Systematic analysis of Research Trends, Methods and Datasets in Mobile Device Security

Dr.B. Prabhakar Reddy, P. Imran Khan, S. Mahaboob Basha

Professor[1], Assistant Professor[2,3]

[1]Bheema Institute of Technology and Sciences, Adoni-518301

[2,3] St.Johns College of Engineering and Technology, Yerrakota-518360

Article Info
Page Number: 12741-12751
Publication Issue:
Vol. 71 No. 4 (2022)

Article History
Article Received: 25 October 2022
Revised: 30 November 2022
Accepted: 15 December 2022

Abstract; The threats, necessities, and rules of security have all changed in the age of mobile devices. Academic and commercial attention has recently been drawn to the problem of authentication for mobile communications networks. It's becoming more popular to study mobile security. This work uses a method called a systematic review to assess, understand, and discover all relevant research resources that could help address the research topic at hand. This review was executed in three steps: (1) deciding on a data source and search string; (2) selecting relevant studies; and (3) summarizing the review's findings. Identifying malware and intrusions, cryptography, authentication, and data breaches are the four main areas of concentration in contemporary Mobile Device Security research. Artificial intelligence might be considered the most widely utilized and experienced of the four approaches. Sixty-six point one percent of studies used open data while thirty-nine point nine percent used proprietary data. This study's findings have implications for both theory and practice, and they may inform future investigations and system designs pertaining to mobile device safety..

Keywords: Mobile device security, systematic reviews, research methodologies, and data sets

1. Introduction

Each of the three tiers of the security architecture—transport, service, and application—as well as the four domains—user, access, network, and application domain—have their own unique security features. The new mobile device ecosystem brings with it new security threats, needs, and rules. Research into mobile security has become a research hotspot because to the growing concern among academics and businesses on the authentication of mobile communications networks (Wang & Fang, 2019). Some of them deal with studies on mobile health and mobile finance. There is a tight connection between these two factors and the value of safety.

The World Health Organization (WHO) defines mobile health, also known as mHealth, as "the use of mobile technologies to support health-related activities across the continuum of care, from prevention and promotion to diagnosis and treatment" (Trigo et al., 2020). Despite widespread consensus on the practicability and accessibility of fundamental telemonitoring m-health services, there are challenges to be overcome, most notably security and privacy concerns.

M-money (mobile money) is also changing the lives of the great majority of people in Sub-

Saharan Africa who do not have access to traditional banking services. The mobile money system (MMS) allows people in rural regions and with low incomes to access a variety of services at reduced rates. MMS has grown rapidly because of the many advantages it provides, including ease of use, reliability, rapidity, adaptability, and low cost. It lessens the need for people to worry about their own country's economy, eliminates certain security risks connected with handling cash, and shortens wait times at banks. The current two-factor authentication system (2FA) approach for electronic currency has been plagued by security concerns due to its popularity (Ali et al., 2020).

The research landscape in the area of mobile device security is fragmented due to the wide variety of available datasets and approaches. This evaluation attempts to describe and evaluate research tendencies, commonly used datasets, and approaches taken in the field of Mobile Device Security from 2017 through 2021.

2. Literature Review

Mobile devices in the form of smartphones, personal digital assistants, tablets, and other mobile gadgets have become increasingly common in people's daily lives for various reasons. This rapidly expanding field is changing people's lives and bringing various benefits such as time savings, the ability to work without being tied to a specific position, and increased productivity.

By using mobile devices, users can also utilize their gadgets to check their emails, tweets, or posts on Facebook. For example, video viewing on mobile devices surged to 40% in 2013 from 25% in 2012 and only 6% in 2011. There has been a significant increase in mobile YouTube traffic is more evidence that smartphones are becoming increasingly ubiquitous. The growth of Facebook's mobile user base has been meteoric. A whopping 73% of Facebook's total users were accessed through mobile devices in the second quarter of 2013, up from 56% in 2012 and 43% in 2011.

Besides passwords and credit card numbers, mobile phones may also store contact lists and other private data (Chan et al., 2016). The convenience of mobile banking stems from the fact that customers may access their accounts from any location, at any time, and from any device. Attackers are shifting their attention to mobile devices because they have the data they need and because security problems are not being adequately addressed on these devices (Alimardani & Nazeh, 2018; Jin et al., 2020; Vaghela, 2020).

Research on the usage of mobile devices has been conducted in numerous industries, including education, retail, advertising, and others in addition to M-health and M-money, which were discussed in the Introduction section. Byeon and Yu (2022) investigated the potential of mobile AR for facilitating distant teamwork. Then, Zou and Wang (2021) looked at how mobile devices are being used to convey stories in online video ads. When it comes to mobile payment services, Jin & Lim (2021) are the ones to look at. And the matter of safety is paramount in every one of them.

Research Method

We committed to doing a comprehensive literature review on Mobile Device Security. The practice of doing a Systematic Literature Review (SLR) has recently gained widespread popularity. Berguig and Abdelbaki (2021) and Dahiya et al. (2021) both agree that SLR is a reliable research technique. It's a strategy for assessing the quality of available resources and locating those most pertinent to answering a research question (Kitchenham & Charters, 2007). In this literature review, we used the 2007 work of Kitchenham and Charters as our starting point.

The three steps of SLR are shown in Fig. 1. In the first step, we establish why a systematic review is necessary. In the second phase, we assess the quality of the included and excluded studies, extract relevant data, and interpret our findings. The last step is a comprehensive report of the findings.

5.1 Question for Studying

The review process might be guided by the Research Question (RQ). Table 1 displays how the PICOC (Population, Intervention, Comparison, Outcomes, and Context) framework (Kitchenham & Charters, 2007) was utilized to shape the study question. The study's central question and stated objectives are presented in Table 2. The primary SLR mind map is shown in Figure 2.

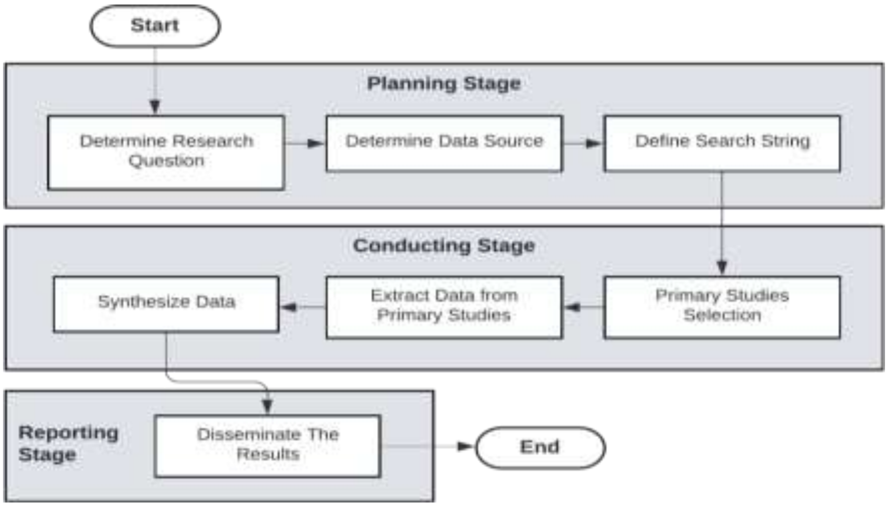


Fig. 1: The systematic literature review steps in this research

Table 1: The PICOC structure on this literature review

Population	Mobile device, smartphone
Intervention	Security, datasets, methods
Comparison	Null
Outcomes	Models/methods of mobile device security
Context	Small and big datasets, research in industry and academics

Table 2: The research question and aims on this literature review

ID	Research Question	Aim
RQ1	What research topics do mobile device security researchers choose?	Identify research topics and trends in mobile device security
RQ2	What kind of datasets are the most used for mobile device security research?	Identify datasets commonly used in mobile device security research
RQ3	What kind of methods are used in mobile device security research?	Identify opportunities and trends for mobile device security method

2.1. Search strategy

In this phase, you will design a search strategy and choose digital library resources. As part of this process, you will develop and refine a search term and compile a preliminary set of chosen research from digital sources that correspond to the search phrase. Some of the most popular sources of relevant past research include

choose to get the most extensive study sample possible. In addition to the ACM Digital Library (dl.acm.org), we also utilize Springer (link.springer.com), ScienceDirect (sciencedirect.com), MDPI (mdpi.com), and ScienceDirect.

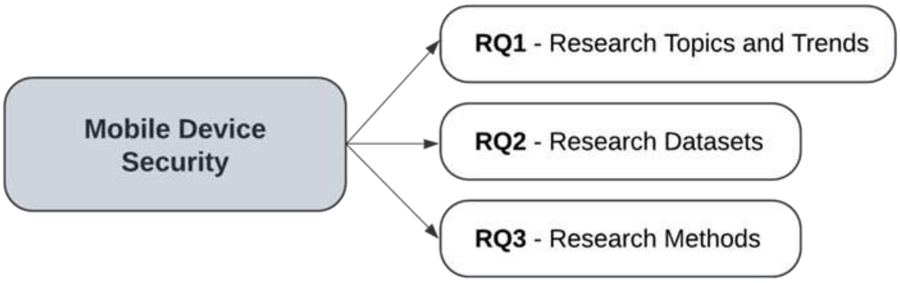


Fig. 2: The SLR's core mind map on mobile device security

The procedures below were accustomed to defining search phrase (search string):

1. PICOC search terms, particular intervention and population, were identified.
2. Using research questions to choose search keywords.
3. Search phrases that are found in related keywords, titles and abstracts.
4. Synonyms, alternate spellings, and antonyms of search phrases are defined.
5. Create a thorough search phrase using specified words, boolean ORs, and ANDs.

The following query was used at the end:

Security and mobile devices, but not the Internet of Things

The search phrase is modified to fit each database's unique requirements. Keyword, title, and abstract searches were performed on all databases. Publication dates between 2017 and 2021 were used to refine the search. Then, we exclude everything except peer-reviewed journal papers and proceedings from conferences. Only studies that appeared in English-language journals were evaluated.

Choose Your Studies Wisely

The inclusion and exclusion criteria were used to select the primary studies. The criteria for inclusion and exclusion are listed in Table 3.

Table 3: The exclusion and inclusion criteria

Inclusion Criteria	Exclusion Criteria
The research is published in between 2017 and 2021. Journal articles or conference proceedings For duplicate publications, just the most recent ones will be listed.	Research that is not written in English. Research without strong validation.

The process of study selection was carried out in two parts, as shown in Fig. 3: primary studies were excluded based on keywords, title, abstract, and then the entire text. Studies that do not provide the experiment's outcome are excluded from the review. The research is read thoroughly and be included in the next step if has a high degree of resemblance with the security of the mobile devices.

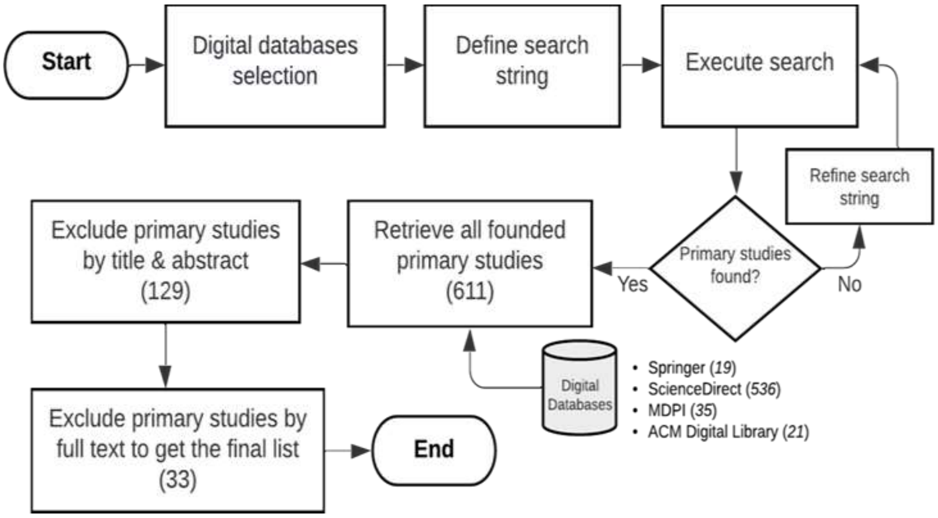

Start
Digital databases selection
Define search string
Execute search
Refine search string
Primary studies found?
Yes
No
Retrieve all founded primary studies (611)
Exclude primary studies by title & abstract (129)
Exclude primary studies by full text to get the final list (33)
End
Digital Databases
• Springer (19)
• ScienceDirect (536)
• MDPI (35)
• ACM Digital Library (21)

Fig. 3: The process of finding and selecting primary studies on literature review

2.2. Data extraction

To address the research question, data from chosen primary studies are gathered. A form of data extraction was filled out for all of the 33 selected research. It was made to gather data from the selected research required to address the research question (see Table 4).

Table 4: Properties of data extraction linked to research question

Substance	Research question
Research topics or trends on mobile device security Mobile Device security datasets Mobile Device security methods	RQ1 RQ2 RQ3

3. Result and Discussion

3.1. Research trends

There are 33 original research here that address the topic of mobile device safety. Figure 4 is a graph showing how people have been more concerned about mobile device security over time. There has been an increase in the number of studies published after 2018, indicating that they are more up-to-date research. Figure 4 further shows how important it is to study mobile device security.

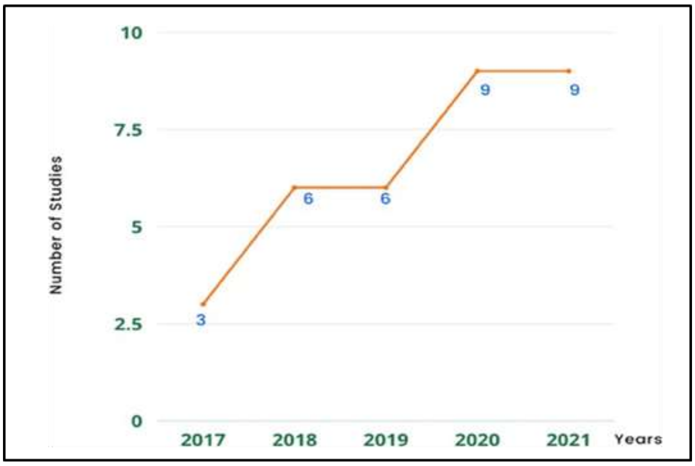


Fig. 4: The allocation of chosen research throughout the years

3.2. Research topics and methods used in mobile device security

We analyzed their contents and came to the conclusion that the majority of recent studies on mobile device security concentrate on four main areas and related methodologies:

1. Malware and Intrusion Detection: This work makes use of the service monitor approach (Salehi et al., 2019), machine classification with analysis tools and algorithms (Zhang et al., 2019), machine learning, neural networks, and deep learning (Fournier et al., 2020, D'Angelo et al., 2020, Millar et al., 2017, Jensen et al., 2017), IRS metric (Dey

Second, cryptography is utilized, including lightweight cryptography techniques (Shahbodin et al., 2019), openkeychain (Schürmann et al., 2017), location-based cryptography (AES + location coordinate) (Mondal & Bours., 2018), and RSA and ECC cryptographic swarm optimization simplified (Mullai & Mani., 2020).

Token-based authentication framework (Niewolski et al., 2021) and proposed D2D security (Edris et al., 2021). Gait-based authentication (Zeng et al., 2021, Axente et al., 2020). Lightweight deep learning model secure authentication (Zeroual et al., 2021).

Fourth, we have information invasion, also known as SonicEvasion (Pattani & Gautam, 2021), which is the use of sound to covertly transmit information.

Artificial intelligence might be considered the most widely utilized and experienced of the four approaches. One of the finest ways to automate the ever-evolving and ever-more-essential digital transition is with the help of artificial intelligence today.

Datasets used in mobile device security 6.3

A dataset serves a certain function. Training data is information fed into a machine learning system so that a model may be developed from the information. Data used to evaluate a model's learning mechanism is known as evaluation data. There are several data sets used for training and for testing purposes. According to a review process, contemporary Mobile Device Security research employs a variety of datasets, including: • Private datasets (Wang & Fang, 2019, Trigo et al, 2020, Ali et al, 2020, Shahbodin et al, 2019, Schürmann et al, 2017, Mullai & Mani, 2020, Niewolski et al, 2021, Edris et al, 2021, Pattani & Gautam, 2021, More- Gimeno et al, 2018, Guo et al, 2018, Yan et al, 2018).

• Malicious software from a variety of sources and families (Salehi et al., 2019; Zhan et al., 2019; Fournier et al., 2020; Millar et al., 2017; Deypir & Horri., 2018; Mathur et al., 2021; Bhandari et al., 2018; Hijawi et al., 2021).

• Minidump of malgenomes spread via contagion (D'Angelo et al., 2020).

• Mobile biometrics for the general public (Mondal & Bours, 2018).

(Axente et al., 2020) The UCI Machine Learning Repository.

(Zeroual et al., 2021) • ORL and extended yale.

Dataset APIs for Sparks (Lima et al., 2020).

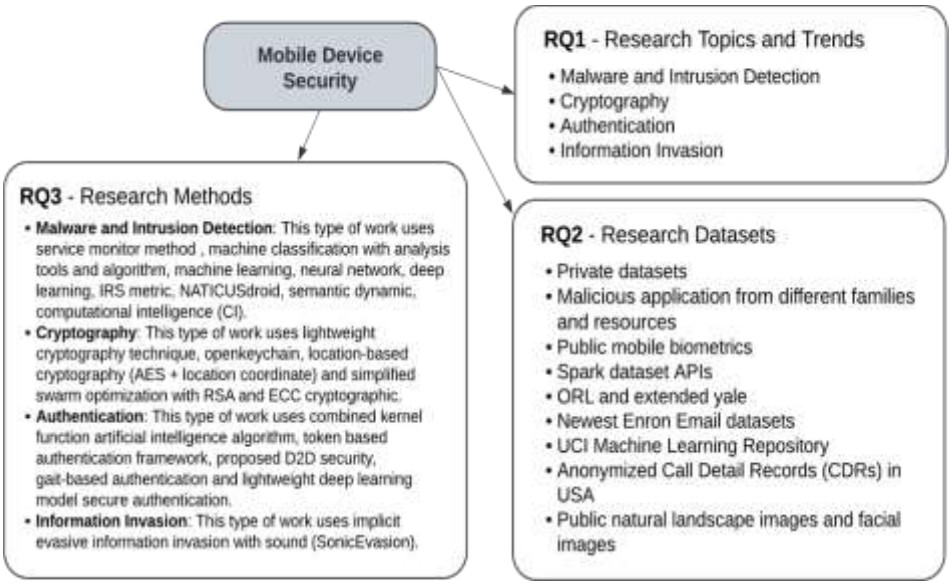
Email databases from Enron (Li et al., 2021).

• Telephony metadata (Forte et al., 2019).

Examples include pictures of landscapes and faces available to the public (Saharan et al., 2021).

According to the classification scheme shown above, public datasets are more often used than private ones. The results of this study provide encouraging evidence that they may be used by the general public or by other academics tackling the same or comparable issues or case studies.

The whole mind map shown in Fig. 5 that sums up the SLR's findings on mobile device security is shown there. As an additional problem-solving tool, mind maps were analyzed for linkages between ideas and components of a dispute. It provides a new perspective by helping us take into account the large picture with all the little details (Buzan & Griffiths, 2013). It also helps in storing information and learning something new.


Mobile Device Security
RQ1 - Research Topics and Trends
• Malware and Intrusion Detection
• Cryptography
• Authentication
• Information Invasion
RQ2 - Research Datasets
• Private datasets
• Malicious application from different families and resources
• Public mobile biometrics
• Spark dataset APIs
• ORL and extended yale
• Newest Enron Email datasets
• UCI Machine Learning Repository
• Anonymized Call Detail Records (CDRs) in USA
• Public natural landscape images and facial images
RQ3 - Research Methods

- **Malware and Intrusion Detection**: This type of work uses service monitor method , machine classification with analysis tools and algorithm, machine learning, neural network, deep learning, IRS metric, NATICUSdroid, semantic dynamic, computational intelligence (CI).
- **Cryptography**: This type of work uses lightweight cryptography technique, openkeychain, location-based cryptography (AES + location coordinate) and simplified swarm optimization with RSA and ECC cryptographic.
- **Authentication**: This type of work uses combined kernel function artificial intelligence algorithm, token based authentication framework, proposed D2D security, gait-based authentication and lightweight deep learning model secure authentication.
- **Information Invasion**: This type of work uses implicit evasive information invasion with sound (SonicEvasion).

Fig. 5: The complete mind map of the results of SLR on mobile device security

This SLR has contributed from the academic and practical sides. First, this SLR depicts the four main themes in Mobile Device Security research on the academic side. Those four themes can guide future Mobile Device Security researchers and scholars. Second, on the practical side, this SLR gives insight to the developer or practitioners in the field of mobile security about what methods can be considered in the development process, as well as about datasets that can be used.

4. Conclusion

The purpose of this SLR is to identify and assess the methodologies, datasets, and approaches used in Mobile Device Security studies between 2017 and 2021. Finally, 33 Mobile Device Security studies published between January 2017 and December 2021 were retained for analysis based on the exclusion and inclusion criteria. This analysis was performed methodically. A systematic literature review (SLR) is a method for gathering and analyzing all relevant data to answer a particular research issue. The findings point to four areas where attention is now being paid in the field of Mobile Device Security study: malware and intrusion detection; cryptography; authentication; and information invasion. Artificial intelligence might be considered the most widely utilized and experienced of the four approaches. Additionally, 60.61 % of research publications used publicly available datasets, whereas only 39.39 % used proprietary datasets.

References

1. (2020) Ali, G., Dida, M. A., and Sam, A. E. A survey of mobile money two-factor authentication threat models and mitigation strategies. Future Internet (MDPI), 12(160), 2012.

2. (2018a) Alimardani, H., and Nazeh, M. Recent mobile malware is categorized according to its characteristics, analytical approaches, and detection methods. Between pages 44 and 49 of the ICEMC 2018: International Conference Proceedings.
3. Dobre, C., Raluca, R.-l. C., Axente, M.-S., and Purtan, P. (2020). Mobile device authentication through gait analysis. 20(15):4110, MDPI Sensors.
4. To cite: Berguig, O., & Abdelbaki, N. (2021). A review of the research on the effect of work-life balance factors on employee intention to leave. 11(2), 134–254 in the Journal of System and Management Sciences.
5. The authors are S. Bhandari, R. Panihar, S. Naval, V. Laxmi, A. Zemmari, and M. S. Gaur. The SWORD malware scanner is smart and aware. Security and Applications in the Journal of Information 42:46-56.
6. Theodore Buzan & Carol Ann Griffiths (2013). The 2nd Edition of "Mind Maps for Business: How to Use the World's Most Powerful Thinking Tool to Transform the Way You Do Business" The Financial Times Press.
7. G. Byeon and S. Yu (2022). Method of making augmented reality content on a mobile device using remote workers. 12(1), 129-142 in the Journal of System and Management Sciences.
8. J. H. Chan and J. L. Hong (2016). The Value of Mobile Security. 89-106, http://dx.doi.org/10.14257/ijsia.2016.10.10.10, International Journal of Security and Its Applications, NADIA.
9. (2020) D'Angelo, G., M. Ficco, and F. Palmieri. Autoencoder and API-image based mobile malware detection. Article 137, pages 26-33, Journal of Parallel and Distributed Computing.
10. Authors: Dahiya, A., N. Gautam, and P. K. Gautam (2021). Online consumer feedback analysis using data mining techniques: a literature review. Science of Systems and Management, 11(3), pp. 1-26.
11. (2020) Deebak, B. D., F. Al-Turjman, & L. Mostarda. Cloud-based mobile edge computing with seamless, anonymous authentication. IEEE Transactions on Computers, 87(10):106782.
12. M. Deypir and A. Horri. 2018. Estimating the worth of security risks for Android apps based on their use cases. Security and Applications in the Journal of Information Technology, 40, 20-30.
13. Reference: Edris, E. K. K., M. Aiash, and J. Loo (2021). 5G device-to-device communications: utilizing proverif for formal verification of authentication and service authorisation protocols. 10(13), 1608 MDPI Electronics.
14. (2019) Forte, A. G., Wang, W., Veltri, L., & Ferrari, G. A design for the backbone of mobile networks for the future generation. 152. MDPI Future Internet.

A. Fournier, F. E. Khoury, and S. Pierre. An Android-specific machine-learning-based client-server malware detection approach. 2(3)553-774 (MDPI IoT).

15. Published in 2018 by Guo, Y., Liu, F., Cai, Z., Xiao, N., and Zhao, Z. Mobile cloud storage with efficient edge-based search over encrypted data. 18(4), 1189 MDPI Sensors.
16. Hassonah, M. A., Hijawi, W., J. Alqatawna, A. M. Al-Zoubi, and H. Faris (2021). Identifying Android botnets with a deep static analysis utilizing machine learning models. Referenced in 58(10):102735 of the Journal of Information Security and

Applications.

17. Arnes, and T. V. Do and K. Jensen (2017). Protecting against security flaws in telecommunications using big data analytics. 20:2363–2374, Cluster Computing.
18. Jin, Z., and C.-K. Lim. Relationship framework for mobile payment service quality, systemic features, customer trust, perceived risk, customer happiness, and continued usage. The Journal of the Systems and Management Sciences, 11(2), pages 48-64.
19. (2020) Jin Z. and Lim CK. Factors that contribute to happy customers and their desire to keep using mobile payment services are the focus of this research. Global Vision Press, Issue 8(2), Pages 25–30, International Journal of Smart Business and Technology.
20. (2007), Kitchenham & Charters. A methodological framework for software engineering literature reviews (EBSE Technical Report, Version 2.3).
21. Researchers Li, Y., F. Zhou, Y. Ge, and Z. Xu (2002)1. K-nearest-neighbor search in mobile social networks with enhanced privacy. Sensors, MDPI, 21(12), 3994.
22. (2020) Lima, A.; Rosa, L.; Cruz, T.; Simes, P. A mobile device security monitoring infrastructure. Specifically, MDPI Electronics is on page 1197 of their 9th edition.
23. Kulkarni, Niyaz, Q., Javaid, A. Y., and Mathur, A. (2021). NATICUSdroid is an Android framework that uses native and custom permissions to identify malware. Security and Applications in the Journal of Information Technology, 58(10):102694.
24. It was published in 2017 by Millar, S., McLaughlin, N., Rincon, J. M. D., and Miller, P. Zero-day Android malware detection using multi-view deep learning. A 58(10)2718 issue of the Journal of Information Security Applications.
25. S. Mondal & P. Bours 2018. A constant integration of mobile device security and forensics. 40, pp. 63-77 in the Journal of Information Security and Applications.
26. Researchers F. J. More-Gimeno, H. Mora-Mora, Daniela Marcos-Jorquera, and Bart Volckaert (2018). A trust-based, multi-tiered mobile edge computing platform for outsourcing data processing tasks. Sensors, 18(10), MDPI (Online) 3211.
27. A Mullai and K. Mani. Simplified swarm optimization and particle swarm optimization are used to improve the security of RSA and elliptic curve cryptography based on addition chain on mobile devices. 13(4-5):551-564 in International Journal of IT.
28. According to Niewolski (2020), Nowak (2020), Sepczik (2020), and Kotulski (2021). 5G Mobile Edge Computing Authentication Token Framework. Electronics, MDPI, 10(14), 1724.
29. According to Pattani and Gautam (2021). SonicEvasion is a covert ultrasound-based incursion that exploits the privacy and security of modern mobile devices. Journal of the Association for Information Systems, 13, no.
30. It was written by Saharan, Laxmi, Bezawada, and Gaur in 2021. Fuzzing and scaling: protecting mobile cloud-stored images against automated assaults. Security and Applications in the Journal of Information 60:102850.
31. (2019) M. Salehi, M. Amini, and B. Crispo. Identifying harmful software by monitoring service requests in the operating system. MobiQuitous: Mobile Computing, Networking, and Service Providers Conference.
32. Schürmann, Daniela; Dechand, Sara; Wolf, Laura; 2017. OpenKeychain is Android's cryptographic smart card and NFC ring infrastructure. 1–24 in ACM Transactions on Interactive, Mobile, Wearable, and Ubiquitous Technologies, volume 1, issue 3, 2016.

33. (2020) Shahab, S., M. Fathi, A. T. Chronopoulos, F. Palumbo, and A. Pescape. Methods for detecting intrusion using computational intelligence in mobile cloud computing settings: a review, taxonomy, and outstanding research questions. Security and Privacy in Networked Systems and Applications 55(10):102582.
34. According to Shahbodin (2019), Azni (2019), and Ali (2019). MHealth Cybersecurity with Minimal Cryptographic Overhead. pp. 44-50 in 2019 Asia Pacific Information Technology Conference Proceedings.
35. J. D. Trigo, O. J. Rubio, M. Miguel Espronceda, A. Alesanco, J. Garcia, and L. S. Arriezu are all authors on a forthcoming paper. Developing social media-based mobile health services that are standardized and secure. 9(2208)MDPI Electronics.
36. In 2020, Vaghela, K. Online shopping security predictions for mobile payments. Global Vision Press's 8(2) issue of the International Journal of Smart Business and Technology, pages 31–40.
37. Security authentication system for mobile communication networks using artificial intelligence algorithms with coupled kernel functions, Wang, Z., and Fang, B. (2019). 75, 5946–5964, The Journal of Supercomputing.
38. Xiao, Hu, Peng, S., Jiang, Y., & Yan, R. There is a new deep learning technique for spotting code injection attacks in hybrid apps. Systems and Software (137), pages 67-77.
39. X. Zeng; X. Zhang; S. Yang; Z. Shi; and C. Chi (2021). Implicit authentication based on gait data utilizing mobile edge computing and deep learning. Sensors (21(13):4592) from MDPI.
40. Bentahar, A., Derdour, B., Amroune, M., & Zeroual, A. (2021). Secure authentication for mobile cloud computing using a lightweight deep learning model. Computer and Information Sciences: A Journal of King Saud University. ISSN 1319-1578.
41. Jian Zhang, Xiaozhi Zhuang, and Yuan Chen. Malware on Android is detected via a hybrid static/dynamic analysis. Referenced on the pages 6-10 of the ICCNS 2019: Proceedings of the 9th International Conference on Communication and Network.
42. K. Zou & D. Wang. (2021). The effect of mobile narrative video ads on consumers' empathetic reactions to advertising. 11(1), pp. 1-20, Journal of System and Management Sciences.