EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Security in Mobile Network: Issues, Challenges, Solutions

Ruby Dahiya[1], Anjali Kashyap[1], Bhupendra Sharma[1], Rahul Kumar Sharma[1], Nidhi Agarwal[1,*]

[1]School of SCSE, Galgotias University, Greater Noida, UP, India

Abstract

INTRODUCTION: Mobile devices are integrated into daily activities of people's life. Compared to desktop computers the growth of mobile devices is tremendous in recent years. The growth of mobile devices opens vast scope for attackers on these devices.
OBJECTIVES: This paper presents a deep study of different types of security risks involved in mobile devices and mobile applications.
METHODS: In this paper we study various mechanisms of security risks for the mobile devices and their applications. We also study how to prevent these security risks in mobile devices.
RESULTS: Various solutions are provided in paper through which operators can protect the security and privacy of user data and keep their customers' trust by implementing these procedures.
CONCLUSION: This paper concludes with their solutions for providing a secure mobile network. This paper is structured as follows. Section 2 contains related work. Section 3 describes security problems. Section 4 discusses defensive methods and Section 5 gives the conclusion.

Keywords: mobile attacks, mobile security, data privacy, mobile applications, malware attacks

Received on 20 September 2023, accepted on 25 November 2023, published on 06 December 2023

doi: 10.4108/eetiot.4542

*Corresponding author. Email: nidhiagarwal82@gmail.com

1. Introduction

Secure computing systems must be secure in order to protect sensitive information and resources against unauthorized access, theft, and damage. Network security has become a major priority for organizations of all sizes and industries due to the proliferation of networked devices and the growing reliance on digital communication and storage. Cyberthreats including malware, phishing, ransomware, and hacking have advanced and proliferated recently, posing serious dangers to the availability, confidentiality, and integrity of information assets. In order to protect networks from potential attacks, it is crucial to implement network security features including firewalls, encryption, access controls, IDS/IPS, and security policies.

In order to provide a thorough overview of this crucial area, this research study attempts to analyze the numerous facets of network security, including its significance, difficulties, best practices, and new trends. Modern communication systems have evolved to include mobile networks as a necessary component, allowing users to access information and stay connected while on the go. Mobile networks have developed from basic voice and text services to complex platforms that support multimedia content, social media, e-commerce, and other applications as a result of the growing use of smartphones and other mobile devices.

The privacy, confidentiality, and integrity of user data are threatened by many security issues that arise as mobile networks become more intricate and linked. The protection of mobile devices, applications, and networks from threats such as malware, phishing, man-in-the-middle attacks, and unauthorized access is referred to as mobile network security. This study intends to investigate the numerous facets of mobile network security, including its significance, difficulties, recommended practices, and developing technologies.

We now enjoy the convenience of remaining connected while on the road thanks to mobile networks, which have

revolutionized the way we communicate and access information. Mobile networks have become a crucial component of our daily lives as smartphones and other mobile devices have grown in popularity. The privacy, confidentiality, and integrity of user data are threatened by many security issues that arise as mobile networks become more intricate and linked. To defend against these dangers and guarantee the safe and secure usage of mobile devices and networks, mobile network security is essential. The goal of this research study is to give readers a thorough grasp of mobile network security, including its significance, difficulties, recommended procedures, and new developments.

2. Literature Review

Khana et al.[1] explored various security challenges faced by mobile users, including threats such as physical-based, network-based, and web-based. Of all the mobile vulnerabilities, botnets were found to be particularly significant. To mitigate these risks and ensure data privacy and mobile security. The authors suggested implementing biometric authentication as a critical security defence mechanism. They also emphasized the importance of integrating security mechanisms at every stage of mobile application development. In summary, Khana et al's study highlight the need for a comprehensive approach to mobile security, from development to deployment, to protect against the various types of mobile threats.

Shukla et al.[2] developed a novel key agreement and authentication protocol specifically for Electronic Health Record(HER) systems, which involve multiple types of users such as doctors, lab staff, patients, and insurance agencies, Authentication and proper key agreements are crucial for ensuring secure and reliable communication in such systems. The proposed protocol employs a commitment scheme that halts communication in case of authentication failure, making it highly effective in preventing Man-in-the-Middle attacks in wireless communications, Furthermore, the binding and hiding nature of the protocol adds an extra layer of security making it suitable for HER systems where data confidentiality and integrity are of utmost importance. Overall, the study highlights the significance of robust authentication and key agreement protocols for securing sensitive information in HER systems.

Cifuentes et al.[3] conducted an analysis of the vulnerabilities present in mobile health applications. They categorized such apps into six groups based on their functionalities and downloaded ten Android apps from the Google Play Store for each group, resulting in a total of 60 apps for analysis. Their findings revealed a total of 157 vulnerabilities with the highest number of vulnerabilities found in apps with remote monitoring functionalities which also had a high-risk level. They also noted that untrusted input was the primary cause of 64% of the vulnerabilities in mobile health apps. The study highlights the need for developers to implement robust security measures to prevent the exploitation of such vulnerabilities in Health apps.

Chatzikonstantinou et al.[4] identified and classified types of cryptographic weaknesses in mobile applications including weak cryptographic algorithms, keys, implementation, and parameters. To investigate the prevalence of such weakness, the authors manually analyzed 49 randomly selected Android apps downloaded from the Google paly store using static and dynamic analysis. Their findings showed that a vast majority of Android apps, almost 87.8%, employed weak cryptographic algorithms, while 12.2% of the apps did not implement any cryptographic algorithm at all. The study highlights the urgent need for mobile app developers to implement robust cryptographic techniques to ensure the secure storage and transmission of sensitive data, including passwords, payment information, and personal data.Ghosh et al. (2023) embarked on a comprehensive study to assess water quality through predictive machine learning. Their research underscored the potential of machine learning models in effectively assessing and classifying water quality. The dataset used for this purpose included parameters like pH, dissolved oxygen, BOD, and TDS. Among the various models they employed, the Random Forest model emerged as the most accurate, achieving a commendable accuracy rate of 78.96%. In contrast, the SVM model lagged behind, registering the lowest accuracy of 68.29%[16].

Alenezi et al. (2021) developed a novel Convolutional Neural Network (CNN) integrated with a block-greedy algorithm to enhance underwater image dehazing. The method addresses color channel attenuation and optimizes local and global pixel values. By employing a unique Markov random field, the approach refines image edges. Performance evaluations, using metrics like UCIQE and UIQM, demonstrated the superiority of this method over existing techniques, resulting in sharper, clearer, and more colorful underwater images [17].

Sharma et al. (2020) presented a comprehensive study on the impact of COVID-19 on global financial indicators, emphasizing its swift and significant disruption. The research highlighted the massive economic downturn, with global markets losing over US $6 trillion in a week in February 2020. Their multivariate analysis provided insights into the influence of containment policies on various financial metrics. The study underscores the profound effects of the pandemic on economic activities and the potential of using advanced algorithms for detection and analysis [18].

3. Issues and Challenges

1. Data breaches: Due to their portability, small size, and ease of loss or theft, mobile devices are susceptible to data breaches. This makes it simpler for hackers to obtain private data, including passwords, credit card information, and personal information.

2. Malware attacks: Because they may infect devices and spread quickly throughout the network, malware poses a serious threat to mobile networks. Malware can control equipment, spy on users, and steal data.
3. Network congestion: As more people use mobile devices, there is a rise in the demand for network capacity, which causes congestion. This may lead to reduced network speeds, missed calls, and subpar service quality.
4. Lack of standardization: Because mobile network security protocols are not standardized, it is challenging for developers to create secure applications and for consumers to determine which applications are secure to use.
5. User behaviour: Users frequently engage in dangerous behaviour that jeopardizes the security of their devices and the network, such as using weak passwords or downloading software from dubious sources.
6. Emerging technologies: There are new security issues that need to be resolved as a result of the development of new technologies like 5G, IoT, and AI.
7. Regulatory compliance: To guarantee the security and privacy of user data, mobile networks are required to adhere to many regulations and standards. Penalties for noncompliance include both monetary and legal consequences.
8. Insider threats: Employees can purposefully or inadvertently damage the security of the network, which presents a serious risk to mobile network security.
9. Lack of knowledge: Users are more susceptible to assaults because they are not aware of the security dangers posed by mobile devices and networks.
10. Cost: It can be expensive to implement effective mobile network security solutions, making it difficult for businesses to put security before money.

4. Solutions

1. Encryption: Encryption should be used by mobile networks to safeguard data both in transit and at rest. This can shield user data from unauthorized access and guarantee its security and integrity.
2. Multi-factor authentication: To prevent unauthorized access, mobile devices should use multi-factor authentication. This may entail employing biometric authentication in addition to a password, such as fingerprint or facial recognition.
3. Network segmentation: To reduce the impact of a compromise, mobile networks should split their networks. This may limit an attacker's ability to access sensitive information or important systems.
4. Regular updates and patches: The most recent security patches and fixes should be regularly applied to mobile devices and applications. This can fix known issues and lower the chance of exploitation.
5. User education: Mobile network service providers should inform users of the value of mobile network security and offer advice on safety procedures. This can include pointers on how to make secure passwords, steer clear of dubious links and downloads, and report unethical behaviour.
6.Standardisation: To maintain compatibility and interoperability between hardware and software, mobile network providers should cooperate to create standardized security protocols.
7. Compliance: To safeguard the security and privacy of user data, mobile network operators shall adhere to all applicable laws and standards. This may entail abiding by HIPAA, the GDPR, or other data protection rules.
8. Monitoring and detection: Mobile networks should use monitoring and detection capabilities to spot security threats in real time and take appropriate action.
9. Incident response strategy: To respond swiftly to security breaches and lessen the impact on users and the network, mobile network providers should have an incident response strategy in place.
10. Investment: To safeguard their networks and users, mobile network providers need to make significant security investments. This may entail working with outside security companies, employing specialized security staff, or putting in place cutting-edge security technologies.2. Literature Review
Khana et al. [1] explored various security challenges faced by mobile users, including threats such as physical-based.

5. Conclusion

In conclusion, the security of mobile networks is a crucial component of contemporary communication technology. The risk of security breaches and data theft rises as mobile devices and networks become more widely used. Mobile network providers must therefore put in place a thorough security strategy that includes encryption, multi-factor authentication, network segmentation, regular updates and patches, user education, standardization, compliance, monitoring and detection, incident response planning, and investment in security measures. Mobile network operators can protect the security and privacy of user data and keep their customers' trust by implementing these procedures.

References

[1] Khan, J., Abbas, H., & Al-Muhtadi, J. (2015). Survey on Mobile User's Data Privacy Threats and Defense Mechanisms. Procedia Computer Science, 56, 376- 383.
[2] Shukla, V., Chaturvedi, A., & Srivastava, N. (2015). A new secure authenticated key agreement scheme for wireless (mobile) communication in an EHR system using cryptography. Communication on applied electronics (CAE), 3(3), 16-21
[3] Cifuentes, Y., Beltrán, L., & Ramírez, L. (2015, August). Analysis of Security Vulnerabilities for Mobile Health Applications. In 2015 Seventh International Conference on Mobile Computing and Networking (ICMCN 2015).
[4] Chatzikonstantinou, A., Ntantogian, C., Karopoulos, G., & Xenakis, C. (2016, May). Evaluation of Cryptography Usage in Android Applications. In proceedings of the 9th

EAI International Conference on Bio-inspired Information and Communications Technologies, pp. 83-90.
[5] Flauzac, O.; Nolot, F.; Rabat, C.; Steffenel, L.-A., "Grid of Security: A New Approach of the Network Security", In Proc. of Int. Conf. on Network and System Security, 2009. NSS '09, pp. 67-72, 2009.
[6] Wu Kehe; Zhang Tong; Li Wei; Ma Gang, "Security Model Based on Network Business Security", In Proc. of Int. Conf. on Computer Technology and Development, 2009. ICCTD '09, Vol. 1, pp. 577-580, 2009.
[7] Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously," Computer, vol.31, no.9, pp.24?28, Sep 1998
[8] Kartalopoulos, S. V., "Differentiating Data Security and Network Security," Communications, 2008. ICC '08. IEEE International Conference on, pp.1469?1473, 19?23 May 2008
[9] P. Vinod, R. Jaipur, V. Laxmi, and M. Gaur, "Survey on malware detection methods," in Proceedings of the 3rd Hackers' Workshop on the computer and internet security (IITKHACK'09), 2009, pp. 74-79.
[10] Voor, H.G., Klievink, A.J., Arnaboldi, M., Meijerc, A.J. ?Rationality and politics of algorithms. Will the promise of big data survive the dynamics of public decision making?, Government Information Quarterly, 2019, Vol. 36(1), pp. 27-38. DOI: 10.1016/j.giq.2018.10.011
[11] Agarwal N., Jain A., Gupta A., Tayal D.K. (2022) Applying XGBoost Machine Learning Model to Succor Astronomers Detect Exoplanets in Distant Galaxies. In: Dev A., Agrawal S.S., Sharma A. (eds) Artificial Intelligence and Speech Technology. AIST 2021. Communications in Computer and Information Science, vol 1546. Springer, Cham. https://doi.org/10.1007/978-3-030-95711-7_33
[12] Agarwal, N., Srivastava, R., Srivastava, P., Sandhu, J., Singh, Pratap P. Multiclass Classification of Different Glass Types using Random Forest Classifier. 6th International Conference on Intelligent Computing and Control Systems (ICICCS), 2022. p. 1682-1689.
[13] Agarwal, N., Singh, V., Singh, P. Semi-Supervised Learning with GANs for Melanoma Detection. 6th International Conference on Intelligent Computing and Control Systems (ICICCS), 2022. p. 141-147.
[14] Tayal, D.K., Agarwal, N., Jha, A., Deepakshi, Abrol, V. To Predict the Fire Outbreak in Australia using Historical Database. 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2022. p. 1-7.
[15] Agarwal, N., Tayal, D.K. FFT based ensembled model to predict ranks of higher educational institutions. Multimed Tools Appl 81, 2022.
[16] Ghosh, H., Tusher, M.A., Rahat, I.S., Khasim, S., Mohanty, S.N. (2023). Water Quality Assessment Through Predictive Machine Learning. In: Intelligent Computing and Networking. IC-ICN 2023. Lecture Notes in Networks and Systems, vol 699. Springer, Singapore. https://doi.org/10.1007/978-981-99-3177-4_6
[17] Alenezi, F.; Armghan, A.; Mohanty, S.N.; Jhaveri, R.H.; Tiwari, P. Block-Greedy and CNN Based Underwater Image Dehazing for Novel Depth Estimation and Optimal Ambient Light. Water 2021, 13, 3470. https://doi.org/10.3390/w13233470
[18] G. P. Rout and S. N. Mohanty, "A Hybrid Approach for Network Intrusion Detection," 2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, 2015, pp. 614-617, doi: 10.1109/CSNT.2015.76.