Lookout Security & Antivirus	Free\$30 \$100	5.0 Lollipop5	No	Free version 5
McAfee Mobile Security	Free\$30\$ 80	7.0 Nougat	Free version	Free version Depends on subscription

Norton Mobile Security for Android	\$30	6.0 Marshmallow	No	3,5,or 10
AVG antivirus	Free \$19-\$39	6.0 Marshmallow	Free version	10

Figure 5.2.2: Security Level

Tool Name	Category of Software	Anti-Theft	Security Level
Avast mobile security	Antivirus	Partly premium	Free: Low Paid: High
Bit defender Mobile Security	Antivirus	Yes	High
Google Play Protect	Antivirus	Yes	Low
Kaspersky Mobile Antivirus	Antivirus	Yes	Free: Low Paid: High
Lookout Security & Antivirus	Antivirus	Partly premium	Free: Low Paid: High
McAfee Mobile Security	Antivirus	Discontinued	Free: Low Paid: High
Norton Mobile Security for Android	Antivirus	No	High
AVG Antivirus	Antivirus	Yes	Free: Low Paid: High
Comodo Firewall	Firewall	Yes	Free: Comparatively Low Paid: High
Tinywall	Firewall	No	Free

5.3 Screenshots of Mobile Security Software

Avast Security Antivirus

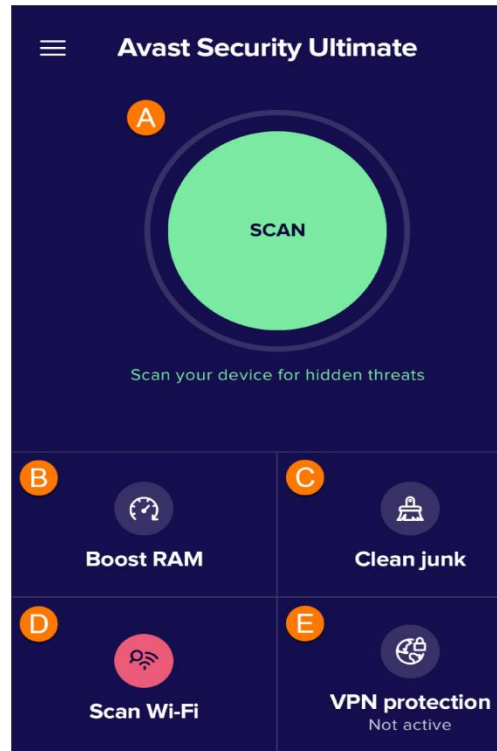


Figure 5.3.1: Avast security antivirus.

AVG Antivirus

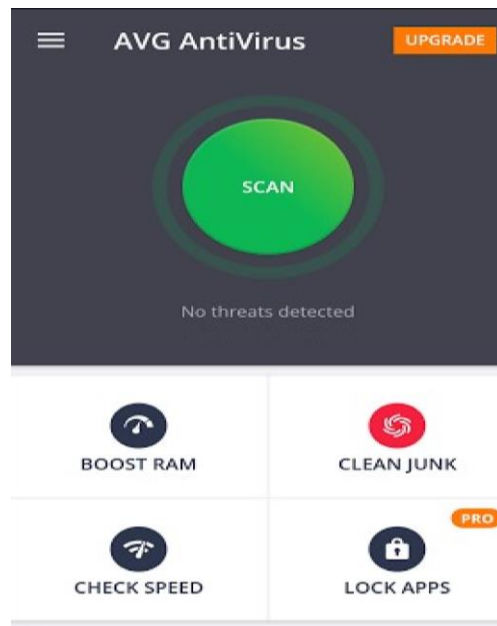


Figure 5.3.2: AVG security antivirus

Kaspersky Antivirus

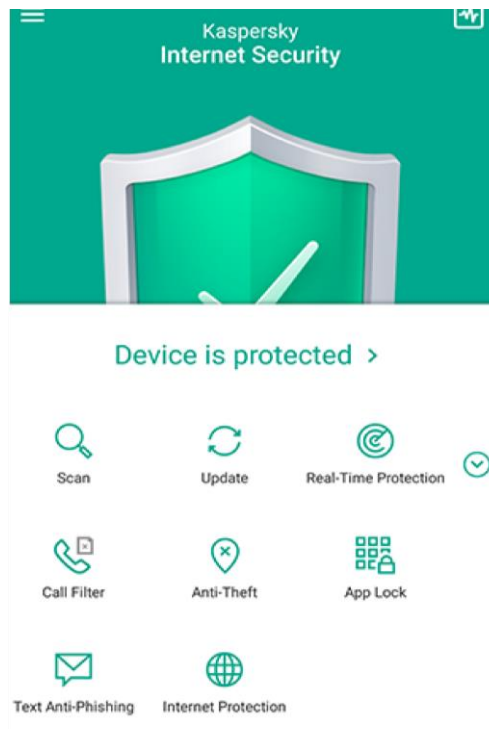


Figure 5.3.3: Kaspersky antivirus.

Comodo Firewall

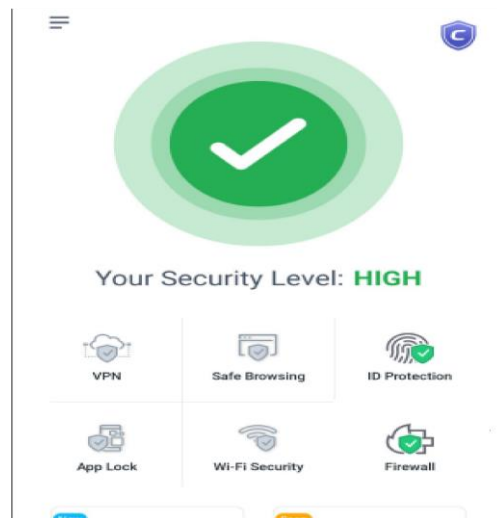


Figure 5.3.4: comodo firewall.

CHAPTER 6

FUTURE WORK & CONCLUSION

6.1 FUTURE WORK

Security tools don't give complete protection. They have to try to give complete protection. Free version gives just a basic protection. Its need some more strength. So that people who are unable to buy they can use it. Day by day new technologies are created. They have to ready for new attack. Side by side I have to be responsible for mobile security. I have to be conscious about what type of website I visiting. I must need to ignore to click on ads. Because most of the attack is happened through ads. So that I can prevent many attack.

6.2 CONCLUSION

Here I can see the security level of mobile devices. Every tool is giving security with lots of features. They can protect you from viruses and unauthorized access. Your data can be safe with those tools. Some are given low performance and some are high. Most of the free versions are given low performance. Every tool has some laciness high cost is one of them, some tools feature don't work well. Some tools have few features. Very few free antiviruses are given well performance. Your system can be slow down for this. They can't give you complete protection especially in free antivirus. Moreover they have limited detection techniques. Their ads are also annoying.

So I can say that paid version is good enough against free version. But most of their cost is high.

References

- [1] Y Wang and Y Alshboul, ‘‘Mobile Security Testing Approaches and Challenges’’, 2015
- [2] Wikipedia, ‘‘security’’,2012
- [3] Kitaboo, what is a mobile based platform? 2018
- [4] AJ Nicholson and MD Corner, Mobile Device Security Using Transient Authentication,2006
- [5] W Jansen and V Korolev, A Location-Based Mechanism for Mobile Device Security,2009
- [6] Y Wang, K Vangury, and J Nikolai, ‘‘Mobile Guardian: A security policy enforcement framework for mobile devices’’,2014
- [7] S Alotaibi, S Furnell and Clarke, Transparent Authentication Systems for Mobile Device Security: A Review, 2015
- [8] A Arabo, and B Pranggono, Mobile Malware and Smart Device Security: Trends, Challenges and Solutions, 2013
- [9] Security Analysis of Mobile Device-to-Device Network Applications, 2018
- [10] Improving Mobile Device Security with Operating System-Level Virtualization, 2013
- [11] Os system, ‘‘ Mobile App Architecture Design’’ , 2020
- [12] MA Harris, KP Patten, ‘‘Mobile device security considerations for small and medium-sized enterprise business mobility’’, 2014
- [13] Digital information world, ‘‘40% of mobile devices are prone to cyber attack of mobile devices’’, 2021
- [14] Lookout, ‘‘Mobile vulnerabilities: what they are and how they impact the enterprise’’, 2017
- [15] Panda, ‘‘how to know if your phone has a virus + how to remove it, 2021
- [16] M Becher and FC Freiling, Towards Dynamic Malware Analysis to Increase Mobile Device Security, 2008
- [17] Developers, ‘‘Application Fundamentals’’,2021
- [18] Techtargat, ‘‘4 types of mobile security models and how they work’’,2020
- [19] Kaspersky, ‘‘Top 7 mobile security threats in 2020’’, 2020
- [20] The times of india,‘‘4 tips to prevent data theft and android phones’’,
- [21] The state of security, ‘‘How to secure your mobile device in six steps’’,2016
- [22] Computerweekly, ‘‘Mobile security tools’’,2012

PLAGIARISM REPORT

Report_Update_-Mahtabur_Rahman_Sobuj__211-25-015.pdf

ORIGINALITY REPORT

23% SIMILARITY INDEX	15% INTERNET SOURCES	5% PUBLICATIONS	19% STUDENT PAPERS
--------------------------------	--------------------------------	---------------------------	------------------------------

PRIMARY SOURCES

1	dspace.daffodilvarsity.edu.bd:8080 Internet Source	6%
2	Submitted to Daffodil International University Student Paper	3%
3	www.ripublication.com Internet Source	2%
4	Submitted to Rosebank College Student Paper	1%
5	Submitted to American Public University System Student Paper	1%
6	Submitted to Ghana Technology University College Student Paper	1%
7	www.coursehero.com Internet Source	1%
8	Submitted to Georgetown University Student Paper	1%
9	ieeexplore.ieee.org	

	Internet Source	1 %
10	Submitted to Harare Institute of Technology Student Paper	1 %
11	www.kaspersky.com Internet Source	1 %
12	www.emeraldinsight.com Internet Source	1 %
13	Fadi Al-Turjman, Ramiz Salama. "Cyber security in mobile social networks", Elsevier BV, 2021 Publication	1 %
14	Wayne Jansen. "A Location-Based Mechanism for Mobile Device Security", 2009 WRI World Congress on Computer Science and Information Engineering, 03/2009 Publication	<1 %
15	mafiadoc.com Internet Source	<1 %
16	Submitted to Varsity College Student Paper	<1 %
17	Submitted to University of Huddersfield Student Paper	<1 %
18	Submitted to Study Group Australia Student Paper	<1 %

19	Submitted to Laureate Higher Education Group Student Paper	<1 %
20	Surabhi S. Pohandulkar, Chhaya S. Khandelwal. "Blood Bank App using Raspberry PI", 2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS), 2018 Publication	<1 %
21	Submitted to Engineers Australia Student Paper	<1 %
22	Submitted to Imperial College of Science, Technology and Medicine Student Paper	<1 %
23	Huaming Wu. "Multi-Objective Decision-Making for Mobile Cloud Offloading: A Survey", IEEE Access, 2018 Publication	<1 %
24	artandpopularculture.com Internet Source	<1 %

Exclude quotes On
Exclude bibliography On

Exclude matches < 10 words