Scorpion shield

Atharv Kadam[1], Himanshu Dhande[2], Divya Karwande[3], Akshata Raut[4]
[1, 2, 3, 4] Dept of Computer Engineering
[1, 2, 3, 4] VIVA Institute of Technology, Virar

Abstract- *People use computers for all kinds of activities: online gaming, shopping, entertainment, emails, facebook, study, research, etc. At the same time, the risk of infection by malicious programs in these computers is rising. The main issue is that general users don't understand what a virus is and how computers get infected. On the other hand, many vendors produce antivirus software with different features to prevent or remove these viruses from people's computers. General users don't understand the concept of each feature in these programs, nor is there a tool to advise users about what the features mean and help them select the right software for personal or business needs. The topic "Antivirus Software " deals with software which is used to prevent or detect malware. Antivirus software is used to prevent, detect and remove all sorts of malware such as computer viruses, hijackers, worms, Trojan horses, etc. The App will begin by checking your os programs and comparing them to known types of malware. It will also scan your mobile operating system as well as installed applications for behaviors that may signal the presence of a new and unknown malware..*

Keywords- Cloud Computing, Reviews, Fraud, Genuine, Sentiment Analysis, Digital Signatures, Security, Antivirus

I. INTRODUCTION

Antivirus is a kind of software used to prevent, scan, detect and delete viruses from a computer [1]. Once installed, most antivirus software runs automatically in the background to provide real-time protection against virus attacks. Comprehensive virus protection programs help protect your files and hardware from malware such as worms, Trojan horses and spyware, and may also offer additional protection such as customizable firewalls and website blocking. Antivirus programs and computer protection software are designed to evaluate data such as webpages, files, software and applications to help find and eradicate malware as quickly as possible.

Most provide real-time protection, which can protect your devices from incoming threats; scan your entire computer regularly for known threats and provide automatic updates; and identify, block and delete malicious codes and software [2]. Because so many activities are now conducted online and new threats emerge continuously, it’s more important than ever to install a protective antivirus program. Fortunately, there are a number of excellent products on the market today to choose from. Antivirus software begins operating by checking your computer programs and files against a database of known types of malware [9]. Since new viruses are constantly created and distributed by hackers, it will also scan computers for the possibility of new or unknown types of malware threats. With so many internet-connected devices in the home today, technology has made everyday living more convenient but also riskier [8]. To help protect your devices, Verizon offers TechSure, which includes a combination of anti-virus software, 24/7 tech support for Verizon services and hardware; identity theft protection, password management; and repair insurance for damaged and broken devices [7]. Antivirus software is a type of program designed and developed to protect computers from malware like viruses, computer worms, spyware, botnets, rootkits, key loggers and such [6]. Antivirus programs function to scan, detect and remove viruses from your computer. There are many versions and types of anti-virus programs that are on the market. However, the prime objective of any antivirus program is to protect computers and remove viruses once detected [2].

Most antivirus programs incorporate both automated and manual filtering abilities. The instant scanning option may check files - downloaded from the Internet, discs that are embedded into the PC, and files that are made by software installers. The programmed scanning process may likewise check the entire hard drive on a day-to-day basis [12]. The manual scanning system enables you to check single documents or even to scan the complete network at whatever point you feel it is necessary. Since new infections are always being made by PC programmers, antivirus programs must keep an updated database of the most recent malware codes [10]. This database incorporates a list of "malware definitions" that the antivirus software implements when filtering records. Since new infections evolve every day , it is essential to keep your product's infection database up and coming. Luckily, most antivirus programs naturally refresh the infection database all the time [14].

While antivirus software is basically intended to ensure complete protection for PCs against virus infections, numerous antivirus programs now secure against different sorts of malware for example, spyware, adware, and rootkits as well [12]. Antivirus software may likewise include firewall features, which anticipate unapproved access to your PC [5]. Utilities that incorporate both antivirus and firewall abilities are commonly called "Internet Security Suite" [9].

While antivirus programs are accessible for Windows, Macintosh, and Unix platforms, most antivirus software is compatible with Windows operating systems [8]. This is on account of the fact that most infections are focused towards Windows PCs and subsequently virus protection is particularly imperative for Windows clients [4]. If you are a Windows user, it is important to install a third party , feature-packed, robust antivirus program on your PC [6]. Comodo Antivirus has been the best and compelling solution to outsmart even the zero-day and unknown threats with efficient features and technologies like default-deny protection, Host Intrusion Prevention, Auto sandboxing solutions and Containment technology [5].

Typically, most programs will use three different detection devices: specific detection, which identifies known malware; generic detection, which looks for known parts or types of malware or patterns that are related by a common codebase; and heuristic detection, which scans for unknown viruses by identifying known suspicious file structures [8]. When the program finds a file that contains a virus, it will usually quarantine it and/or mark it for deletion, making it inaccessible and removing the risk to your device [9]. Antivirus software is designed to prevent computer infections by detecting malicious software, commonly called malware, on our computer and, when appropriate, removing the malware and disinfecting the computer. Malware can be classified into various kinds, namely, Trojans, viruses (infectors), rootkits, droppers, worms, and so on. Antivirus software is special security software that aims to give better protection than that offered by the underlying operating system (such as Windows or Mac OS X) [5]. In most cases, it is used as a preventive solution.

However, when that fails, the AV software is used to disinfect the infected programs or to completely clean malicious software from the operating system [4]. AV software uses various techniques to identify malicious software, which often self-protects and hides deep in an operating system. Advanced malware may use undocumented operating system functionality and obscure techniques in order to persist and avoid being detected [12]. Because of the large attack surface these days, AV software is designed to deal with all kinds of malicious payloads coming from both trusted and untrusted sources [6].

II. LITERATURESURVEY

The following chapter is a literature survey of the previous research papers and research whichgivesdetailedinformationaboutthepreviussystemalongwithitsadvantagesanddisadvantagesto make the system.

Y.Z.Liet.al[1],malwares are being produce data an unprecedented scale with hundreds of new entities targeting users across all of technology as malware developers explore new ways or exploit old ones to evade detection and defeat analysis. The process of obfuscation was originally used to protect benign applications from code alterations, manipulations and reverse engineering, but this mechanic is also a tool malware developers could manipulate to mask the malicious applications they create.

B. Fechner et.al [2], in the cloud environment there are many unique and different on demand services available for users. Those services allocate workable and easy accessibility to use various web applications. In this environment malicious attacks and threats can occur anytime and can destroy useful files and applications. So the cloud needs to be well secure and highly maintained. In this paper we will discuss various malicious attacks which can dismantle ourcloud environment and how we can make our cloud more powerful by using strong and robust cloud antivirus.

X. Zha and S. Sahni et.al [3], Banking Malware, has become a popular and ever more prevalent mechanism to monetize malware development. Since the development of the Zeus malware kit in 2007, the frequency and complexity of banking malware has been in- creasing. Developing a good understanding of the operation of a malware family is a first step in the reverse engineering required to create tools to extract the malware configuration, which is used in the remediation of malware infrastructure. This reverse engineering process in recent years has become increasingly challenging. This manuscript provides a brief summary of the reverse engineering of banking malware families over a two year period and emphasizes the anti- analysis techniques employed by the authors of six families of banking malware. The manuscript presents this analysis, and examines trends in the development of these anti- analysis techniques.

K. Nakano et.al [4], In the last several decades, the arms race between malware writers and antivirus programmers has become more and more severe. The simplest way for a computer user to secure his computer is to install antivirus software on his computer. As antivirus software becomes more sophisticated and powerful, evading the detection of antivirus software becomes an important part of malware. As a result, malware writers have developed various approaches to increase the survivability and concealment of their malware. One of these technologies is to terminate antivirus software right after the execution of the malware.

D. Man, K. Nakano, and Y. Ito el.al [5], malware Analysis is the top trend in the security industry. The number of new malware samples and toolkits for automated malware generation are growing exponentially, whereas the analysis capacity and knowledge are going down. In this paper we are going to discuss the infrastructure we created for malware analysis, with network dissection of traffic, execution of samples on multiple virtual machines or in real ones if required. The architecture performs fast analysis, comparing the results of multiple different anti-viruses and uses customized kernel-drivers, loaders and a clustered environment. New machines can be easily added to increase performance. Dispatchers, memory dumpers and dissectors are going to be discussed, as well as results we got in our live lab.

A. K. Sahoo, K. S. Sahoo, and M. Tiwary el.al [6], Antivirus is most widely used to detect and stop malware and other unwanted files. Cloud antivirus is a malware detector architecture where virus definitions and other behaviors of suspicious files are analyzed on cloud and controlled by a lightweight Agent on the client system. We suggest using a two-way caching scheme where local-cache is stored on the client system and cloud-cache is present on network cloud, where we store virus definitions and behaviors according to collective intelligence techniques. Local- cache is used to detect the virus and other malware files while offline and cloud cache uses the Artificial Intelligence Techniques for the whole client base to get the most susceptible and prone virus and malware definitions thus increasing the optimality of virus definition search and hence the speed of the whole process gets increased.

M. Vincent el.al [7], Hackers use malware to gain access to target computers. Malicious payloads are usually generated using tools such as Metasploit. As a means of defense, the target computers deploy anti-virus solutions to detect these malicious payloads and protect the victim machines. In a reaction to this, the hackers created anti-virus evasion tools to evade detection by these antivirus solutions. But how effective are these antivirus evasion tools? This paper seeks to evaluate the effectiveness of some selected antivirus evasion tools: Avet, Veil 3.0, The Fat Rat, PeCloak.py, Phantom-Evasion, Shellter, Unicorn and Hercules against current best Antivirus Solutions on Windows and Android platforms.

B. Rajesh et.al [8], countering the proliferation of malware has been for recent years one of the top priorities for governments, businesses, critical infrastructure, and end users. Despite the apparent evolution of anti-virus (AV) systems, malicious authors have managed to create a sense of insecurity amongst computer users. Security controls do not appear to be sufficiently strong to stop malware proliferating. There seems to be a disconnect between public reports on AV tests and what people are experiencing on a daily basis. In this research, we are testing the efficiency of AV products and their ability to detect malicious files commonly known as malware.

A. P. Namanya et.al [9], there are different types of embedded portable iDevices which can be used in criminal activities. The most commonly used gadget in the field of embedded portable iDevices is the iPad. Techniques used to acquire data from iPad include jail breaking, using inbuilt operating system utilities and using forensic tools (open source, freeware or commercial). Data integrity is a vital element of digital forensics which must be ensured for acceptability of findings (retrieved forensic artifacts) in a court of law. In order to establish data integrity in iDevices forensics, investigations were performed using different techniques, specifically an operating system inbuilt utility, a freeware tool and a commercial tool. The forensic artifacts acquired from these tools and techniques were then compared to ascertain their data integrity. The results have shown that on one hand the freeware tools, under certain circumstances, also preserve data integrity as their commercial counterparts but on the other hand the commercial tools, under certain circumstances, also make data integrity doubtful as generally believed for freeware tools. Based on the results, the research has also recommended various data acquisition tools that the forensic examiner can select depending on the requirement.

M. Zakeri et.al [10], In this paper are given mean and types of audit, probabilities of transitions between the functioning states of information of protection tools with discrete work time. Also, in this work are given four types of antivirus errors with possible situations in the performance of means of discrete work time. Performance cases of antivirus software are described in the form of directed Graph. By four types of antivirus errors is calculated average time of operation without breaking, intensity of appearing of error, average time of backup and intensity of backup of error.

III. METHODOLOGY

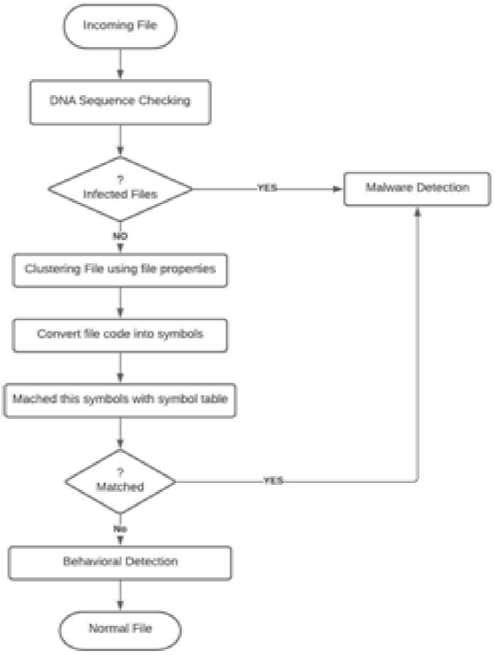


Fig 1: Malware Detection System

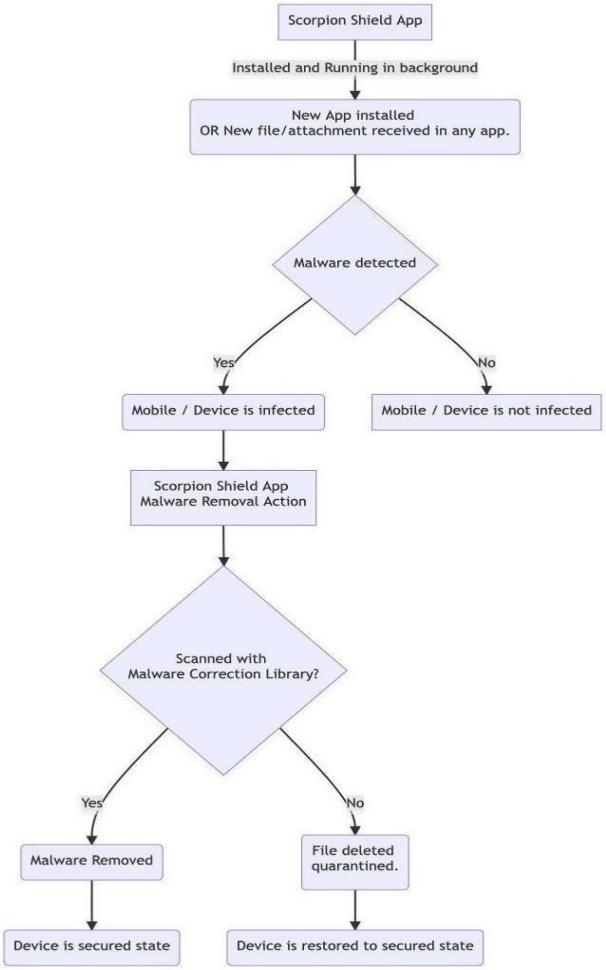

Scorpion Shield App
Installed and Running in background
New App installed
OR New file/attachment received in any app.
Malware detected
Yes
No
Mobile / Device is infected
Mobile / Device is not infected
Scorpion Shield App
Malware Removal Action
Scanned with
Malware Correction Library?
Yes
No
Malware Removed
File deleted
quarantined.
Device is secured state
Device is restored to secured state

Fig 2: Malware Correction System

App will begin by checking OS programs and comparing them to known types of malware. It will also scan your mobile operating system as well as installed applications for behaviors that may signal the presence of a new, unknown malware. All these methodologies will be implemented in our app. Also, not only detection but also protection and advance notifications will be enabled with this app.

Heuristic-Based Detection

Heuristic Virus Checking is a methodology of virus detection. Anti-virus software makers develop a set of rules to distinguish viruses from non-viruses. Should a program or code segment follow these rules, then it is marked a virus and dealt with accordingly. This allows detection of any virus, and theoretically, should be sufficient to deal with any new virus attacks. F-secure virus software uses this method in addition to scanning, although not very many software packages available today utilize heuristic virus checking. Heuristic-based detection is considered the most common form of virus detection that uses an algorithm to differentiate the signature of known viruses against a potential threat. It can unearth viruses that have not yet been discovered, as well as known viruses that have been modified or disguised, and released into the wild again. The only downside is that it can also generate false positive matches, meaning an antivirus scanner may report a file as being infected when it actually isn’t. While these “false positives” are minimal, they’re not uncommon. Antivirus software utilizes several methodologies in scanning, detecting, and protecting computers and systems from viruses. As understanding increases about the vectors malicious code uses to attack and how antivirus software protects computer systems from the viruses, people will be able to more effectively help in creating an environment that is secure and virus free.

Interception Methodology

Interception software detects virus-like behavior and warns the user about it. How to detect virus-like behavior? Use heuristics again. Many viruses will perform some suspicious action, like relocating themselves in memory and installing themselves as resident programs.

Signature-Based Detection

Signature-based detection searches for the specific digital code of a virus (you can think of it as a virus’ fingerprint) and if it finds it, quarantines or deletes it. Once a virus has been identified, it can be added to a signature database, which is kept locally or in the cloud to be accessed when scanning a system for threats moving forward. However, this process requires at least one user or system to be attacked by the malicious software and recognize it before everyone else can be protected against it. Put simply, it’s not very useful for brand new threats.

Behavioral Detection

Behavioral detection is a more modern technique for tracking down known and unknown viruses. It generally looks at what software does rather than examining what a piece of software is. For example, it checks for viruses that attempt to shut down or bypass your antivirus solutions on the system and once found, quarantine or delete them subsequently.

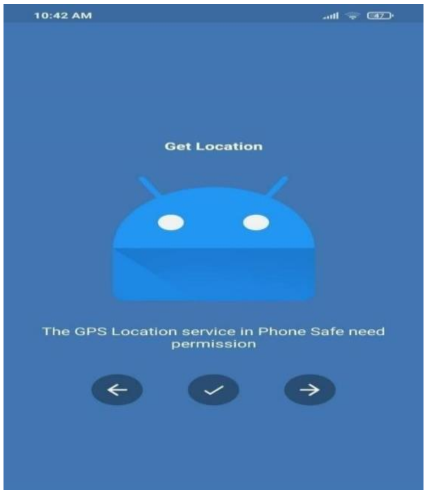
Cloud Antivirus Detection

Cloud antivirus needs an Internet connection to collect information, which is uploaded to, and processed by, a server in the cloud. It generally spares your computer additional processing by running all detection on the server.

IV. RESULTS

This chapter provides the final result and analysis of our project. The app will begin by checking your OS programs and comparing them to known types of malware. It will also scan your mobile operating system as well as installed applications for behaviors that may signal the presence of a new and unknown malware.

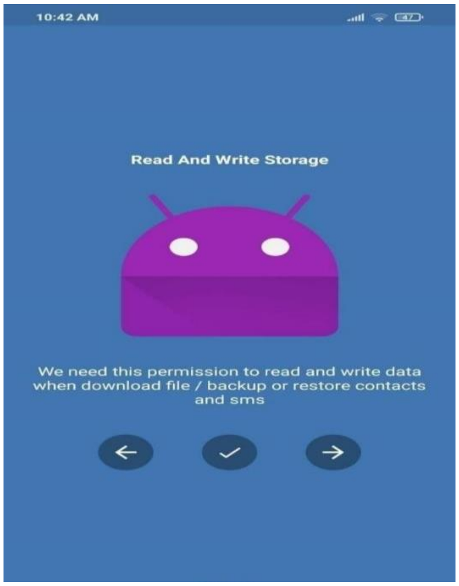
Initially, when the app is started we have to grant permission for Location, Read and write storage, read and write contacts and system alert window. Below are the figures describing these four permissions.



Get Location

The GPS Location service in Phone Safe need permission

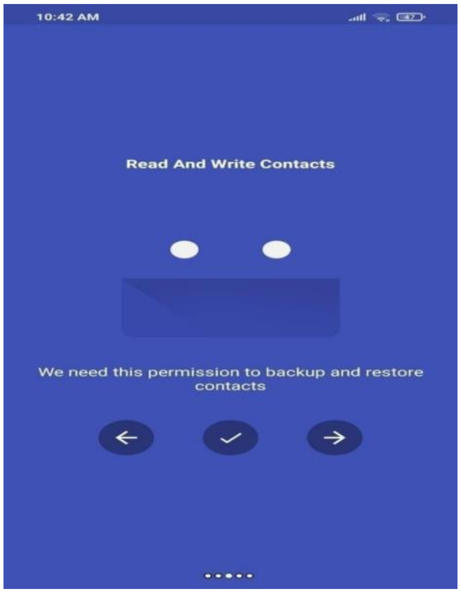
Figure5.1: GetLocation



Read And Write Storage

We need this permission to read and write data when download file / backup or restore contacts and sms

Figure5.2:Read andWriteStorage



Read And Write Contacts

We need this permission to backup and restore contacts

Figure5.4:System Alert Window

Fig 5.5 and Fig 5.6 displays the Index and six features of our application which are Virus scan, Anti-theft, App locker, Wi-Fi security, Call blocker and battery saver.

Virus scan: Virus scans search through your system to locate and remove any malicious threats on your device. You'll find most antivirus software guards against malware. This can include threats like viruses and worms, as well as, spyware, Trojans, ransomware, and adware.

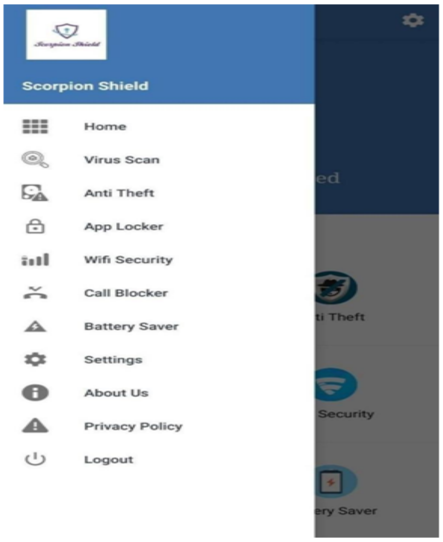
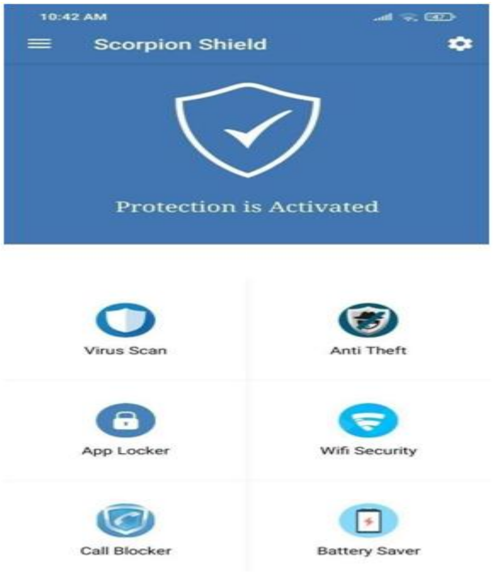


Figure5.5:Index



Protection is Activated

Figure5.6:FeaturesofAntivirus

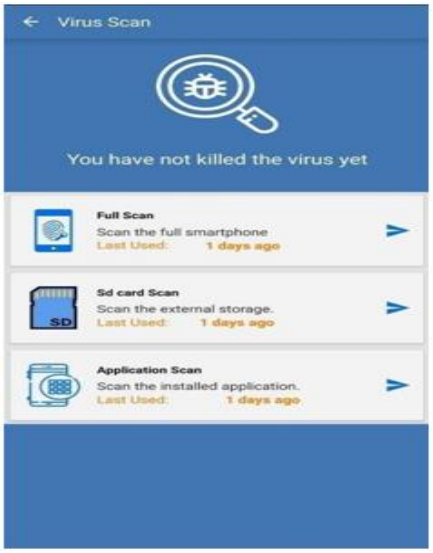
Starting with the first section of Virus scan, as the name suggests it will scan for viruses in the system but on three different levels –

1. Full scan
2. SD Card scan
3. Application scan

Full scan: Full scan does the job of scanning the entire system for the harmful viruses in each and every internal and external files and folders. As you can see when we start the scan we can see two different sections on the user interface. On the left side we can see the progress of the ongoing scan and on the right side detected issues encountered in the scan are seen. A predefined, in- depth scan of your system that checks your storage drives and memory for malware. Quick scan may not detect some malware, but it can still inform you about a virus if your computer is infected. Full Scan requires much more time and OS resources but it detects all known viruses. We recommend performing a Full Scan every week.

SD Card Scan: This scanning does the job of checking for issues in the attached SD card in the system. All of this scanning looks the same as the full scan.

Application scan: This section scans each and every internal and external applications in the system and in the results categorizes every application as medium or high risk application. Antivirus is a kind of software used to prevent, scan, detect and delete viruses from an application. Once installed, most antivirus software runs automatically in the background to provide real-time protection against virus attacks.



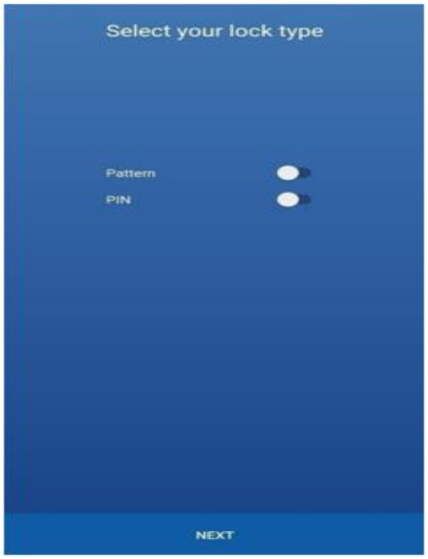
You have not killed the virus yet

Full Scan
Scan the full smartphone
Last Used: 1 days ago

Sd card Scan
Scan the external storage.
Last Used: 1 days ago

Application Scan
Scan the installed application.
Last Used: 1 days ago

Figure 5.7:ScanTypes



Select your lock type

Pattern
PIN

Figure5.8:LockTypes

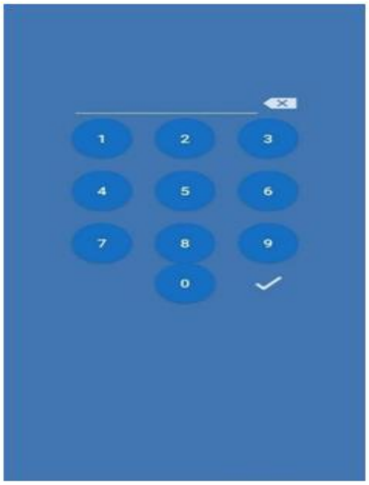
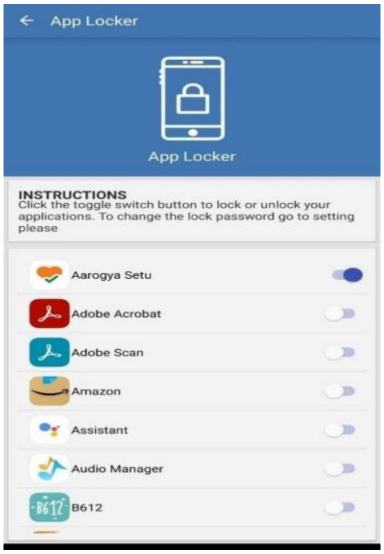


Figure5.9:AddingPin Code



INSTRUCTIONS
Click the toggle switch button to lock or unlock your applications. To change the lock password go to setting please

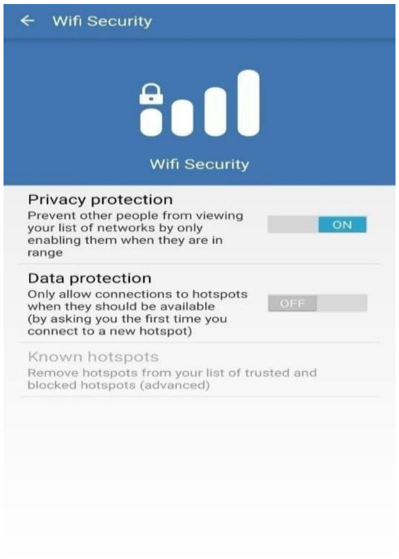
Figure5.10:App Locker

Remote lock screen functionality will lock the system if it received a message of locking it due to security concerns. App locker Pattern and PIN supported- This can be used to lock the system's screen by either setting the password or PIN.

WifiSecurity:- Privacy protection- Warns the system before connecting to an unknown hotspots in the range in order to not lose the system data protection Allows it to connect to the host only if it's safe.

Call Blocker:- Blocks the manually added contact numbers in the system.

Battery Saver:- It optimizes battery, Wi-Fi, Bluetooth, brightness, rotate, mode and timeout when the screen should go on sleep. Turns on the battery saver by turning off the applications in the system such as Bluetooth hotspot etc. so that consumption of power is reduced.

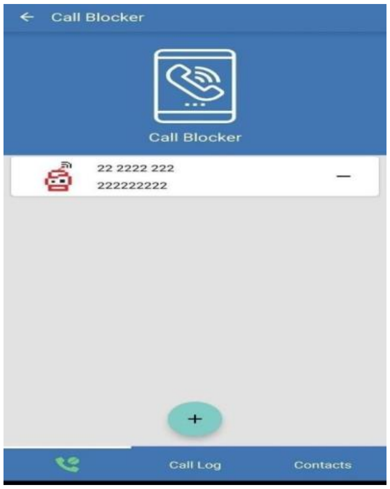


Privacy protection
Prevent other people from viewing your list of networks by only enabling them when they are in range
ON

Data protection
Only allow connections to hotspots when they should be available (by asking you the first time you connect to a new hotspot)
OFF

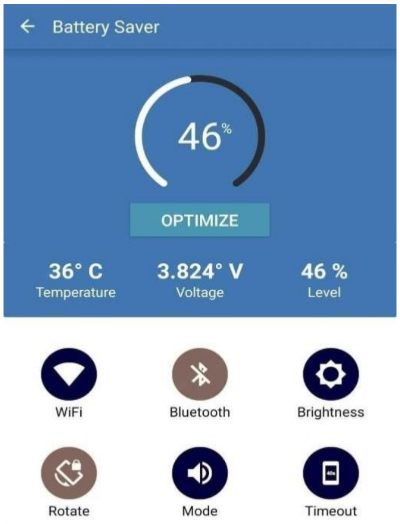
Known hotspots
Remove hotspots from your list of trusted and blocked hotspots (advanced)

Figure5.11:WifiSecurity



22 2222 222
222222222

Figure5.12:CallBlocker



36° C Temperature
3.824° V Voltage
46 % Level

Figure5.13:BatterySaver

V. CONCLUSION

Antivirus software acts as the final line of defense for PC and other devices, which means it can protect or at least mitigate threats to the devices when every other security software fails. Due to swift internet technology development, malicious viruses spread through the developed network. The existing traditional detection antivirus cannot kill new viruses and unwanted malicious files. These antiviruses need improved features to overcome virus problems. Faced with all these situations, this project proposes a new antivirus architecture based on cloud computing. In this engine, different techniques will kill the remaining viruses that a traditional antivirus cannot. This model offers significant advantages over the previous host-based antivirus, including better detection of malware in the cloud..

REFERENCES

[1] Y. Li , "Memory efficient parallel bloom filters for string matching, in Networks Security, Wireless Communications and Trusted Computing", 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, vol. 1, 2009, pp. 485– 488.Ms. Shraddha Jhundhare and Ms. Padmaja Gajare," Fraud Application Detection using Summary Risk Score", IEEE, ICISC-2017.

[2] B. Fechner, "Gpu-based parallel signature scanning and hash generation", 2010 23rd International Conference on Architecture of Computing Systems (ARCS), 2010, pp. 1–6.

[3] X. Zha and S. Sahni, "Gpu-to-gpu and host-to-host multi pattern string matching on a gpu", IEEE Transactions on Computers, vol. 62, no. 6, 2013, pp. 1156–1169.

[4] K. Nakano, "Efficient implementations of the approximate string matching on the memory machine models" Third International Conference on Networking and Computing(ICNC), 2012, pp. 233–239.

[5] D. Man, K. Nakano, and Y. Ito, "The approximate string matching on the hierarchical memory machine, with performance evaluation", IEEE 7th International Symposium on Embedded Multicore Socs (MCSoC), 2013, pp. 79–84.

[6] A. K. Sahoo, K. S. Sahoo, and M. Tiwary, "Signature based malware detection for unstructured data in Hadoop", 2014 International Conference on Advances in Electronics, Computers and Communications (ICAECC), 2014, pp. 1–6.

[7] M. Vincent, A. Mesdaq, E. Thioux, A. Singh, and S. Vashisht, "Dynamically adaptive framework and method for classifying malware using intelligent static, emulation, and dynamic analyses", 2015.

[8] B. Rajesh, Y. J. Reddy, and C. Chakradhar, "Efficient detection of malicious worms with different analysis methods and techniques", vol. 5, no. 4, 2016.

[9] A. Namanya, J. Pagna-Disso, and I. Awan, "Evaluation of automated static analysis tools for malware detection in portable executable files" in 31st UK Performance Engineering Workshop 17 September 2015, 2015, p. 81.

[10] M. Zakeri, F. Daneshgar, and M. Abbaspour, "A static heuristic approach to detecting malware targets", Security and Communication Networks, vol. 8, no. 17, 2015, pp. 3015– 3027.