**ISSN** 1816-6075 (Print), 1818-0523 (Online)
**Journal of System and Management Sciences**
Vol. 12 (2022) No. 2, pp. 66-78
DOI: 10.33168/JSMS.2022.0204

# Mobile Device Security: A Systematic Literature Review on Research Trends, Methods and Datasets

Mychael Maoeretz Engel[1,2], Arief Ramadhan[1], Edi Abdurachman[1], Agung Trisetyarso[1]

[1]Computer Science Department, Binus Graduate Program, Doctor of Computer Science, Bina Nusantara University, Jakarta, Indonesia

[2]Department of Informatics, Universitas Ciputra, Surabaya, Indonesia

arief.ramadhan@binus.edu

**Abstract.** Security risks, requirements, and security policies have all changed in the new mobile environment. The authentication for mobile communications networks techniques has piqued academic and business interest as an issue for mobile communications evolution. Research about mobile security has turned into a research hotspot. This paper conducts a systematic review, which is a technique to evaluate, interpret and locate all accessible research materials to answer the specific research question. This review was carried out in three stages: planning the data source and search string, conducting the study selection, and then reporting the results of the review. According to the analysis of the selected primary studies, current Mobile Device Security research focuses on four issues and trends: malware and intrusion detection, cryptography, authentication, and information invasion. Of the four focuses, it can be said that the method most frequently encountered and used is artificial intelligence. In addition, 60.61 percent of research papers utilized public datasets, whereas 39.39 percent used private datasets. This research has contributed to the academic and practical side and can guide future research or system development related to Mobile Device Security.

**Keywords:** Systematic review, mobile device security, research trends, methods, datasets

# 1. Introduction

The security architecture is organized into three layers (transport, service, and application) and four distinct realms (user, access, network, and application domain), each with its own set of security characteristics. Security risks, requirements, and policies have changed in the new mobile device environment. The authentication for mobile communications networks techniques have piqued academic and business interest as an issue for mobile communications evolution, and study into mobile security has turned into a research hotspot (Wang & Fang, 2019). Some of them are research related to M-Health and M-money. These two things are closely related to the importance of security.

Mobile health, often known as mHealth, is defined by the World Health Organization (WHO) as the practices of public and medical health supported by mobile technology, which covers the collection, modification, classification, and transport of health-related data (Trigo et al, 2020). Even though the feasibility and availability of basic telemonitoring m-health services are widely established in the literature, there are still difficulties to be resolved, most notably security and privacy concerns.

Then there's the M-money (mobile money), which is revolutionizing the lives of Sub-Saharan Africa's vast unbanked population. Rural areas and low-income persons can use the mobile money system (MMS) to get various services at a low cost. MMS has expanded fast, offering various benefits such as simplicity, dependability, speed, flexibility, and cost. It also alleviates domestic financial concerns, reduces the security dangers associated with carrying real money, and reduces long queues at banking institutions. Due to the high demand, security issues linked to the present two-factor authentication system (2FA) technique for e-money have surfaced (Ali et al, 2020).

Because there are so many different datasets and methodologies for Mobile Device Security systems, a complete view of the situation of Mobile Device Security research is lacking. The goal of this systematic review is to define and assess Mobile Device Security trends in research, frequently used datasets, and approached methods utilized in Mobile Device Security research between 2017 and 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

rise in the number of people who use their phones on YouTube service, which demonstrates the growing popularity of mobile devices. Facebook mobile users have significantly increased. According to the research, mobile users accounted for 73% of Facebook's total users in the second quarter of 2013, up from 56 percent and 43 percent in 2012 and 2011.

Mobile phones also store sensitive information like lists of contact, numbers of credit cards, and passwords (Chan et al 2016). People love banking on the go because it allows them to have mobile access to their accounts while also saving their account credentials on the device. Because their chosen data is easily available on these devices, attackers are now focusing their efforts on mobile devices., where security concerns are addressed less carefully (Alimardani & Nazeh, 2018; Jin et al., 2020; Vaghela, 2020).

Apart from M-health and M-money that have been mentioned in the Introduction section, research on the use of mobile devices has also been carried out in many other fields, for example in the fields of education, retailing, advertising, and others. Research on the use of Augmented Reality on mobile devices for remote collaboration has been carried out by Byeon & Yu (2022). Then Zou & Wang (2021) researched the use of mobile devices for storytelling in video advertising. Meanwhile, Jin & Lim (2021) focus on mobile payment services. And all of them need special attention to the security aspect

# 3. Research Method

We determined to evaluate the literature on Mobile Device Security thoroughly. A Systematic Literature Review (SLR) has become a well-known reviews method. SLR has been accepted as a valid method in research, as done by Berguig & Abdelbaki (2021) and Dahiya et al (2021). It is a technique to evaluate, interpret and locate all accessible and relevant research materials to answer the specific research question (Kitchenham & Charters, 2007). This literature review was done based on Kitchenham and Charters' core characteristics stated in 2007.

Fig. 1 depicts the three stages of SLR. Stage one identifies the prerequisites for a systematic review. Stage two consists of study selection based on exclusion-inclusion criteria, evaluation of the literature quality, data extraction, and interpretation of the synthesized data. The last stage is to report the result thoroughly.

## 3.1. Research question

The Research Question (RQ) stated to keep the review process on track. The criteria of PICOC (Population, Intervention, Comparison, Outcomes, and Context) were used to design the research question (Kitchenham & Charters, 2007) and are shown in Table 1. Table 2 is used to list the research question and aims of the literature review. Figure 2 depicts the main mind map for the SLR.

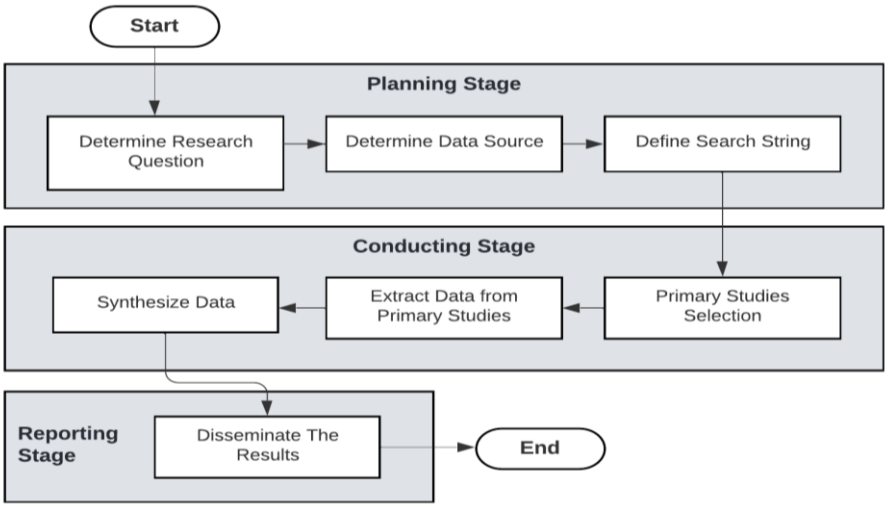


Fig. 1: The systematic literature review steps in this research

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 |

## 3.2. Search strategy

This steps is about selecting digital library resources and establishing the search method. This also includes creating a search phrase, polishing the search phrase, and collecting a preliminary collection of selected research from digital repositories that match the search phrase. The most widely used literature databases in the subject are

slected to obtain as comprehensive as set of potential research. We use Springer (link.springer.com), ScienceDirect (sciencedirect.com), MDPI (mdpi.com), and ACM Digital Library (dl.acm.org).

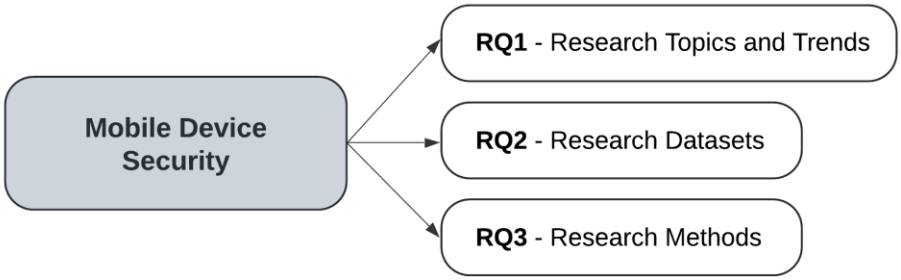


Fig. 2: The SLR's core mind map on mobile device security

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.

Finally, the following search string was employed:

(Mobile Device OR Smartphone) AND (Security) NOT (IoT OR Internet of Things)

The query term is adjusted to match the particular parameters for every database. All databases were examined on keyword, title, and abstract. The query was narrowed by the year of publication, which was between 2017 and 2021. Then, we restrict to only taking journal articles or conference proceedings. We only considered research that is published in English.

## 3.3. Study selection

Primary studies (research) were picked using the exclusion and inclusion criteria. Table 3 below shows the exclusion and inclusion criteria.

Table 3: The exclusion and inclusion criteria

| Inclusion Criteria | Exclusion Criteria |
|---|---|
| The research is published in between 2017 and 2021.<br>Journal articles or conference proceedings<br>For duplicate publications, just the most recent ones will be listed. | Research that is not written in English.<br>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.

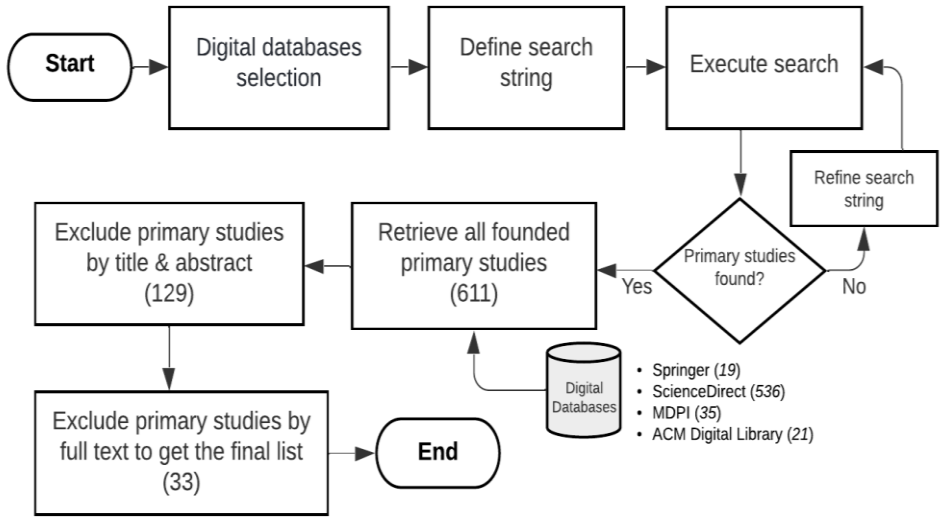


Fig. 3: The process of finding and selecting primary studies on literature review

## 3.4. 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<br>Mobile Device security datasets<br>Mobile Device security methods | RQ1<br>RQ2<br>RQ3 |

# 4. Result and Discussion

## 4.1. Research trends

There are 33 primary studies included that talk about Mobile Device Security. The graph in Figure 4 depicts the evolution of interest in Mobile Device Security. More research have been published since 2018, suggesting more current and relevant

research. Fig. 4 also demonstrates that the mobile Device security research field is still highly relevant today.

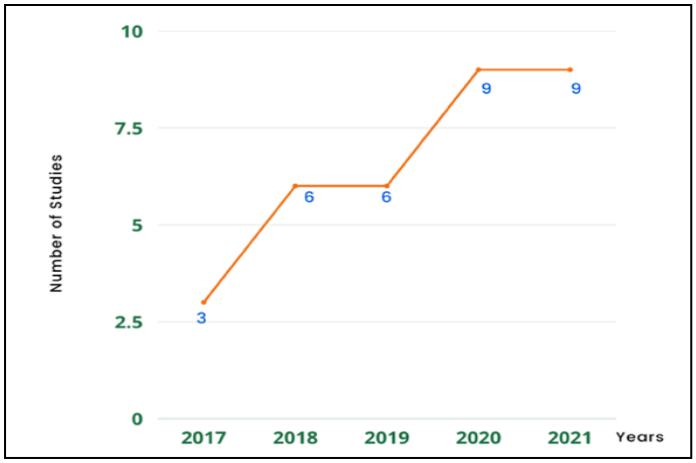


Fig. 4: The allocation of chosen research throughout the years

## 4.2. Research topics and methods used in mobile device security

Based on their content, we synthesized that current Mobile Device Security research focuses on four topics with their methods, ie:

1. Malware and Intrusion Detection: This type of work employs the service monitor method (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 (Deypir & Horri, 2018), NATICUSdroid (Mathur et al, 2021), semantic dynamic (Bhandari et al, 2018)), and computational intelligence (CI) (Shahab et al, 2020), among others.
2. Cryptography: 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) are all used in this kind of research.
3. Authentication: This type of work uses combined kernel function artificial intelligence algorithm, seamless secure anonymous (Deebak et al, 2020), token-based authentication framework (Niewolski et al, 2021), proposed D2D security (Edris et al, 2021), gait-based authentication (Zeng et al, 2021, Axente et al, 2020), and lightweight deep learning model secure authentication (Zeroual et al, 2021).
4. Information Invasion: This type of work uses implicit evasive information invasion with sound, called SonicEvasion (Pattani & Gautam, 2021).

Of the four focuses, it can be said that the method most frequently encountered and used is artificial intelligence. Artificial intelligence is currently one of the best methods of automating digital transformation which is always evolving and is increasingly needed in human life.

### 4.3. Datasets used for the security of mobile device

Dataset is used for a certain purpose. A set of training data is the collection of data put into a system of machine learning, which is analyzed and creates a useful model from it. A set of tests or evaluations data is a collection of data to assess a learning system of the model. The training and test set data include distinct data sources. 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 application from different families and resources (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).
- Malgenome contagio minidump (D'Angelo et al, 2020).
- Public mobile biometrics (Mondal & Bours, 2018).
- UCI machine learning repository (Axente et al, 2020).
- ORL and extended yale (Zeroual et al, 2021).
- Sparks dataset APIs (Lima et al, 2020).
- Enron email datasets (Li et al, 2021).
- Call detail records (Forte et al, 2019).
- Public natural landscape images and facial images (Saharan et al, 2021).

From the explanation of the grouping of datasets above, it can be concluded that the use of public datasets is higher than that of private datasets. Thus, the research that has been carried out has indications that it can be applied by the general public or other researchers who have similar problems or case studies.

Fig. 5 depicts the entire mind map, which summarizes the findings of the SLR on the mobile devices security. Mind maps were also used to study connections between ideas and different parts of a debate and come up with problem-solving solutions. It gives us a fresh way of looking at things by viewing all of the crucial concerns and weighing our options in light of the big picture (Buzan & Griffiths, 2013). It also facilitates effectively organizing knowledge and absorbing new information.

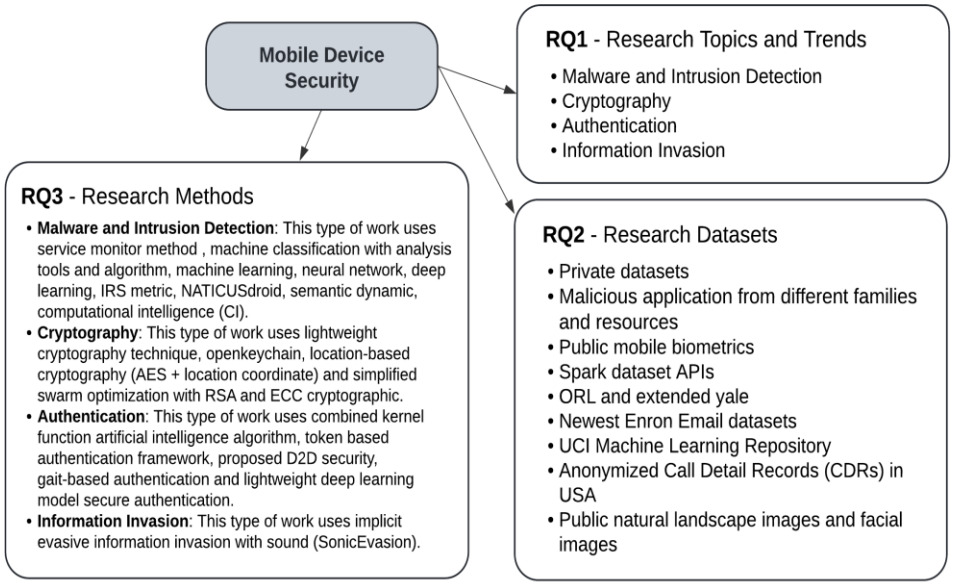


Fig. 5: The complete mind map of the results of SLR on mobile device security

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.

## 5. Conclusion

This SLR aims to determine and evaluate the trends, methods, and datasets utilized in Mobile Device Security research between 2017 and 2021. Finally, based on the exclusion and inclusion criteria, 33 Mobile Device Security research issued around January 2017 until December 2021 were kept to be analyzed. This review was carried out systematically. An SLR is a strategy to locate, assess, and understand all research information that is accessible in a position to respond to the specific research question.

Based on the results, it can be concluded that current Mobile Device Security research focus on four themes, i.e., malware and intrusion detection, cryptography, authentication, and information invasion. Of the four focuses, it can be said that the method most frequently encountered and used is artificial intelligence. In addition, 60.61 percent of research papers utilized public datasets, whereas 39.39 percent used private datasets.

We managed to find four themes in the Mobile Device Security research. We also identify methods and datasets that can be used. Those results contribute to both the

academic side for further research and can become a guidance to the practitioner on the practical side.

# References

Ali, G., Dida, M. A. & Sam, A. E. (2020). Two-factor authentication scheme for mobile money: A review of threat models and countermeasures. *MDPI Future Internet*, 12, 160.

Alimardani, H. & Nazeh, M. (2018). A taxonomy on recent mobile malware: features, analysis methods, and detection techniques. In *Proceedings of the 2018 International Conference on E-business and Mobile Commerce, ICEMC 2018,* 44-49.

Axente, M. -S., Dobre, C., Raluca, R –l. C. & Purtan, P. (2020). Gait recognition as an authentication method for mobile devices. *MDPI Sensors*, 20(15), 4110.

Berguig, O. & Abdelbaki, N. (2021). Impact of quality of work life's dimensions on turnover intention: a systematic literature review. *Journal of System and Management Sciences*, 11(2), 134-254.

Bhandari, S., Panihar, R., Naval, S., Laxmi, V., Zemmari, A. & Gaur, M. S. (2018). SWORD: semantic aware android malware detector. *Journal of Information Security and Applications*, 42, 46-56.

Buzan, T. & Griffiths, C. (2013). Mind maps for business: Using the ultimate thinking tool to revolutionise how you work (2nd Edition). *FT Press*.

Byeon, G. & Yu, S. (2022). Mobile AR contents production technique for long distance collaboration. *Journal of System and Management Sciences*, 12(1), 129-142.

Chan, J. H. and Hong, J. L. (2016). Mobile Security and its Application. *International Journal of Security and Its Applications*, NADIA, 10(10); 89-106, http://dx.doi.org/10.14257/ijsia.2016.10.10.10.

D'Angelo, G., Ficco, M. & Palmieri, F. (2020). Malware detection in mobile environments based on autoencoders and API-images. *Journal of Parallel and Distributed Computing*, 137, 26-33.

Dahiya, A., Gautam, N. & Gautam, P. K. (2021). Data mining methods and techniques for online customer review analysis: A literature review. *Journal of System and Management Sciences*, 11(3), 1-26.

Deebak, B. D., Al-Turjman, F. & Mostarda, L. (2020). Seamless secure anonymous authentication for cloud-based mobile edge computing. *Computer and Electrical Engineering*, 87, 106782.

Deypir, M. & Horri, A. (2018). Instance beased security risk value estimation for Android applications. *Journal of Information Security and Applications*, 40, 20-30.

Edris, E. K. K., Aiash, M. & Loo, J. (2021). Formal verification of authentication and service authorization protocols in 5G-enabled device-to-device communications using proverif. *MDPI Electronics*, 10(13), 1608.

Forte, A. G., Wang, W., Veltri, L. & Ferrari, G. (2019). A next-generation core network architecture for mobile networks. *MDPI Future Internet*, 11(7), 152.

Fournier, A., Khoury, F. E. & Pierre, S. (2020). A client/server malware detection model based on machine learning for android devices. *MDPI IoT*, 2, 355-374.

Guo, Y., Liu, F., Cai, Z., Xiao, N. & Zhao, Z. (2018). Edge-based efficient search over encrypted data mobile cloud storage. *MDPI Sensors*, 18(4), 1189.

Hijawi, W., Alqatawna, J., Al-Zoubi, A. M., Hassonah, M. A. & Faris, H. (2021). Android botnet detection using machine learning models based on a comprehensive static analysis approach. *Journal of Information Security and Applications*, 58, 102735.

Jensen, K., Nguyen, H. T., Do, T. V. & Årnes, A. (2017). A big data analytics approach to combat telecommunication vulnerabilities. *Cluster Computing*, 20, 2363-2374.

Jin, Z. & Lim, C. -K. (2021). Structural relationships among service quality, systemic characteristics, customer trust, perceived risk, customer satisfaction and intention of continuous use in mobile payment service. *Journal of System and Management Sciences*, 11(2), 48-64.

Jin, Z. & Lim, C. K. (2020). A study on the influencing factors of customer satisfaction and continuous use intention in mobile payment service. *International Journal of Smart Business and Technology*, Global Vision Press , 8(2), 25-30.

Kitchenham, B. & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering, *EBSE Technical Report Version 2.3*.

Li, Y., Zhou, F., Ge, Y. & Xu, Z. (2021). Privacy-enhancing k-nearest neighbors search over mobile social networks. *MDPI Sensors*, 21(12), 3994.

Lima, A., Rosa, L., Cruz, T. & Simões, P. (2020). A security monitoring framework for mobile devices. *MDPI Electronics*, 9(8), 1197.

Mathur, A., Podila, L. M., Kulkarni, K., Niyaz, Q. & Javaid, A. Y. (2021). NATICUSdroid: A malware detection framework for android using native and custom permissions. *Journal of Information Security and Applications*, 58, 102696.

Millar, S., McLaughlin, N., Rincon, J. M. D. & Miller, P. (2017). Multi-view deep learning for zero-day android malware detection. *Journal of Information Security and Applications*, 58, 102718.

Mondal, S. & Bours, P. (2018). A continuous combination of security & forensics for mobile devices. *Journal of Information Security and Applications*, 40, 63-77.

More-Gimeno F. J., Mora-Mora, H., Marcos-Jorquera, D. & Volckaert, B. (2018). A secure multi-tier mobile edge computing model for data processing offloading based on degree of trust. *MDPI Sensors*, 18(10), 3211.

Mullai, A. & Mani, K. (2020). Enhancing the security in RSA and elliptic curve cryptography based on addition chain using simplified swarm optimization and particle swarm optimization for mobile devices. *International Journal of Information Technology*, 13, 551-564.

Niewolski, W., Nowak, T. W., Sepczik, M. & Kotulski, Z. (2021). Token-based authentication framework for 5G MEC mobile networks. *MDPI Electronics*, 10(14), 1724.

Pattani, K. & Gautam, S. (2021). SonicEvasion: A stealthy ultrasound based invasion using covert communication in smart phones and its security. *International Journal of Information Technology*, 13, 1589-1599.

Saharan, S., Laxmi, V., Bezawada, B. & Gaur, M. S. (2021). Scaling & fuzzing: personal image privacy from automated attacks in mobile cloud computing. *Journal of Information Security and Applications*, 60, 102850.

Salehi, M., Amini, M. & Crispo, B. (2019). Detecting malicious applications using system services request behavior. In *Conference: MobiQuitous: Computing, Networking and Services*, 200-209.

Schürmann, D., Dechand, S. & Wolf, L. (2017). OpenKeychain: An architecture for cryptography with smart cards and NFC rings on android. In *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 1(3), 1-24.

Shahab, S., Fathi, M., Chronopoulos, A. T., Palumbo, F. & Pescape, A. (2020). Computational intelligence intrusion detection techniques in mobile cloud computing environments: review, taxonomy, and open research issues. *Journal of Information Security and Applocations*, 55, 102582.

Shahbodin, F., Azni, A. H. & Ali, T. (2019). Lightweight cryptography techniques for mhealth cybersecurity. In *Proceedings of the 2019 Asia Pacific Information Technology*, 44-50.

Trigo, J. D., Rubio, O. J., Miguel, Espronceda, M., Alesanco, A., Garcia, J. & Arriezu, L. S. (2020). Building standardized and secure mobile health services based on social media. *MDPI Electronics*, 9, 2208.

Vaghela, K. (2020). E-commerce mobile payment risk trend prediction. *International Journal of Smart Business and Technology*, Global Vision Press, 8(2), 31-40

Wang, Z. & Fang, B. (2019), Application of combined kernel function artificial intelligence algorithm in mobile communication network security authentication mechanism. *The Journal of Supercomputing*, 75, 5946-5964.

Yan, R., Xiao, X., Hu, G., Peng, S. & Jiang, Y. (2018). New deep learning method to detect code injection attacks on hybrid applications. *The Journal of System and Software*, 137, 67-77.

Zeng, X., Zhang, X., Yang, S., Shi, Z. & Chi, C. (2021). Gait-based implicit authentication using edge computing and deep learning for mobile devices. *MDPI Sensors*, 21(13), 4592.

Zeroual, A., Amroune, M., Derdour, B. & Bentahar, A. (2021). Lightweight deep learning model to secure authentication in mobile cloud computing. *Journal of King Saud University – Computer and Information Sciences*. ISSN 1319-1578.

Zhang, J., Zhuang, X. & Chen, Y. (2019). Android malware detection combined with static and dynamic analysis. In *Proceedings of the 2019 the 9th International Conference on Communication and Network, ICCNS 2019*, 6-10.

Zou, K. & Wang, D. (2021). A study on consumer empathic response to advertising expressions: focusing on mobile storytelling video advertising. *Journal of System and Management Sciences*, 11(1), 1-20.