EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Enhancing Security of Android Operating System Based Phones using Quantum Key Distribution

Nageen Saleem[1], Areeba Rahman[1], Muhammad Rizwan[1], Shahid Naseem[2], Fahad Ahmad[1,*]

[1]Department of Computer Sciences, Kinnaird College for Women, Lahore, Pakistan
[2]Department of Information Sciences, University of Education, Lahore, Pakistan

Abstract

The Android-based devices are gaining popularity now a day. With the widespread use of smartphones both in private and work-related areas, securing these devices has become of paramount importance. These devices are prone to various security issues of malicious attacks and performance problems. Owners use their smartphones to perform tasks ranging from everyday communication with friends and family to the management of banking accounts and accessing sensitive work-related data. These factors, combined with limitations in administrative device control through owners and security-critical applications, make Android-based smartphones a very attractive target for attackers and malware authors of any kind and motivation. Applications keep and manage diverse intrinsic data as well as sensitive private information such as address books. Smartphones enable swift and easy data exchange via 3G, 4G, and Wi-Fi. Thus, personal information stored on smartphones is prone to leakage. Up until recently, the Android Operating System's security model has succeeded in preventing any significant attacks by malware. This can be attributed to a lack of attack vectors which could be used for self-spreading infections and low sophistication of malicious applications. The research provides a distinctive solution to the security threats being found in the Android operating system. This paper presents a data security and quality enhancement method based on amalgamating quantum attributes into the Android operating system that could effectively solve the issue raised. The paper provides a proposed architecture of Quantum Key distribution being embedded within the Android OS to improve efficiency. However, QKD is a new technology. The research unleashes the possible ways in which quantum could be effectively embedded in smartphones to resolve certain data security problems. Quantum key distribution implements the Android to guard and use in the case of a run-time kernel compromise. That is, even with a fully compromised kernel, an attacker cannot read key material stored in Quantum key.

Keywords: Quantum Key Distribution (QKD), BB84 Protocol, Third-party applications, Encryption.

Received on 10 October 2019, accepted on 12 June 2020, published on 15 June 2020

doi: 10.4108/eai.13-7-2018.165281

*Corresponding author. Email: Fahad.ahmad@kinnaird.edu.pk

1. Introduction

The most prevalent mobile platform is Android mobile OS in the world. The Android operating systems have been subjugated the smartphone world with a share of 86.8% [1]. Android systems provide a very user-friendly interface and due to its vulnerable and open-source characteristics, it has attracted many software developers. As a result, a large number of user-friendly applications have been developed until now that not only made our life easier but also provide a platform for learning [2].The applications are developed for some specific purpose that targets a single domain. But there are many apps worldwide that are used in different research areas. Nowadays, smartphones are sensor-based and they have a built-in feature of sensing that provides ease and it is also a gateway towards research in many different realms [3]. A typical Android architecture is presented in Fig.1 [4].

Hardware and sensors. Android is based on Linux kernel and it follows Linux Discretionary Access Control (DAC) [5]. The unique ID and sandbox assigned to each

application is a way to secure data. Different applications communicate with each other by exchanging some data. A sandbox is used for this purpose and sandbox is a built-in feature in Android architecture, However, there still exits system permissions that not only restrain an application from unauthorized access but sometimes if granted access could be harmful to the users' data.

For this very reason, the system permissions are classified into four categories i.e. Normal dangerous, signature and signature or System. In the Android operating system, every application has a separate space for its data protection. This separate space can be said as a Sandbox. Every application has its own sandbox. If any app needs to communicate with the other such as update features, private data and information are stored in smartphones as well making them more vulnerable to malicious attacks by various applications. With the immense use of smartphones, a variety of complexities, susceptibilities, and attacks have been noticed. It determines different inadequacies in the security mechanism of the Android operating system. It has become a point of awareness at the universal level because smartphones have been used everywhere. Privacy protection over data is a very important issue that needs to be raised now. Every software that has developed and all the applications have security measures designed by developers. Each smartphone that comes in the market also has built-in security features that support security but many frail facts also been noticed [6].

The research highlights how the security issue might lead to many problems such as leakage of personal information and data, passwords, financial loss, personal images and pictures and much more [7]. The research highlights the threats of current Android apps that have been downloaded in smartphones that might be virus infected. The virus might be any type like Trojan horse, spyware, gunpowder, etc. [8]. One of the ways to determine whether the app is malicious or not is noticing the permissions. A series of studies have been showed and presented related to the permissions that an app might request. Another way of a welcoming virus is Third-party applications. Though they provide a lot of safe and protected applications, there are still some risks to data privacy [9]. Cryptography can be the solution to currently prevailing security issues [10].

It is one of the most secure and extensively used techniques for the specified purpose. The article focuses on the alteration of these cryptography techniques as Android smartphones use Bouncy Castle package within the OS to perform the cryptography tasks. However, it supports a lot of algorithms for the purpose [11]. Moreover, this research represents the use of quantum computing attributes which is a domain using photonics to communicate via different protocols [12]. This computing technology provides a security feature free from all the threats and much stronger than the recently used protection techniques in ubiquitous computing. As encryption of data in any device coats the confidential and personal data with higher protection level and security so that data should be saved from attacks. Quantum Key distribution method is a cryptography technique that uses special properties to exchange important and secret information. A secure key is used which can be said as the cryptographic key that encrypts the data [13]. The data that is going to be communicated between concerned parties through some insecure way is encrypted through this key.

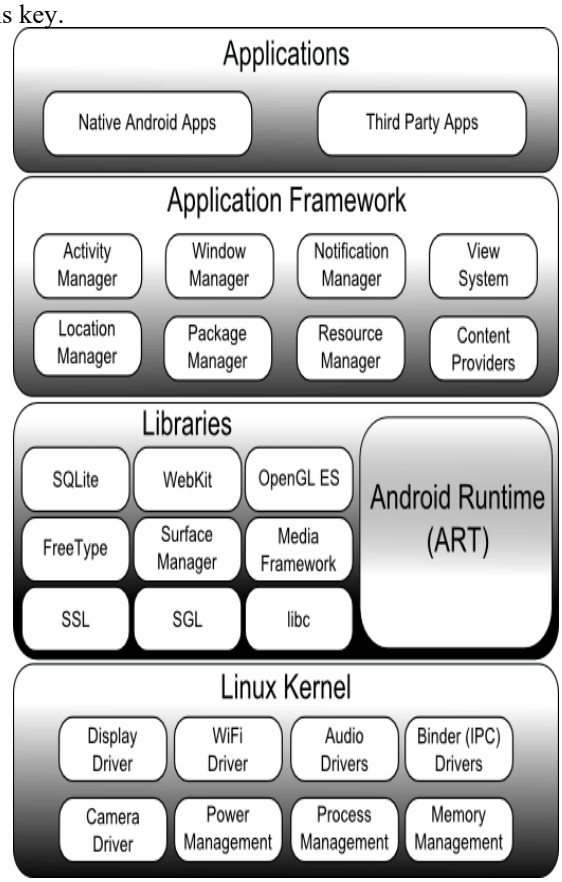

Figure 1. Current Android Architecture

QKD resolves the cryptography challenges being currently faced as shown in Figure 2 [14]. It is based on Heisenberg's uncertainty principle and photon polarization [15]. It reduces the risk of the data being stolen or intruded via another party or person. It's a new technology for the establishment of a connection between the sender and the receiver. It is based on photon polarization where one state that via communicating and photon carrying any kind of information, the data cannot be cloned by any malicious attacked and nor do the position and movement of information can be exactly known by anyone. QKD can be implemented by applying protocols, such as the BB84 protocol, the six-state protocol, and the EPR protocol [16].

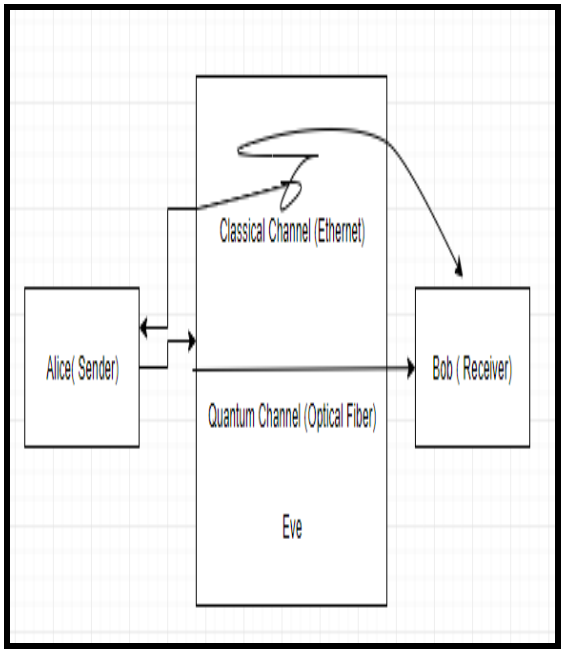

Figure 2. Working Mechanism of QKD

The next sections highlight the problem statement, literature review, the proposed solution of the existing problem i.e. the current Android cryptography algorithm and the proposed quantum-based algorithm.

2. Problem Statement

This segment illuminates the motivation for our research the problem observed in various smartphones and their optimized solution. The major drawback of the Android operating system is its security and third-party applications. It allows a malicious application to collaborate with other applications so as to access critical resources without requesting for corresponding permissions explicitly. Android operating system also uses application sandboxing which is used to limit application to access the resources. It an app needs to access the resources outside of its sandbox, it needs to request the appropriate permission. Being relied on existing encryptions can bring serious security threats. There have been a lot of malicious attacks when downloading and communicating with the third party. The hacker always tries to intrude and fetch some personal data and the user gives the personal data by clicking the ACCESS to the required permissions [17]. While browsing via mobile phones and communicating online via various social media platforms, there is a need to establish a connection between the source and destination. There is an exchange of keys and the formation of key pairs. This encryption is vulnerable to attacks and hacking. Various cybercrimes have gained rise due to these kinds of security threats. There are many proposed solutions to the problem, but our research provides an optimized solution based on the future to get the best desired results.

This problem can be overwhelmed by quantum cryptography. We scrutinized various studies related to the current Android architecture and saw the loopholes in detail. Quantum cryptography need not be limited in Android architecture. During data exchange, there was a chance of data to be attacked by malicious attackers. Android lags behind iPhone architecture due to this shortfall of security. This research focuses on how to enhance security in a more hone manner. Quantum key distribution implements the Android to guard and use in the case of a run-time kernel compromise. That is, even with a fully compromised kernel, an attacker cannot read key material stored in Quantum key. Apps can explicitly request key to be stored in key master, i.e. to be hardware-bound, to be only accessible after user authentication and request attentional certificates to verify these key properties, allowing verification of compatibility in terms of rules.

3. Literature Review

There has been a sheer increase in the number of malicious apps with an increase in the sale of smartphones. Youngho Kim and Tie Oh highlighted the issue of privacy leaks through mobile apps and proposed a methodology that is helpful in the understanding of the internal functions of mobile applications and used the Taint Droid-ported emulator for their experiments [18]. Maria Antonietta La Polla and Fabio Martinelli surveyed on threats and security solutions for mobile devices grouping the existing methods that protect the smartphones against different attacks. They focused on high-level attacks that are closely related to users such as user applications. They surveyed existing solutions for protecting mobile devices especially on IDS based tools [19]. IDS are signature-based models that look for some specific patterns for the detection of attacks. [20] analyzed the Android OS and its encryption by measuring different Android encryption systems in response to malicious attacks and presented a workflow. By emphasizing the importance of encryption they assessed different encryption systems that have been implemented in Android. The work they presented provides the placement of the Android platform and the practice of encryption systems.

[21] reviewed the Android operating system and presented her work on the diversity of Android OS and compared it with IOS and found that Android is much more flexible than IOS and Windows. She also reviewed why Android become popular all at once as it did not release one phone from one company but numerous numbers of phones throughout the year. The paper also presents a comparison of Android with iPhone and

Windows 7 users. [22]reviewed quantum computing and its importance and also compared quantum mechanics with the classical systems and presented why quantum is very fast as compared to the classical system. The paper also presented that quantum mechanics based on qubits instead of bits and use photons.

[23]researched on IO characteristics of two platforms. One is Android and the other is Tizen. He compared both of them and presented that Android is way better than Tizen in terms of storage, databases, and file systems by picking and analyzing seven different apps that were common in both the Android operating system and Tizen. The paper presented the results by comparison that the Android IO stack is classier than that of Tizen and also provided that the exact percentage of all write IO counts in the Android operating system and Tizen. [24] reviewed quantum key distribution and addressed the security standards. QKD based protocols have been discussed and analyzed. The paper focused on those issues that are cryptographically based and not on those problems that are physics-based. The QKD based protocols have been discussed in terms of the features that are rationality, extensiveness, and competence of security that have been achieved so far. It also presents a comparison between QKD proved security and symmetric key ciphers.

[25] researched on sensor-based authentication of smartphone users by proposing a new approach that is context-based authentication. The proposed methodology provides the exact results through simulations. This method validly differentiates the owner of the smartphone and other users with a 98.1% accuracy level [26]worked on the Android operating system and proposed an approach with the name of the box mate. This method secures Android users from dangerous apps by mining the sandbox. Sandbox keeps the applications in isolation. Each app's data kept separate from the other app. If any app needs some data from outside the application, then permissions are generated. [27]researched on the box mate proposal and found the limitations and gave a more comprehensive way of mining the sandbox by experiments.

4. Proposed Solution

Security and trustworthy problems that come along with Android operating systems can be reduced with quantum computing. Quantum key distribution (QKD) can be the solution to this problem because of its highly secure mechanism. Basically, in the QKD mechanism, a sender sends a series of single photons in two polarizations each. This polarization must be measured at the receiver side. If any spy or observer tries to measure the polarization of any photon released by laser, it would be destroyed and that's how the security feature is very high in quantum. It is like communication is between two parties that would the same numbers and the quantum key is the line between these numbers. This paper would represent a Quantum distribution key (QKD) based solution that will diminish the current security problems in Android. We would name the new operating system as Quantum based Android operating systems. Presently the Android OS uses public-key distributions. We propose a meager of the currently existing systems with quantum attributes using QKD as a technique for data protection and security. As many researchers suggest that quantum computing is the future in Android computing, and it is now veracity. Also, QKD ensures that nobody annealed with the numbers and secures the data with some strange rules. Various studies when scrutinized and with experiments being done, concluded that it was the access of permissions by third-party applications which created hindrances in the path to security. This research, therefore, proposed a unique mechanism shown in Figure 3 to curb the prevailing security threats by the use of Quantum attributes being used within the Android operating system [28]. The research provides a way to embed the QKD attributes on the third-party application layer of Android. The access to permission will be now by QKD instead of conventional access in the smartphone architecture.

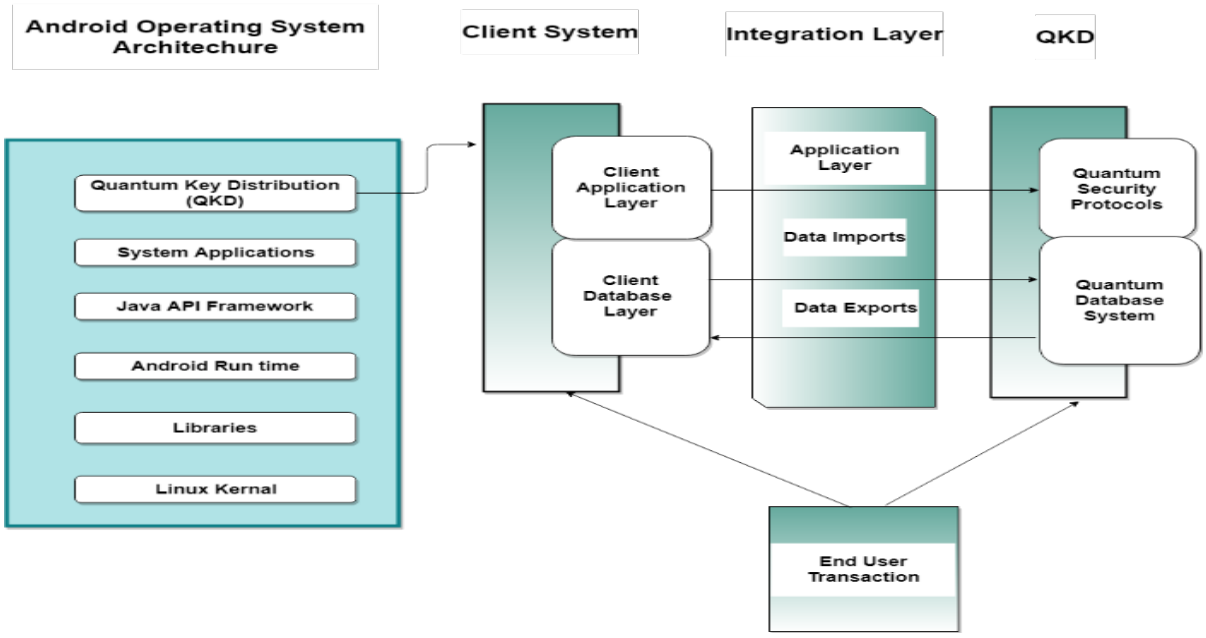

Figure 3. Proposed Architecture of the Android System.

As the user demands its data, QKD will establish communication using the BB84 protocol and do the encryption. Here, now Alice will act as the Client i.e. Android user who desired to send an information to the system, the QKD using Advanced Encryption Algorithm 256 as shown in Figure 4 will translate the sent message and form a cipher key via key combiner and sent it to the BOB i.e. the receiver of the data (either server or any third-party application) [29]. This can be done when an additional integrated layer that connects the Quantum and Client replaces the third-party Application layer. It is proposed that as the user access data a connection is established between the client and the Quantum Key Distribution mechanism. The BOB will get its accurate data only when the intruder has not played its cards on the sent information. If there is malicious activity, the end-user transaction would show a pop message that data is at the risk of being stolen and end the transaction. The Quantum database would allow as many transactions and as many cache data to be stored over it. However, in order to import or export data, the client must interact with QKD.

The third-party applications are replaced by the quantum key distribution. The client's application layer integrates with quantum-based security protocols and a quantum database integrates with the client's database layer. While end-user transactions would integrate with both of the client and the quantum-based protocols and database as shown in Figure 5 [30].

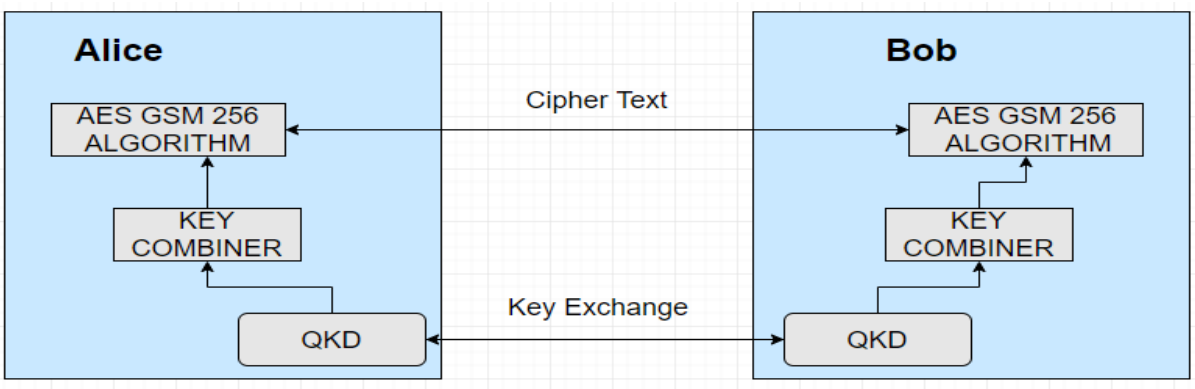

Figure 4. Communication Mechanism in Encryption Algorithm

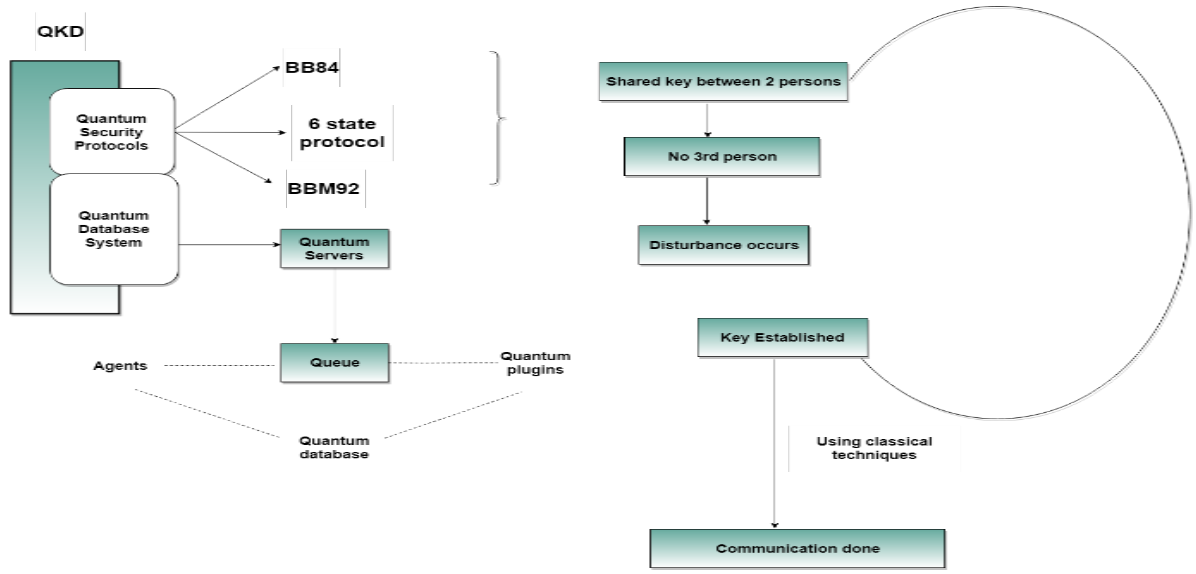

Figure 4. Extension of the Proposed Scheme

5. Simulations of BB84 Protocol using QUVIS

Like all other key distribution mechanisms, QKD also provides various protocols for communication, amongst which the popular is BB84 protocol. Quantum mechanics when ensuring secure communication by using the property that taking a measurement would not allow the communication or create a problem until both the sender and the receiver get appropriate data and establish a connection. After the creation of the key, Android user i.e. (Alice) the sender of the information and the receiver of the requested information i.e. Bob, in this case, could detect the presence of malicious attack i.e. eavesdropper when a transaction ends without being completed. This is the proposed scheme of the research. We used QUVIS software to check and validate this to be true or not. Four kinds of scenarios are taken into consideration using polarized photons. For BB84 protocol, when there is no malicious attack by the third party the key generated by AES 256 encryption is in time received on the destination i.e. via online interactions or emailing or web browsing as shown in Figure 6. However, as there occurs an attack in the Android architecture by any third party to misuse private information e.g. card numbers or account passwords, the transaction would immediately stop as depicted in Figure 7.

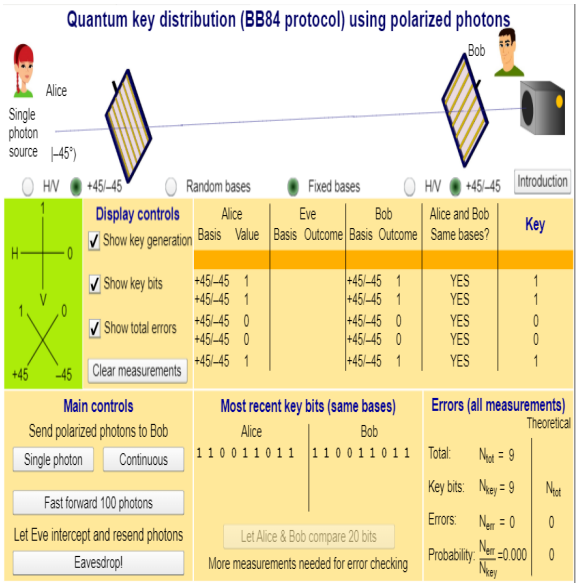

Figure 5. Simulations without Intruder

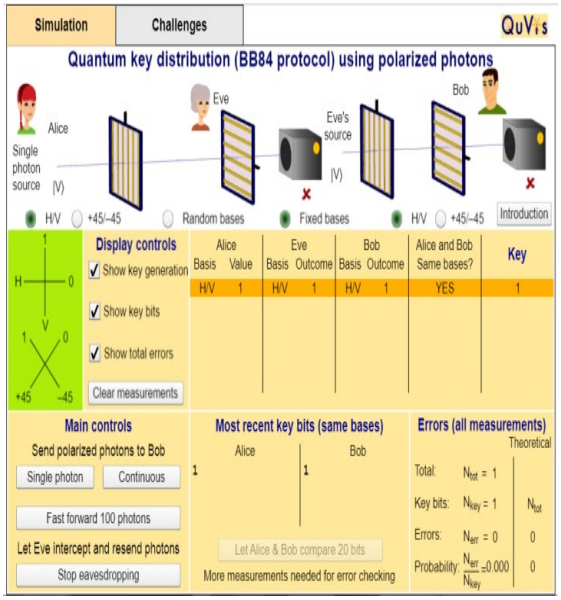

Figure 7. Simulations with Malicious Attack

6. Conclusion

As the use of Android increases, its vulnerability to data leakage also increases. The study reveals a proposed framework to counter the security issue of Android by increasing its architectural complexity i.e. embedding an attribute of Quantum solution if implemented so far. Thus, Quantum Key Distribution (QKD) is a secure method of communication that implements a cryptographic protocol and enhances the security of the system. The proposed model is a merger of Android and Quantum computing. BB84 Protocol can provide better security management. This solution in the future could potentially be used to eliminate the security issues in the Android operating system for better performance. This may include branding, software-enforced usage limitations (e.g., prohibition of tethered network access) or even special hardware features. Finally, a system image has to be generated and distributed over the air to customer devices for installation. Erroneous installation images may immediately render customer devices unusable. These limitations make attacks on the underlying operating system from Android apps nearly impossible.

References

[1] S. Narain and G. Noubir, "Mitigating Location Privacy Attacks on Mobile Devices using Dynamic App Sandboxing," *Proceedings on Privacy Enhancing Technologies,* vol. 2, pp. 66-87, 2019.

[2] M. Ahvanooey, Q. Li, M. Rabbani and A. Raza, "A survey on smartphones Security: Software Vulnerabilities, Malware and Attacks," *IJACSA,* vol. 8, no. 10, pp. 215-225, 2020.

[3] S. Ali, "New System of Encryption of User Data in Android 5.0," DZone, Lahore,Pakistan, 2019.

[4] F. Umer, "Android Operating System Architecture," *Research Gate,* pp. 1-6, 2019.

[5] S. Karthick and S. Binu, "Androiid Security issue and solutions," in *International Conferrence on Innovative Mechanisms for Industry Applications*, 2017.

[6] J. Shu, X. Jia, K. Yang and H. Wang, "Privacy-Preserving Task Recommendation Services for Crowdsourcing," in *IEEE Transactions on Services Computing*, Singapore, 2018.

[7] S. Yadav, "Android vulnerabilities and security," in *International Conference on Computing and Communication Technologies for Smart Nation*, 2017.

[8] A. Rawal, G. Chhikara, G. Kaur and H. Khanna, "Cryptography Algorithm," *Journal of Analog and Digital Communications,* vol. 4, no. 1, pp. 31-38, 2019.

[9] M. Kim, M. Lee and Y. Won, "IO chaaracteristics of modern smartphone platform: Android vs. Tizen," in *International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2015.

[10] D. Mewada, N. Dave and R. Prajapati, "A survey: Prospects of Internet of Things (IoT) using Cryptography Based on its Subsequent Challenges," *Australian Journal of Wireless Technologies, Mobility and Security,* vol. 1, no. 1, pp. 28-30, 2019.

[11] W. Lee and R. Lee, "Sensor-based implicit authentication of smartphone users," in *47th Annual IFIP International Conference on Dependable Systems and Networks*, 2017.

[12] J. Singh and M. Singh, "Evolution in quantum computing," in *International Conference on System Modeling & Advancement in Research Trends (SMART)*, 2016.

[13] T. Lee, "Towards mining comprehensive android sandboxes," in *23rd International Conference on Engineering of Complex Computing System (ICECCS)*, 2018.

[14] T. Zhou, J. Shen, X. Li, C. Wang and J. Shen, "Quantum Cryptography for the Future Internet and the Security Analysis," *Cyberspace Security for Future Internet-Hindawi,* pp. 1-7, 2018.

[15] M. Niemiec, "Quantum-based solutions for the Next-generation Internet," *Information & Security,* vol. 43, pp. 21-33, 2019.

[16] H. Wang, W. Yongzhi, T. Taleb and X. Jiang, "Editorial: Special issue on Security and privacy in network computing," *World Wide Web, Springer,* vol. 23, pp. 951-957, 2020.

[17] S. Pooja, P. Tiwari and S. Santosh, "Analysis of Malicious Behavior of Android Apps," *Procedia Computer Science-Elsevier,* vol. 79, pp. 215-220, 2016.

[18] M. Carsten, "Security and Privacy in the Internet of things," *Journal of Cyber Policy,* vol. 2, no. 2, pp. 155-184, 2017.

[19] R. Bitton, K. Boymgold and S. Asaf, "Evaluating the Information Security Awareness of Smartphone users," in *CHI Conference on Human Factors in Computing Systems*, 2020.

[20] T. Kimberly, F. Ali, N. Anuar and L. Cavallaro, "The Evolution of Android Malware and Android Analysis Techniques," *ACM Computing Surveys,* vol. 49, no. 4, pp. 1-41, 2017.

[21] B. Kirthika, S. Prabhu and S. Visalakshi, "Aandroid Operating System: A review," *International Journal of Trend in Research and Development,* vol. 2, no. 5, pp. 2394-9333, 2015.

[22] P. Madhu and S. Dixit, "Review on QuantumComputing," in *Second International Conference on Computer Networks and Communication Technologies (ICCNCT)*, India, 2019.

[23] G. Lee, M. Kim, K. Koroki, A. Ishimoto, ShinnsukeH and L. Seiji, "Wireless IC Tag Based Monitoring System for Individual Pigs in Pig Farm," in *Life and Technology*, Osaka, Japan, 2018.

[24] P. Horace, "Security of Quantum Key Distribution," *IEEE Access,* vol. 4, pp. 724-749, 2016.

[25] L. Wei-Han and L. Ruby, "Implicit Sensor-based Authentication of Smartphone Users with Smartwatch," *ACM Digital Library,* pp. 1-8, 2016.

[26] T. Lee, L. Bao, L. David, D. Gao and L. Li, "Towards Mining Comprehensive Android Sandboxes," in *23rd International Conference on Engineering of Complex Computer Systems (ICECCS)*, Melbourne, VIC, Australia, 2018.

[27] B. Tien-Duy and L. David, "Deep Specification Mining," in *27th ACM SIGSOFT International Symposiumon Software Testing*, New York,USA, 2018.

[28] S. Saroj, A. Sharma and S. Chuhan, "A Novel CPU Scheduling with Variable Time Quantum based on Mean Difference of Burst Time," *Research Gate,* pp. 1-6, 2016.

[29] S. Rajesh, V. Paul, M. Varun and R. Khosravi, "A Secure and Efficient Lightweight Symmetric," *MDPI,* vol. 11, no. 293, pp. 1-21, 2019.

[30] A. Nurhadi and N. Syambas, "Quantum Key Distribution (QKD) Protocols: A Survey," in *2018 4th International Conference on Wireless and Telematics (ICWT)*, Indonesia, 2018.