AI-ENABLED CYBERNETIC ANALYTICS OF SECURITY MODELS FOR SMART SERIOUS GAMES-BASED MOBILE OPERATING SYSTEMS

Abid Ali[1], Faisal Jamil[2], Taegkeun Whangbo[1] and Shabir Ahmad[1*]

[1]Department of Computer Science,
University of Engineering and Technology, Taxila, Pakistan
[2]Computer Engineering Department, Gachon University, Korea

ABSTRACT

Smart serious games are games which are primarily designed for a serious job such as education and training rather than entertainment. Mobile Phones are an essential enabler of smart serious games. Over the past few years, there has been an exponential growth in the security of the cyber-physical system of multiple operating systems. Security challenges have emerged from access scenarios in conventional operating systems. However, in Mobile Operating Systems, there is a lack of systematic study about mobile security measurement. Artificial Intelligence (AI) is one of the critical features which exists inside mobile operating systems. AI enhances the working of Mobile OS functionality by providing thinking on user behavior and extending the functionality. We explore some key security models for different mobile Operating System providers. In particular, the comparison of security policies implemented by multiple mobile operating system vendors. It's challenging to deal with and study the related data models and measurements for mobile operating system platforms. This paper collects, analyzes, and provides effective decisions about the existing research on multiple mobile operating systems. We consider the built-in security, Authentication, Data Protection, Device protection, Application Security, Device Wipe, Mobile Device Management, Cooperate Managed e-mail, Active Sync Support, Device Firewall, Security Certifications, and Virtualizations. AI supports all these features to help OS to extend its functionality for effective game management. We have focused on these components that clearly understand the Mobile operating system structure and support services. General, as well as specific features, are explored about the different platforms of the operating systems. The systematic research study is applied to these platforms to capture the response, and based on these responses, and we developed results based on the feedback and research responses. This comparison aims to make the right choice for mobile users to device the best mobile with a high-security Operating System installed for mobiles partaking serious games in cyber-physical environment.

KEYWORDS

Serious Games, Mobile OS, Symbian OS, Android OS, Windows OS, Blackberry OS, iOS, Artificial Intelligence.

1. INTRODUCTION

Serious games have been evolved with the recent advances in internet of things (IoT) and Cyber-physical systems (CPS). The collection of sensors data and consume it to make informed decisions during a gameplay has taken the serious games into a whole next level, which in literature often known as smart serious games [1-2]. The use of IoT nodes, instead of

David C. Wyld et al. (Eds): AIAP, IT, MoWiN, CCSEIT, CNSA, ICBB - 2022
pp. 23-38, 2022. CS & IT - CSCP 2022 DOI: 10.5121/csit.2022.120402

sophisticated controller offer a variety of advantages, such as context-awareness, pervasiveness, to name a few [3]. However, due to limited computational abilities, they suffer from security challenges. Recently, mobile operating systems are more common for personal and other uses like banking, office, and many other purposes. These devices are commonly known as smartphones. These devices are more generally used today in almost all platforms like social websites, banking, personal information keeping, and others [4]. When people try to access different personal information on their pocket phone, there is an issue discovered that each device is manufactured by other mobile companies like Apple, Samsung, Blackberry, to name a few. Each vendor and smartphone device uses a different operating system for its use. For instance, android operating systems used by Samsung, LG and HTC[5,6]. Windows operating systems are also optimized to use on various smartphones such as Nokia. Apple and Blackberry uses their own operating systems [7]. Rasberry PI, acting as IoT nodes in modern-day CPS uses a variant of android named AndroidThings. However, the optimization of size which is the focus of IoT devices leads to security challenges. For instance, a user using a smartphone, its device's video calls, GPS, Wi-Fi, and many more services are running almost all the time, and due to the internet's openness, the security of these devices is an issue. In the first quarter of 2018, a report issued from McAfee labs showed several malware attacks on smartphones that targeted the Android operating system [8]. When the number of attacks increases, there is a lot of effect on users' data and applications [9]. Different sophisticated security protocols are deployed but it has an associated overhead which at times degrade the performance of IoT nodes due their constraints abilities. Therefore, different sets of security protocols need to considered if the target devices are smart phones or IoT devices.

To this end, we investigate security models used by different operating systems in the context of smart serious games. We also discuss various techniques provided by the operating systems for ensuring the security of personal data and information. Each category of operating system has its security mechanism and thus reviewing the user's knowledge of recent smartphone operating systems' dangers, threats, vulnerabilities, and what exists is fundamental when choosing a smartphone for gameplay. In other words, the paper focuses on optimizing the existing security models in different operating systems to be used in smart serious games devices.

The rest of the paper provides: Section 2 provides the security models implemented in major mobile operating system. Section 3 defines the AI features in the context of Mobile OS. Section 4 describes the comparison based on the security vulnerability of these equipped security models. Finally, Section 5 provides a suitable operating system based on our findings from the study which can be a potential candidate for devices participating in smart serious games.

2. SECURITY MODELS DISCUSSION

2.1. Android Security Model

Since 2008, Android OS has been one of the most used operating systems around the globe. The reason behind this use is its application-free availability and ease to use interface. Despite it has been the leading OS in the market for terminal devices being used in games, according to some data sources from 2011, the security threats on these devices has increased significantly over time, leading to the amount of new malware/hackers [10, 11]. Android is an OS developed for smartphone us and can be used by different vendors. As depicted in Figure 1, the Android OS provides a boxed application and data execution environment. A well customized and groomed embedded Linux kernel system interacts with the smartphone hardware and other hardware equipment. The middleware includes Android RT, libraries, and VM, application's Application Programming Interface runs on top of Linux Kernel [12]. To simplify the running and execution

environment, an application's management interface is used via APIs. Each application executes itself under the supervision of a Dalvik Virtual Machine (DVM) that is running under the control

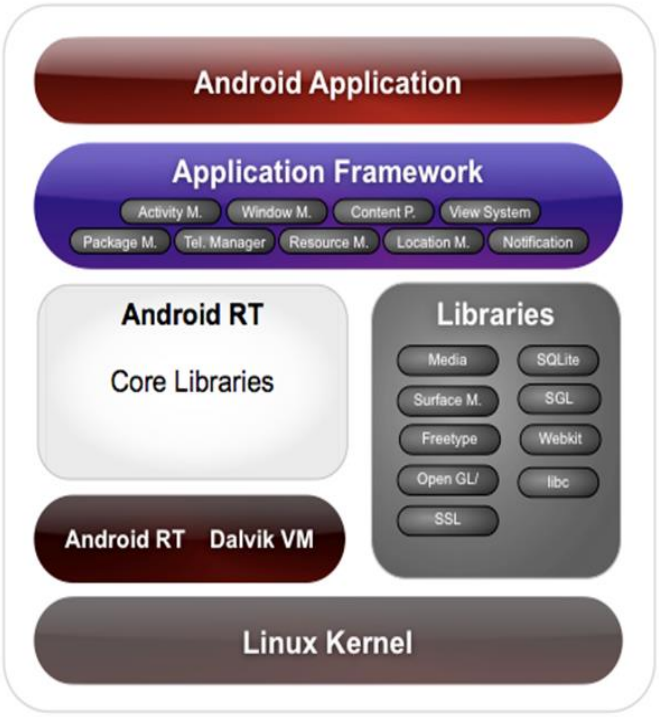

Figure 1. Android Application architecture [13]

of a unique UNIX user id (UID) [14]. The smartphone comes with a pre-installed applications, such as address book, call dialer, messenger for SMS and MMS, etc. When a user chooses the device based on the Android operating system for the applications and their data usage, the user does not know what type of attacks they can suffer while using this operating system platform. The user does not need to perform the security arrangements on these terminal devices.

The security is purely based on the operating system structure in which structure it is used for security permission. Android OS provides two different levels of security, i.e., application-level security and kernel-level security [15].

Application permissions in android OS only check and set the security and check license at the install time of the application after the install application on an android user does not change the application permission on these devices. App of the authorization are set at the install time of the application, so the user needs to keep a check on all of permission access levels at the install time when its application wants to check all of the applications needs to set the app permission when the user chooses the application at from the Android play store and wants to install that application on the device. Figure 2 shows some at from the Android play store and wants to install that application on the device. Figure 2 shows some of the access permissions on the Android OS [12-15]. Android OS provides the component level security that the whole application on the Android should be designed on these four components [16, 17].

First off, the activity component defines the application user interface; each screen of the android application defines an activity. One activity on the screen can cause the start-up of other events and for returning the fundamental values. One of the significant activities of the android

operating system is its phone dialer activity in which the user dials the call to other android devices. The service component performs the background processing. When the user interface disappears from the current interface, but the application is still running on the back, that activity is provided by the services component (like when users download a file). Services are the way of communication between different components and application interaction via some form of Remote Procure Call (RPC). Data is collected back with the help of this application and call-back services. The content provider provides the facility for database handling and stores and retrieves data by using the relational database. Every type of content provider has different authorities that describe which kind of content it takes during its execution. Some of the components need to handle the SQL queries on the database like (INSERT, UPDATE, and DELETE) for content reading and writing. Content provides stores all the activities in the database record.

The broadcast receiver component acts as the main box for sending and receiving messages from different applications, commonly in the Android OS application code broadcast messages to the intended receivers. The broadcast receivers thus subscribe to the procedures to receive the messages sent to them.

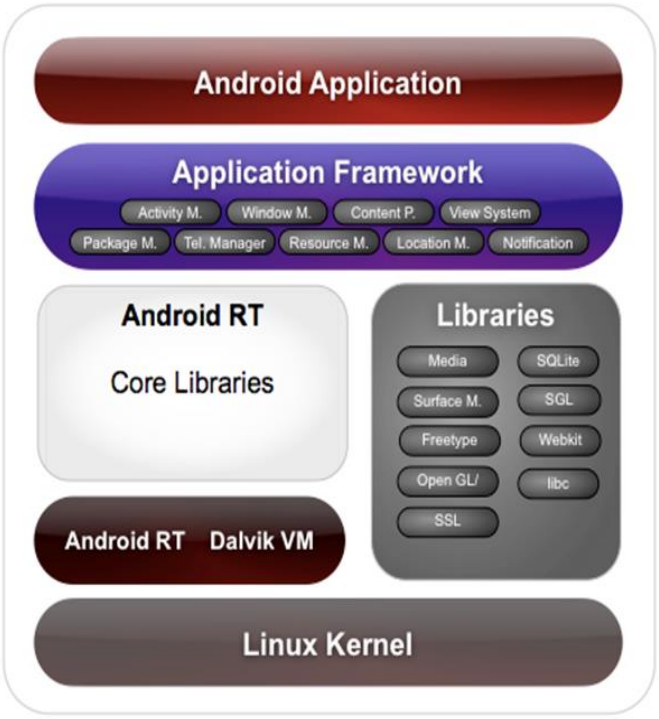

Figure 2. Android Application Permission [18]

2.2. iOS Security Model

Today iOS is also an effective and most widely used mobile operating system in the smartphone market. In the initial years of iOS, apple products were mainly used in Europe. Still, nowadays, it is also one of the widely used operating systems all around the globe, especially in Asia and Africa [19, 20]. If we talk about the security point of view, this mobile operating system provides security at the component and application levels. iOS offers one of the most robust security technology and features [21]. Apple iOS provides two types of security, both at the hardware and OS levels [22]. At the Low level of the operating system, firmware security features protect from viruses and malware attacks. High-level OS levels provide security of information at the app's

level access. That leads to preventing unauthorized use and helping thwart attacks provided on iOS.

In Figure 3, the iOS operating security model secures information while mobile usage is enabled, other installed apps from different sources, and synchronization. The complete design is based on the international standard procedure—and an apple a lot of time for enhancing the security of its products and improving the plan without any effect on the security precautions. Apple strongly focuses on having done additional design work to improve its safety. The iOS security model consists of the following architectural design [23-27]

System Architecture apple iOS is one of the best operating systems in terms of the boot loading process. Each step in the booting ensures the system is trusted cryptographically and signed by Apple itself. When the iOS is turned on the device, the application processor on the device loads the executable code from read-only memory called Boot ROM. The Boot ROM code has Apple Root CA public key, and this public key is used to authenticate Boot loader at the low level (LLB). Apple iOS assign this boot loader. It is the first step for the security measure by Apple iOS.

When the Boot Loader for the low-level completes its assigned task, this loader has the built-in functionality to load the next stage of the iOS booting process, iBoot, which then loads the final set of the booting process book kernel. This whole boot process allows iOS to load on only validated apple devices.

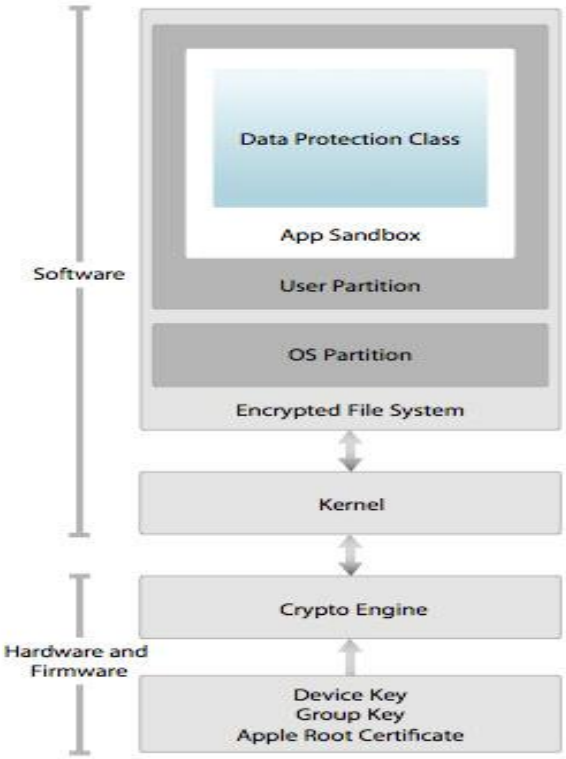

Figure 3. The security architecture of iOS [25]

Once the apple kernel is loaded, its next responsibility is to start and control all the user iOS processes and applications. Ensure that all of the apps need to be approved by the Apple iOS-

issued certificate [26]. Applications from the other sources must also be run and started by using the apple issue certificate.

Encryption and Data Protection On iOS, the encryption and protection facilities are based on hardware and software technologies. Every iOS has a path between the phone's main memory and the ROM-based storage with the help of a crypto-based key called AES 256 based key to achieve a high level of encryption and security [27]. This SHA-1 cryptographic algorithm is implemented at the hardware level to improve safety for implementing the security overhead. When the Apple mobile processor is manufactured, this 256-bit key cryptographic algorithm is fed unique ID and group ID in this hardware device. There is a unique ID and a standard group ID for all the Apple products used in the market on every Apple device.

Data protection is also an essential consideration in iOS, where all the user data is secure using a crypto key technology that is only used in the iOS platform. Whenever iOS need to secure users' data, it assigns a class to each segment. These class keys ensure when data needs to be accessed, and the key will unlock when information is accessed. When a new fine is created for the data protection, this data protection makes a unique key 256-bit in length; this key is based on a per-hardware basis and then forwarded to the AES engine. This AES engine uses a key to encrypt the file for storing it on the flash memory by sing CBC coding scheme [28]. When the file is encrypted with the SHA-1 encryption scheme, an output file is created that is Initialization Vector (IV) and stored in the shift register. iOS device passcode is one of the data protection mechanisms and for accessing the device. Every iOS device is equipped with a four-digit passcode that the user device needs to enable on its mobile platform. The whole iOS device is protected when the passcode is enabled on the device. This passcode interacts with the UID. The start screen passcode security is to make the iOS much more secure, and when a user attempts a passcode, then every time makes it safe. If a user attempts all the password combinations, then it will take approximately 80 for each attempt [29]. Using this speed, users need to try all the passcode combinations for about five and a half years. There is a six-character passcode that will take, and for the nine characters, it will take two and a half years. If the user attempts all these combinations, they will make it more secure because no one can try all the combinations. So, it is tough to break the security of the iOS passcode with encryption mechanism.

Network security including all other services iOS also provides network security services to its users. iOS provides authenticated, authorized, and encrypted communication between different devices over Wi-Fi and cellular internet services. iOS is less target for network attacks because of the limitations of ports and unavailability of the network firewall and other network utilities such as web servers, telnet, and shells. iOS uses its built-in encrypted apps for communication and other entertainment activities because these applications are very encrypted and authenticated by iOS users. These communication apps include FaceTime, iMessage, and iTunes. All the iOS devices are equipped with SSL and TSL layers for encryption of their data. iOS operating system supports three types of security measures [25]; Transport layer security, Secure socket layer and STLS. On iOS, all its internet-related applications like mail cylinder internet services and Safari use these types of encrypted communication mechanisms to ensure security between devices and the network.

Device access, one of another iOS security parameters is device access, and every smartphone has its optionality to active passcode to access the User Interface (UI) of that particular device. iOS is built-in with a four-digit passcode to access its first UI interface. This four-digit passcode is highly encrypted, and hard to guess such type of encrypted passcodes. Users can also set long alphanumeric passcode from 4 digits to longer passcode because this longer passcode is hard to guess. Every iOS device has a configuration file called XML. This XML file is based on all system configuration settings like passcode policies, Wi-Fi settings, VPS settings, e-mail settings,

exchange settings, web clips, credentials and keys, and a lot more. If a user comes and deletes this configuration XML file, all system settings will be removed and need to re-establish all locations.

2.3. Blackberry RIM (Research in Motion) OS Security Model

One of the Operating systems for mobile platforms is Blackberry. This blackberry operating system is specially designed for the enterprise's use, and individual users in terms of confidentiality, integrity authenticity Blackberry operating system is developed by Blackberry Inc and called it Blackberry RIM (Research in Motion) for their Blackberry devices. It is not a multi-platform operating system; it is only installed on Blackberry phones and smartphones [30].

Blackberry operating system is an ultimately end-to-end platform for mobile devices [31]. Here we now discuss the security model used by the Blackberry operating system. It encompasses the following subcategories; protecting data, protecting work data on personal use devices, enforcing strong access control and managing devices

Protecting data: The fundamental component of the blackberry data transection is its security for both enterprise and individual use. Blackberry provides a built-in data encrypting mechanism that provides robust data security policies. It also protects and manages the applications and devices from end-to-end security of data. Fig 4 shows the blackberry enterprise security and application access from the blackberry enterprise servers. This US-based company protects against all types of illegal entry. Data using Blackberry is strongly encrypted, and corresponding encrypted key is also used within these [32].

Messages and e-mail encryption are also handled by the Operating system using industry-standard S/MIME encryption. This operating system uses the concept of tunnelling in which multiple encryptions are done during the transmission over the network, which leads to achieving a higher level of security for these devices [33]

Enabling Work Data on Personal Use devices

Protecting users' data is the critical and comprehensive part of mobile devices, but the device's operating system only provides this protection. Blackberry allows the user to establish a quick setup for password creation to secure the data from illegal access. In Blackberry OS, the Blackberry Balance is a registered application that provides the control employee's data, companies data security, control network connection, and many more features that this application contains to process [34].

Enforcing Strong Access Control

Blackberry OS provides multiple control access features like authentication, anti-counterfeiting manufacturing, and device protection. Authentication is also taken place in blackberry devices for minimum chances for data loss [35].

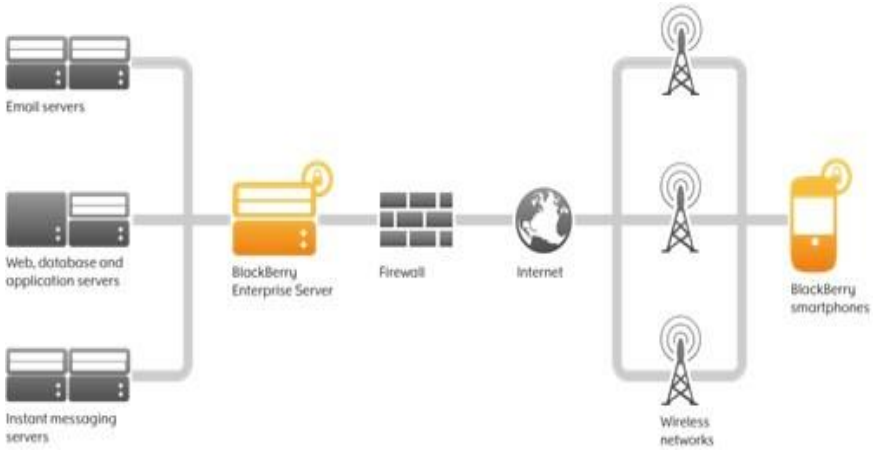

Figure 4. Blackberry enterprise security [36]

This authentication is key based, where all of the keys are kept private and secure for data protection. Fig. 5 shows the Blackberry 10 operating system application and data access mechanism. Whenever a blackberry device is activated, this device has a built-in tool that is first generated and key. It then sends this key to the operating system's server for creating and authenticating by the OS Server. Then this server sends back a certificate for authenticating the client device. Blackberry uses the management root certificate for authenticating the certificate for accessing the web services and their contents.

Managing Devices: Blackberry operating system is also one of the devices that can manage other devices like iOS, Android, and Windows phones. It has a built-in administration console to handle such a type of system. App of the managed application and data is secure from all the data and personal information applications. A trusted blackberry security model provides built-in security for blackberry devices apps developed to secure their private Virtual Private Network (VPN) [37]. Blackberry mobile device management is software used to connect and provide data sharing in a security manager for other operating systems.

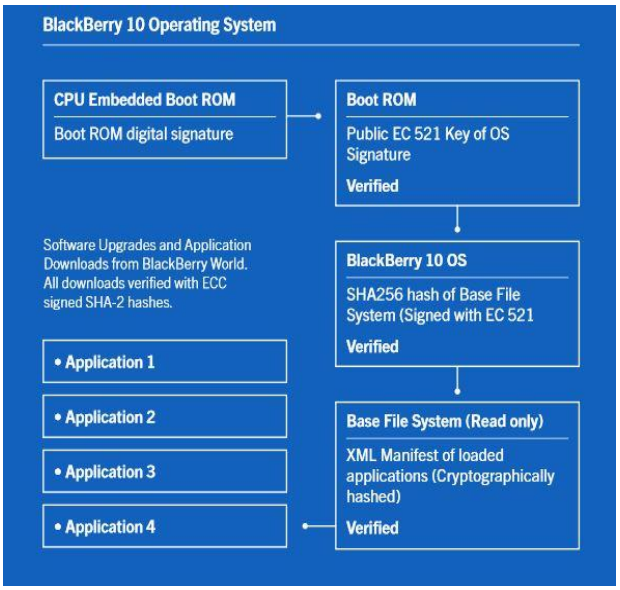

Figure 5. Application and data access mechanism in blackberry OS [38]

2.4. Windows Operating System Security

Windows operating system gained popularity from its desktop operating system, which provides a productive operating system for its users, and it is also now on the mobile platform [39]. At the start, Microsoft brought forward and developed windows seven operating systems for the Nokia smartphones. Later, they enhance user experience and get a new UI for their windows operating system, consisting of a 'Metro' based design. This new type of operating system supports the new kind of experience, which is multi-core processor support, high-resolution screen support, and also, most but not least, their more significant storage [40]. And the latest operating system is currently in use which is Windows 8.1 for mobile users [41].

The windows 8 phone consists of the following security measure taken by the windows 8 phone from a security perspective [42, 43].

Device Encryption: Windows phone provides complete internal protection against different attacks. Windows built-in BitLocker architecture gives full device encryption.

Data Encryption: Data encryption is another security measure in windows eight phones which is very important from the data point of view. When data is encrypted in the device, no other device can collect that data because it does not support it. It also helps to provide authentication between communicating parties.

Data Leak Prevention: Windows 8 phone has a built-in mechanism to prevent its data from leakage. So, Information Right Mechanism (IRM) is a way to avoid this type of information. IRM also protects e-mail and phone contents from illegal access from other devices and other applications on another phone.

Digital Signature: Windows 8 phones also provide security from other applications using a digital signature. It also helps to authenticate the information from another party.

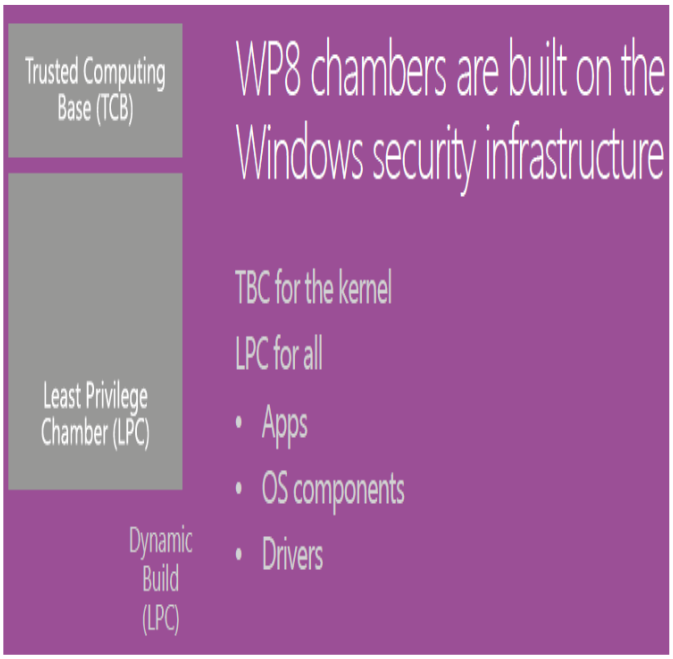

Figure 6. Windows 8 phone Application security model [41]

3. ARTIFICIAL INTELLIGENCE IN OS

Recent developments in AI and electronic technology raised the demand for these technologies in a modern OS. All current OS have AI in their User Interfaces, Human Machine Interaction features, Hardware Technology, Communication, Application support, etc. Machine to Machine Communication is possible through global services such as Internet services and other related platforms. In Modern OS, the AI component have become necessary partly because it controls the user actions, change working with the incomplete scenario, control user actions, and work with unsatisfied, incomplete, and noisy input values [43, 42]. All modern OS contains the user interface with a compelling voice as an AI feature to process and respond without typing a single word.

Besides all these, the advanced level of hardware technology also supports the next generation OS with AI features. The modern hardware contains new technology called AI on Chip (AI SOC). It includes AI sensors that effectively control the multi-user tasks with an effective computation environment [44]. Figure 7 contains such OS AI-enabled features.

AI controls user Interfaces to enhance the working of the OS for users and interactive user programming and other related facilities. Different OS platforms govern the inputs for practical reasoning and system analysis, and good communication level features. There are several reasonable devices which enhance the total working performances [45]. Figure 8 shows the AI features for the Human User interface for handling all such types of interfaces. In figure 8, CLI is Command Line Interface, GUI is Graphical User Interface, AUI is Audible User Interface, and UGI is User Gesture Interface.

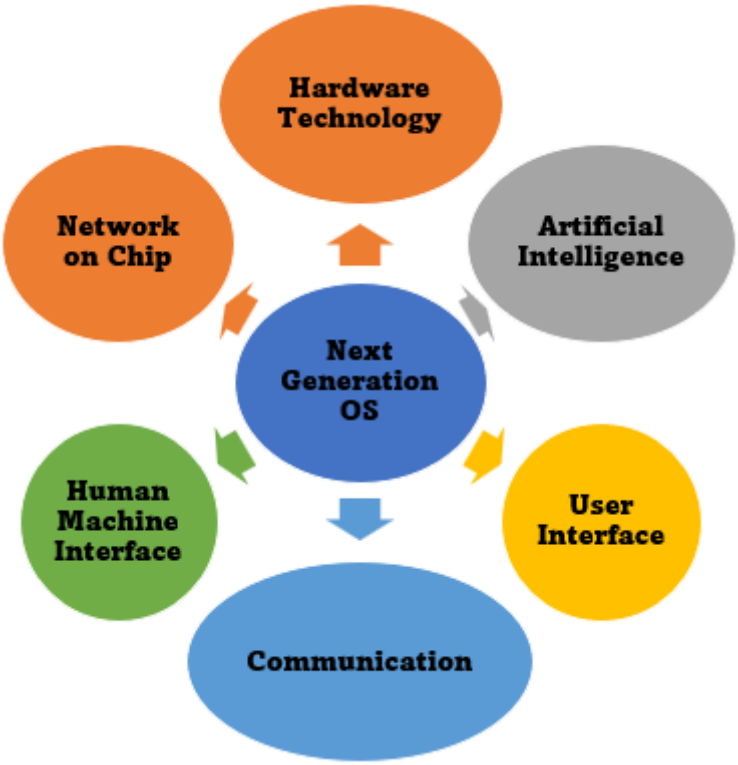

Figure 7. Operating Systems with AI features

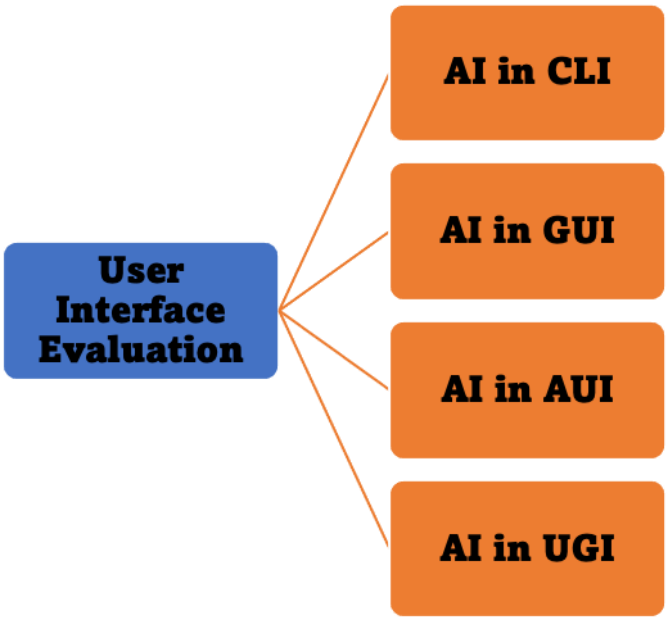

Figure 8. Evaluation of AI in OS User Interfaces

4. DISCUSSION

Every mobile operating system focused on Security, Data Protection, Authentication of users, Device Protections, Wipe of Device, Mobile Support, Concurrent E-mail management, Mobile Firewall Capabilities, Security Certifications, and Virtualization Security Certification based on descriptive technology. Every mobile device manufacturer wants appropriate mobile operating systems for their mobile devices. Figure 7 shows the usage statistics of mobile phone operating system users around the world. This gives us a clear picture that active mobile users using mobile operating systems. Based on the analysis found in the study, we announced that the most significant number of users using Android. But based on the evaluation in figure 7, according to the security, the Blackberry mobile operating system is best suitable for users. On the second, the security of the iOS for Apple mobile devices takes the second number with the second number on the mobile device selection procedure. According to the report, the most number of attacks are found yet on android devices [46].

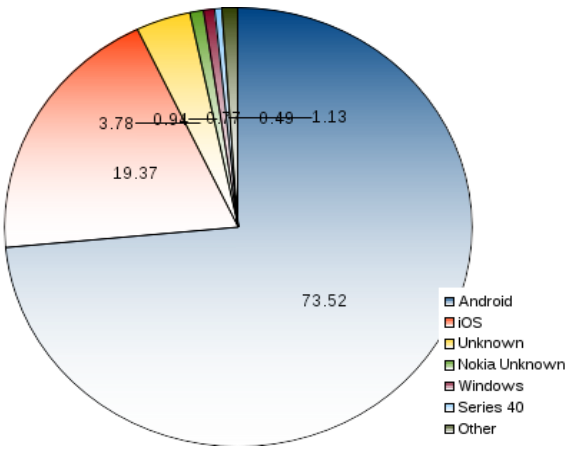

Figure 9. Mobile Operating Users Statistics

We have four primary Mobile Operating systems that have existed till now for most smartphones. Descriptive research is applied to the gathered data from multiple online and offline sources. Based on the analysis and data collected from different sources, we conclude that every type of mobile operating system has its own security mechanism for its users to secure their data from different malware and attacks either from the internal system or from the external system.

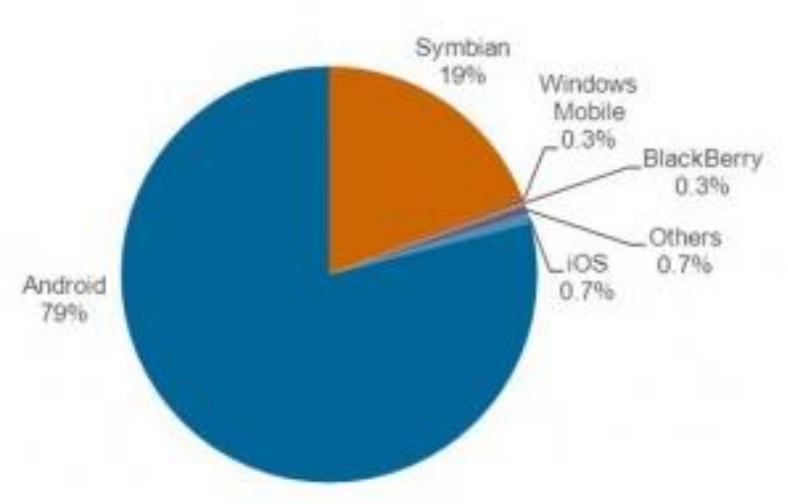

Figure 10. Mobile Phone Operating System attacks

Figure 7 describes the results based on our research. Based on our results, as Android is a free open-source mobile operating system, most of the data is handled by different programmers, changing its security. Apple iOS is, on the other hand, is another OS for mobile users, and it provides better security measures than Android because it is not open source. It offers better security as internal data, applications, as well as online security measures. Few other operating systems give other security measures and provide a better user experience as Blackberry uses its type of security measures. We must assign parametric values to the data gathered. Figure 8 shows a complete descriptive research result that shows the security according to multiple parameters listed below.

We compare our comparison based on the following security measures

1. Built-in security
2. Authentication
3. Data Protection
4. Device protection
5. Application-level security
6. Device Wipe
7. Mobile device management
8. Cooperate managed e-mail
9. Support for active sync
10. Device firewall
11. Security certifications
12. Virtualizations

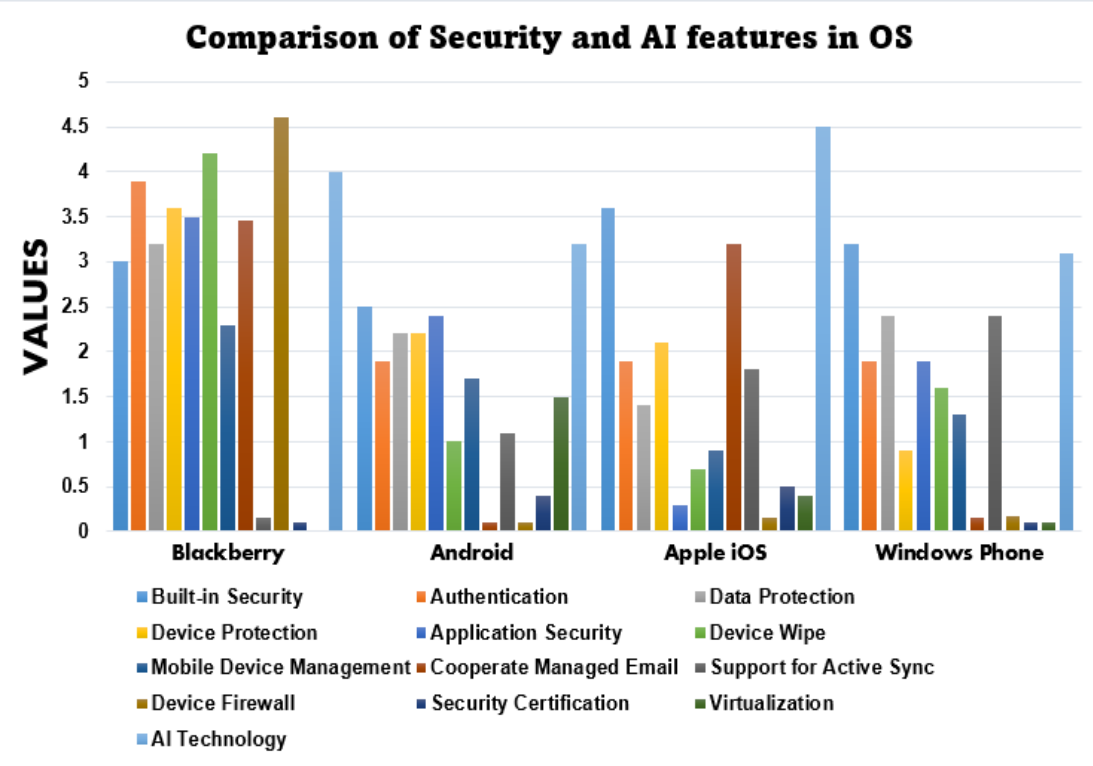

Figure 11. Cybernetic Comparison of Security Tools

5. CONCLUSIONS

Mobile Devices are remarkable inventions with more advanced Operating Systems with the most outstanding features for users to use in their daily and work purposes. Multiple applications on mobile phones extend the functionality of mobile phones. Technological advancements bring more elements to the smartphone with the penalty of features. This paper focuses on major vital points that are very helpful for the organization to adapt to the secure and well-groomed operating system from all of the operating systems in the market. Users of the operating system choose the best features of mobile devices with highlighted parts. All Operating systems of mobile devices effectively manage the processing power, unit of processing (processor), data storage and processing capabilities, network selection, and internet resource allocations. In support of security, the AI also enables multiple intelligence features in Mobile Operating Systems. AI controls the working of Mobile OS with its numerous features to get practical and under control. Users have some priority features when choosing the operating system from all operating systems in their interest. It's like an easy interface (user-friendly), secure, professional motions, multiple functionalities, official activities, entertainment, financial research, news. The priority of the OS design is to provide faculty to the users, so it controls and AI coordinates the user values and provides adequate user interface coordination. User priority is significant for choosing the best operating system for their personal use and their business purposes..

ACKNOWLEDGEMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (grant number: 2021R1I1A1A01045177)

REFERENCES

[1] Ahmad, S., Khan, F., & Whangbo, T. K. (2022). Performance Evaluation of Topological Infrastructure in Internet-of-Things-Enabled Serious Games.

[2] Ahmad, Shabir, Faisal Mehmood, Faheem Khan, and Taeg K. Whangbo. 2022. "Architecting Intelligent Smart Serious Games for Healthcare Applications: A Technical Perspective" Sensors 22, no. 3: 810. https://doi.org/10.3390/s22030810

[3] Ahmad, Shabir, et al. "An Adaptive approach based on resource-awareness towards power-efficient real-time periodic task modeling on embedded IoT devices." Processes 6.7 (2018): 90.

[4] Lipp, M., et al. Armageddon: Cache attacks on mobile devices. in 25th {USENIX} Security Symposium ({USENIX} Security 16). 2016.

[5] Bhushan, A., A Comparative Analysis of Consumer Behavior of Nokia and Samsung Mobile Users. International Journal of Industrial Organization, Forthcoming, 2016.

[6] Schlagkamp, S., et al., Understanding user behavior: from HPC to HTC. Procedia Computer Science, 2016. 80: p. 2241-2245.

[7] Riadi, I., R. Umar, and A. Firdonsyah, Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method. International Journal of Computer Science and Information Security (IJCSIS), 2017. 15(5): p. 155-160.

[8] McAfee, L., McAfee Labs 2018 Threats Predictions. Mission College Boulevard, Santa Clara, CA, 2017.

[9] Zhou, Y. and X. Jiang. Dissecting android malware: Characterization and evolution. in 2012 IEEE symposium on security and privacy. 2012. IEEE.

[10] Enck, W., M. Ongtang, and P. McDaniel, Understanding android security. IEEE security & privacy, 2009. 7(1): p. 50-57.

[11] Bhat, P. and K. Dutta, A survey on various threats and current state of security in android platform. ACM Computing Surveys (CSUR), 2019. 52(1): p. 1-35.

[12] Zhauniarovich, Y., Android Security (and Not) Internals. Trento: ASANI, 2014.

[13] Shukla, H., A Survey Paper on Android Operating System. Journal of the Gujarat Research Society, 2019. 21(5): p. 299-305.

[14] Oliver, E., A survey of platforms for mobile networks research. ACM SIGMOBILE Mobile Computing and Communications Review, 2009. 12(4): p. 56-63.

[15] Palmieri, M., I. Singh, and A. Cicchetti. Comparison of cross-platform mobile development tools. in 2012 16th International Conference on Intelligence in Next Generation Networks. 2012. IEEE.

[16] Sbîrlea, D., et al., Automatic detection of inter-application permission leaks in Android applications. IBM Journal of Research and Development, 2013. 57(6): p. 10: 1-10: 12.

[17] Felt, A.P., et al. Android permissions demystified. in Proceedings of the 18th ACM conference on Computer and communications security. 2011.

[18] Zarni Aung, W.Z., Permission-based android malware detection. International Journal of Scientific & Technology Research, 2013. 2(3): p. 228-234.

[19] Wang, G. Designing smule's iphone ocarina. in Proceedings of the International Conference on New Interfaces for Musical Expression. Pittsburgh. 2009.

[20] McMillan, D., et al. Further into the wild: Running worldwide trials of mobile systems. in International Conference on Pervasive Computing. 2010. Springer.

[21] Giese, D., et al., Security Analysis of Near-Field Communication (NFC) Payments. arXiv preprint arXiv:1904.10623, 2019.

[22] Philip, J. and M. Raju, An Overview About the Security Architecture of the Mobile Operating System iOS. Indian Journal of Computer Science, 2019. 4(1): p. 13-18.

[23] D'Orazio, C.J., et al., A Markov adversary model to detect vulnerable iOS devices and vulnerabilities in iOS apps. Applied Mathematics and Computation, 2017. 293: p. 523-544.

[24] Bhardwaj, A., K. Pandey, and R. Chopra, Android and iOS Security-An Analysis and Comparison Report. Int'l J. Info. Sec. & Cybercrime, 2016. 5: p. 30.

[25] Zlatolas, L.N., et al., Models of Privacy and Security Issues on Mobile Applications, in Mobile Platforms, Design, and Apps for Social Commerce. 2017, IGI Global. p. 84-105.

[26] Leavitt, N., Mobile security: finally a serious problem? Computer, 2011. 44(6): p. 11-14.

[27] Yang, W., et al. Vulnerability analysis of iPhone 6. in 2016 14th Annual Conference on Privacy, Security and Trust (PST). 2016. IEEE.

[28] Lauer, I. and T. Lauer, Undoing encryption: the argumentative function of metonyms. Argumentation and Advocacy, 2018. 54(1-2): p. 53-71.
[29] Saicheur, V. and K. Piromsopa. An implementation of AES-128 and AES-512 on Apple mobile processor. in 2017 14th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON). 2017. IEEE.
[30] Gao, F., L. Leng, and J. Zeng. Palmprint recognition system with double-assistant-point on iOS mobile devices. in Proceedings of the 29th British Machine Vision Conference, BMVC. 2018.
[31] Goldsmith, M.A., et al., Mobile communications device providing heuristic security authentication features and related methods. 2019, Google Patents.
[32] Eisner, A., et al., BLACKBERRY LIMITED: IS THERE A PATH TO RECOVERY? Global Journal of Business Pedagogy Volume, 2018. 2(1).
[33] Philippe, E. and L. Bes, Method for manufacturing a multilayer data medium with security marking which can be marked by laser. 2019, Google Patents.
[34] Bender, C.L., D.J. Major, and J.R. Cardy, Data source based application sandboxing. 2019, Google Patents.
[35] Zaborski, A.A. and A.Y.W. Tam, Mobile phone shell. 2016, Google Patents.
[36] Novac, O.C., et al. Comparative study of Google Android, Apple iOS and Microsoft Windows phone mobile operating systems. in 2017 14th International Conference on Engineering of Modern Electric Systems (EMES). 2017. IEEE.
[37] Yesilyurt, M. and Y. Yalman, Security threats on mobile devices and their effects: estimations for the future. International Journal of Security and Its Applications, 2016. 10(2): p. 13-26.
[38] Joseph, J. and K. Shinto Kurian, Mobile OS–Comparative Study. Journal of Engineering Computers & Applied Sciences, 2013. 2(10): p. 10-19.
[39] Pawłowicz, B., A. Strzałka, and M. Tybura, Privacy and security of contact data on mobile phones with Windows Phone Operating System. Measurement Automation Monitoring, 2017. 63.
[40] Jaafar, A., et al. Dynamic home automation security (DyHAS) alert system with laser interfaces on webpages and windows mobile using rasberry PI. in 2016 7th IEEE Control and System Graduate Research Colloquium (ICSGRC). 2016. IEEE.
[41] Zaidi, S.F.A., et al., A survey on security for smartphone device. International journal of advanced computer science and applications, 2016. 7(4): p. 206-219.
[42] Waheed, A. and H.A.F. Khan. Artificial Intelligence in Operating System. in Proceedings of the 2019 3rd International Conference on Computer Science and Artificial Intelligence. 2019.
[43] Tonogai, D., AI in Operating Systems: An Expert Scheduler. 1988: University of California.
[44] Thórisson, K.R.J.M. and Machines, Integrated AI systems. 2007. 17(1): p. 11-25.
[45] Malallah, H., et al., A comprehensive study of kernel (issues and concepts) in different operating systems. 2021: p. 16-31.
[46] Omelchenko, T., et al. Protection Software for Mobile Operating Systems. in 2018 International Conference on System Modeling & Advancement in Research Trends (SMART). 2018. IEEE.

AUTHORS

ABID ALI is pursuing his Ph.D. degree in Computer Science at the Department of Computer Science, The University of Engineering and Technology Taxila Pakistan. He did his MS (CS) from the same institution in 2018. He is currently serving as a Lecturer in Computer Science in Higher Education Department KP Pakistan. He has 8 years of teaching and 5 years of research experience. His Currently Research interests are IoT, Distributed Computing, Big Data, Task Scheduling, Data mining, Cloud and Mobile Cloud Computing ICN, SDN, and VANET.

Faisal Jamil has secured his Ph.D. in the Department of Computer Engineering from Jeju National University, the Republic of Korea. He received his MS in Computer Science from University of Engineering and Technology, Taxila Pakistan in 2018. He did his BS in Computer Science from the Capital University of Science. His research work mainly focused on Internet of Things application, Blockchain application, energy optimization and prediction intelligent service, and mobile computing. He is currently serving as a postdoctoral researcher with Gachon University at the department of Computer Engineering.

Shabir Ahmad has earned his PhD in Computer Engineering from Jeju National University, the Republic of Korea. He received his Master's degree in Computer Software Engineering from the National University of Science and Technology, Islamabad, Pakistan, in 2013. He did his Bachelor of Science in Computer Systems Engineering from the University of Engineering and Technology, Peshawar, Pakistan, and is now serving in the same university as a faculty member of the Software Engineering Department. His research work mainly focused on Internet of Things applications, cyber-physical systems and Intelligent systems.