Identifying Security Risks of Digital Transformation - An Engineering Perspective

Anh Nguyen Duc, Aparna Chirumamilla

Identifying security risks of digital transformation - an engineering perspective

Anh Nguyen Duc[1][0000−0002−7063−9200] and Aparna Chirumamilla[2][0000−0002−7063−9200]

[1] Business school, University of South Eastern Norway
Bø i Telemark, Norway
Anh.Nguyen.duc@usn.no
[2] IDI, Norwegian University of Science and Technology
Trondheim, Norway
aparna.vegendla@ntnu.no

Abstract. Technological advancements continue to disrupt how organizations compete and create value in almost every industry and society. The recent digital transformation movement has expanded the reliance of companies and organizations in software technologies, such as cloud computing, big data, artificial intelligence, internet-of-things, and also increase the risk associated with software usage. This work aims at identifying security risks associated with these technologies from an engineering management perspective. We conducted two focused groups and a literature review to gather and discuss the list of security risks. The findings have implications for both practitioners to manage software security risks and future research work.

Keywords: Digital transformation · Cybersecurity · Software vulnerability · Internet-of-things · Cloud computing · Big data · Artificial Intelligence

1 Introduction

Technological changes continue to disrupt how organizations compete and create values in almost every industry and societies. Recent trending technologies, such as cloud computing, big data, artificial intelligence, and internet-of-things have expanded the reliance of organizations in data and data processing software. Many companies have experienced an organizational process so-called "digital transformation" to explore these new digital technologies and to exploit their benefits [13, 16]. However, this process is not risk-free. Before realizing the potential benefits of adopting such technologies, digital strategy makers should be aware of pitfalls that might impact the digital transformation process [10].

Cybersecurity is recognized as a significant cross-cutting concern that influences various aspects of digital transformation, from the choice of technology to the financial outcomes [36]. The Center for Strategic and International Studies estimates that "*the likely annual cost to the global economy from cybercrime is*

more than 400 billion US dollars" [28]. A recent industrial survey shows that almost 60 percent of respondents experienced a phishing attack in 2015, and in 30 percent of these organizations, it is occurring on a daily basis [9]. While considering software technology to adopt, it is increasing demand on securing safety and security of organizations' data [3]. However, securing software is not a simple task, due to not only the emergence and evolution of software technologies, but also the peer pressure of digital transformation movement. While many organizations recognize the importance of cybersecurity, it is still a limited understanding of the actual effort on identifying and managing risks of cybersecurity [9]. Towards a risk management framework for digital transformation, such as [8], we aim at providing an overview of cybersecurity risks in digital transformation. Instead of looking at organizational or managerial factors, the work focuses on engineering aspect. Our research question is:

> RQ: What are engineering-level security risks relevant to a digital transformation process?

From an academic perspective, this paper contributes to business research about digital transformation by a list of security concerns in emerging technologies. From a practitioner's perspective, the list can be used as a checklist for further analysis when an organization wants to adopt one or many digital technologies.

The paper is organized as follows. Section 2 presents the terminology of security. Section 3 describes our research methodology. Section 4 presents technology-specific security challenges. Section 5 discusses the finding and concludes the paper.

2 Terminologies of security

In the software-driven world, it is common to consider security as a quality or non-functional attribute of a software system. Software security is about making software behave correctly in the presence of a malicious attack [17]. Software security is always relative to the data and services being protected, the skills and resources of adversaries, and the costs of potential assurance remedies; security is an exercise in risk management [17, 4]. Several distinguishable terms about software security that are relevant to this work include:

- Vulnerability: a part of the software source code that possesses some weakness in specification, development and operation which will allow any external user to exploit it for any malicious activity.
- Error: a mistake caused by developers of the software is called an error.
- Fault: a piece of source code which on execution causes a failure to occur. It is a hidden programming error caused by programmers.
- Failure: It is the deviation of software from its normal functioning. Software, when exploited or targeted for attack is denied from performing its intended functionality.

– Attack: It is the event that exposes the software's inherent errors. The individuals breaking into the system or program for any malicious activity are termed as attackers.

The general objective of (software) security includes (1) availability, (2) integrity, and (3) confidentiality [33]. Federal Information Processing Standard 199 defines the security categories, security objectives, and impact levels to which SP 800-60 maps information types [33]. The security categories are based on the potential impact on an organization when certain events occur, as shown in Table 1.

Table 1. The three objectives of security

Security aspect	FIPS 199's definitions [33]
Confidentiality	A loss of confidentiality is the unauthorized disclosure of information.
Integrity	A loss of integrity is the unauthorized modification or destruction of information.
Availability	A loss of availability is the disruption of access to or use of information or an information system.

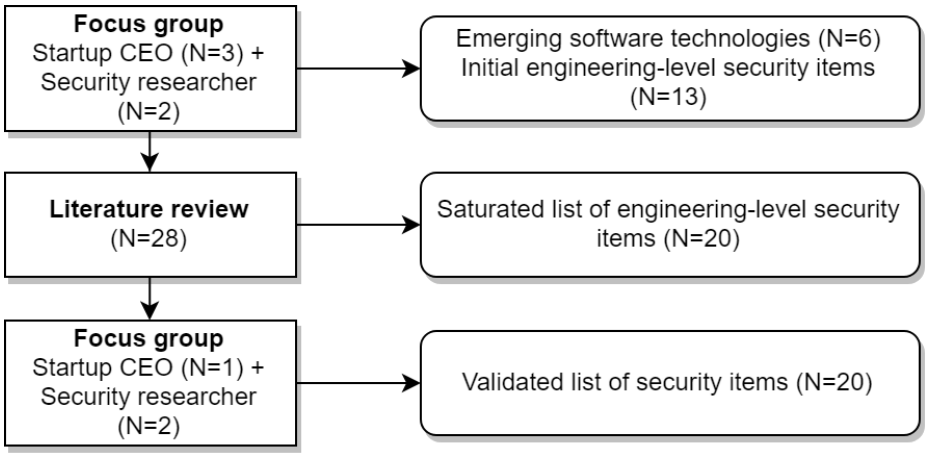

Fig. 1. Research methodology

3 Research Methodology

The research approach adopted in this study is interpretivism [2]. Security risk during digital transformation is subjective to managers and decision makers.

To collect the relevant security risks for organizations, we performed focused groups and literature review. Focused groups are successfully used to collect ideas and initiate the process of further investigation of software engineering phenomenon [34]. We invited managers, strategic decision makers of software companies, software startups and researchers in both engineering and business areas to participate. The first meeting included five participants from both software industry and academia. During this meeting, we identified a list of emerging software-relevant technologies that organization might adopt in their digital transformation process. We also came up with an initial list of security risks that participants were aware of.

The major data collection approach in this work is a literature review. Due to the time limitation, we did not adopt any systematic literature or mapping study [24]. Moreover, the focus of this work is not exhaustively coverage of security risks but raising the awareness of security as a cross-cutting concern in digital transformation. We searched with the string: ("security" or "risk management") AND ("big data" or "artificial intelligence" or "mobile apps" or "digital transformation" or "cloud computing" or "internet-of-things"). We collected risk items from articles that are recent (preferable articles published after 2010), from known journals and conferences, and articles with high citations. The review is stopped when we can add no more new risk items. The final list of risks was extracted from 28 articles given in the Reference section.

The second focused group was dedicated to discussing the relevance of identified security risks. Although there are different opinions on the importance of each risk items in a specific context, we were consensus on the relevance of all identified risks for the digital transformation process. The research process is illustrated in Figure 1.

4 Security risks in software-relevant technologies

The first focused group resulted in thirteen security risk items (65% of the risk items from the literature review), showing that participants were aware of security risks to a good extent. The final list includes 20 unique risk items that will be presented according to software technologies below. Some risks that occur in more than one technology will be presented in one category.

4.1 Mobile security

Current smartphone devices provide lots of the capabilities of traditional personal computers (PCs) and, also, offer a large selection of connectivity options, and inclusion of a wide variety of sensors such as biometric, GPS, compass, gyroscope, barometer, and camera. Although these smartphone functions are more useful for users, often they are vulnerable to attacks. In recent year, researchers have recognized the importance of mobile security [22, 5, 25]. The investment in mobile application's security has steadily increased [27]. Compared to the traditional computing environment, mobile presents some unique risks due to its configurations [22]:

- Resource-limited security mechanisms: Mobile devices have strict resource constraints in both computational and power capabilities due to their mobility and small size. Therefore, while complex security algorithms may scale in standard non-constrained desktop environments, they can be less effective in resource-constrained mobile environments.
- Varied use cases of mobile attacks: Compared to traditional computer attacks, the case of botnets is not as straightforward [22]. Some of the traditional attacks on hosted servers include spam, denial of service extortion, sensitive data theft, and phishing. However, as much sensitive data such as login credentials are stored on mobile devices, attackers may still wish to target them for harvesting data. Moreover, a mobile device is a one-stop-shop for hackers to steal voice/SMS/data communications, track their physical locations in real-time via GPS functionality, and even eavesdrop on non-cellular conversations via the device's microphone. Mobile devices may also act as bridges, allowing penetration of an enterprise's network. [22].
- Platform obscurity: While many mobile platforms are based on commodity operating systems (e.g., Android vs. iOS), they can look significantly different from a security perspective. Besides, different platforms often associate with their ecosystems of mobile apps and communities with different security mechanisms [18]. In addition, platforms are often intentionally restricted from modification and instrumentation due to mobile carrier agreements and regulatory requirements.
- Diverse set of testing configurations Hundreds of different mobile devices are on the market, produced by different vendors, and with different software features and hardware components [20]. Mobile applications, while running on different devices, may behave differently due to variations in the hardware or O.S. components. Hence the protection of mobile devices includes thorough security tests of various combinations of operational environments and mobile devices' configurations.
- Attacks via varied communication channels: Viruses can spread not only through internet downloads or memory cards, but they can also spread through Bluetooth, AirDrop (iPhone-specific communication) or even voice recognition [25, 26]. For instance, a virus can send unsolicited messages over Bluetooth to smartphones and access unauthorized information.

4.2 Cloud storage security

Via different cloud business models[1], organizations are now largely depending on cloud computing for storage, processing and analysis of their data [39]. Despite the affordable cost and easy-to-use as two major motivations for cloud computing, there can be serious threats to security if no proper governance is provided:

- Limited control of third-party services: It is more and more important that customer's data and computation tasks should be kept confidential from

[1] https://www.ibm.com/cloud/learn/iaas-paas-saas

both cloud providers and other customers who are using the service. Users private or confidential information should not be accessed by anyone in the cloud computing system, including application, platform, CPU, and physical memory. Whether adopting public or hybrid cloud environments, a loss of visibility in the cloud can mean the limited control on data security.
- Exposing data to public: Shifting stored data from local computers to cloud servers also means that the data now might be searchable and exploitable by public users [29].Data stored in an IaaS environment can be encrypted to decrease the risk of private data becoming public. However, this is not always as easy as it sounds as the level encryption always depends on the type of encryption method. Moreover, there are other security-relevant challenges of searching, retrieving, and sorting encrypted data [1, 29].
- Expensive on-cloud data auditing: The data owners would less control to ensure data integrity of outsourced data storage than local storage. Moreover, a large amount of cloud data and the users constrained computing capabilities to make data correctness auditing in a cloud environment is expensive and even formidable [29].
- Exploitable Application programming interfaces (APIs): Cloud vendors provide their customers with a range of APIs, which can also be a source of security threats. They may have been deemed to be initially, and then at a later stage be found to be insecure in some way. This problem is compounded when the client company has built its own application layer on top of these APIs. The security vulnerability will then exist in the customers own application. This could be an internal application, or even public facing application potentially exposing private data.

While in-house storage infrastructure is entirely under the control of the company, cloud services delivered by third-party providers do not offer the same level of granularity with regards to administration and management. Although private cloud services could be more secure than legacy architecture, there is still a potential cost for data breaches and downtime.

4.3 Securing Big data

Big Data is defined via the three V: the magnitude of data (volume), the structural heterogeneity of datasets (variety) and the rate at which data are generated (velocity) [12]. Security issues could not be discussed without the context of Big data processes and infrastructures for data management and analytic [6, 32].

- Risks of switching database models Switching from relational databases to NoSQL databases should be done with a careful evaluation due to the differences of security mechanisms between these two types of databases. For instance, in Cassandra[2] databases, nodes in a cluster can communicate freely and no encryption or authentication is used [37, 23]. Moreover, all communication between the database and its clients is unencrypted. It is shown that

[2] http://cassandra.apache.org/

NoSQL has not been designed with security as a priority, so developers or security teams must add a security layer to their organisations.
- Outsourcing data control: Big data administrators may decide to mine data without permission or notification [37]. Whether the motivation is curiosity or criminal profit, the adopted security tools need to monitor and alert on suspicious access no matter where it comes from. If the big data owner does not regularly update security for the environment, they are at risk of data loss and exposure, as seen in Cloud Computing models (Section 4.2)
- Efficient mechanisms for volume and velocity: The sheer size of a big data installation, terabytes to petabytes, is too big for routine security audits. Moreover, most big data platforms are cluster-based, this introduces multiple vulnerabilities across multiple nodes and servers. Besides, classical method to make sure data integrity is that getting all data blocks from the server and has been verified by client [23]. However, this way is inapplicable on big data space. Hence, auditing big data is an active research topic recently [14].

4.4 Security and Internet-of-things

Internet-of-things refers to a systems of sensing devices, hubs, gateways, and servers that provides services on top of a networked of connected devices [21]. Internet-of-things implies the compositions of multiple hardware, communication and software technologies that we have mentioned in the previous sections.Here we describe security issues that is specific for the whole Internet-of-things systems [35, 31, 3]

Table 2. Security concerns across layer of IoT systems [35]

IoT layer	Typical security concerns
Application layer security	Authentication, access control, security audit, etc.
Network layer security	Wireless network security, secure routing, firewall, content analysis, etc.
Physical layer security	Attack detection, intrusion response, cryptography, virus control, etc

- Cross-layer security approaches: Sensing layers could be a subject to physical attacks, including invasive hardware attacks, side-channel attacks, and reverse-engineering attacks [11]. Application layers, including cloud computing, big data, can be compromised by malicious code, such as Trojans, viruses, and runtime attacks (see Section 3.4 and 4.3). Communication protocols are subject to protocol attacks, including man-in-the-middle and denial-of-service attacks [30].
- Flexible system architecture [3]: IoT systems would require multiple and diverse security protocols and standards in order to support (i) multiple security objectives (e.g., secure communications, DRM), (ii) interoperability

in different environments (e.g., a handset that needs to work in both 3G cellular and wireless LAN environments), and (iii) security processing in different layers of the network protocol stack. The overall security architecture should be flexible enough to adapt easily to changing requirements.
- Hardware-based versus software-based security solutions [31]: There is a rich body of literature on security architectures for Internet-of-Things systems, mainly due to the broad range of devices considered as embedded systems. On one hand, hardware-based security solutions might be complex and expensive for low-end embedded systems. On the other hand, software-based isolation of components might not satisfy security and performance requirements.

4.5 Security and Artificial Intelligence (AI)

There have been increasing scientific discussions about AI and cybersecurity [19]. Research shows that 60 percent of surveyed people think AI could be positively used to find attacks before they do damage. AI's strength is its ability to learn and adapt to its current environment and the threat landscape. If deployed correctly, AI would be able to consistently collect intelligence regarding new threats, attempted attacks, successful breaches, blocked or failed attacks and learn from all of it. However, AI could also be configured to learn the specific defenses and tools that it runs up against, which will allow it to be able to better breach them in the future. Viruses could be created that host this type of AI, which produces malware that can bypass even more advanced security implementations. Moreover, hackers do not even need to tamper with the data itself, and they could work out the features of code that a model is using and mirror it with their own code they are using with malicious intent so the algorithm is not able to catch it.

4.6 Security and digital transformation

Digital transformation, lead by organizational strategy, is causing explosive growth in digital organizations [10]. It is creating new ways to engage customers, collaborate with partners, and achieve operational efficiency. We discuss here the security risk at the business level:

- Securing adopted technologies: These are technologies mentioned above, including smartwatches, health bands, smart home devices, smart cars and voice assistants, artificial intelligence, big data analytics, etc. These products and services need to be provided with suitable security controls mechanisms (detail in Section 4.1. to 4.5) to handle the vulnerabilities, threats and attacks for these technologies.
- Business-driven risk management: Risk management techniques are used to identify information risks arising out of business processes. In digital business, processes are dynamic and evolve, which traditional risk modeling can not handle. Moreover, digital businesses depend on using data and assets,

which increase the risk profile for example, the use of consumer data for digitizing retail.
- Evolving user behaviors: The digital world is built around the consumer or user. The user is given the tools to make a choice. The user can define the level of engagement, such as sharing location information to get relevant services. Traditional security models treat users as the weakest link. This means that, now, the weakest element has the most power.
- Regulation support: Regulations are changing to support digital business and control standards for managing risk and privacy. A good example is the General Data Protection Regulation (GDPR). Compliance assurance and sustenance need to transform to adapt to the relevant changes.

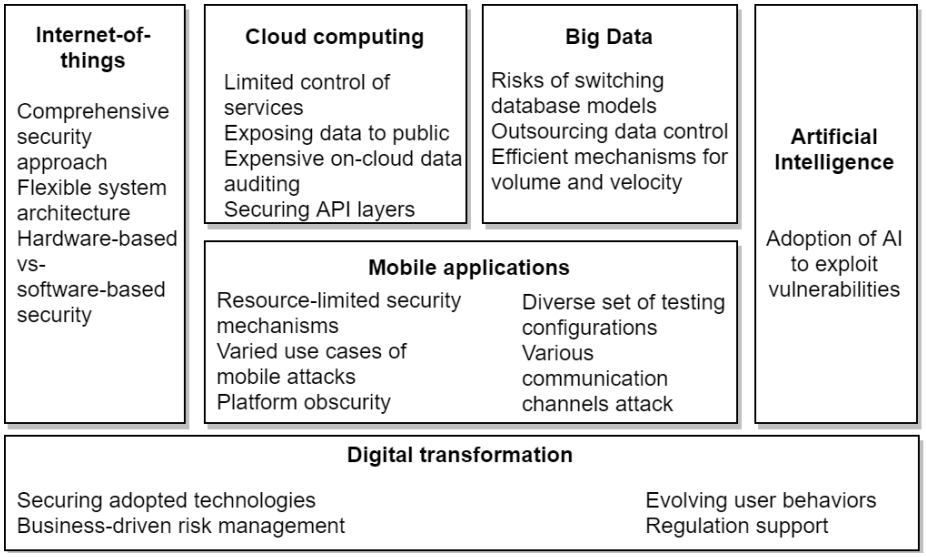

Fig. 2. An overview of security risks associated with emerging technologies

5 Discussion and Conclusions

Digital transformation is recognized as a complex issue, which managers need to balance between achieving organizational agility and other objectives [7]. While there exists research about organizational and managerial risks of digital transformation [38, 7], to the best of our knowledge we found no previous research on engineering-level risks of cybersecurity for digital transformation. Similar research about product engineering, for instance, is about risk management at system architecture level [15].

While digital transformation is considered as strategy-driven actions with risk-taking becoming a cultural norm [10], we found that strategic decision-makers were aware of technical risks associated with the technologies they would adopt. Organizations transform their business by taking advantage of technologies such as mobility, Internet-of-Things and cloud computing, there are security risks in digital transformation to consider. In business models that rely on the quality of offered software-based services and products, cybersecurity has a direct impact on both value creation and financial aspects.

Based on focused groups and literature review, this paper presents a list of security risks for emerging software-based technologies. As shown in Figure 2, the security risks were presented according to the technology stack. The adoption of these technologies in digital transformation can be assisted by this list to reduce the negative impact of software vulnerabilities on business activities. The findings from this study are based on limited empirical evidence. Hence, we do not claim for the comprehensiveness of the list. Future research can adopt surveys or case studies to investigate cybersecurity concerns of digital transformation systematically. Last but not least, this work treats digital transformation at a conceptual level. Future work can explore in detail the process of transforming, i.e., possible effect before, during, and after the transformation.

6 Acknowledgments

This work was co-funded under the Vietnam national project entitled " *Towards the development of secured Operating Systems and App Stores for e-Goverment solutions*". The project is led by MQ Solution [3].

References

1. Behl, A., Behl, K.: An analysis of cloud computing security issues. In: 2012 World Congress on Information and Communication Technologies. pp. 109–114 (Oct 2012). https://doi.org/10.1109/WICT.2012.6409059
2. Creswell, J.W.: Research design : qualitative, quantitative, and mixed methods approaches /. SAGE Publications
3. Duc, A.N., Jabangwe, R., Paul, P., Abrahamsson, P.: Security Challenges in IoT Development: A Software Engineering Perspective. In: Proceedings of the XP2017 Scientific Workshops. pp. 11:1–11:5. XP '17, ACM, New York, NY, USA (2017). https://doi.org/10.1145/3120459.3120471, event-place: Cologne, Germany
4. Felderer, M., Bchler, M., Johns, M., Brucker, A.D., Breu, R., Pretschner, A.: Chapter One - Security Testing: A Survey. In: Memon, A. (ed.) Advances in Computers, vol. 101, pp. 1–51. Elsevier (Jan 2016). https://doi.org/10.1016/bs.adcom.2015.11.003
5. Furnell, S.: Handheld hazards: The rise of malware on mobile devices. Computer Fraud & Security **2005**(5), 4–8 (May 2005). https://doi.org/10.1016/S1361-3723(05)70210-4

[3] https://mqsolutions.vn/

6. Gandomi, A., Haider, M.: Beyond the hype: Big data concepts, methods, and analytics **35**(2), 137–144. https://doi.org/10.1016/j.ijinfomgt.2014.10.007
7. Hess, T., Matt, C., Benlian, A., Wiesbck, F.: Options for formulating a digital transformation strategy **15/2**, 123–139
8. InfoQ: Guide to digital transformation. define, price, and plan a digital transformation (part 1), https://www.infoq.com/articles/Digital-Transformation-Guide-1
9. ISACA: State of Cybersecurity: Implications for 2016 - An ISACA and RSA Conference Survey. Tech. rep., ISACA (2016)
10. Kane, G.C., Palmer, D., Phillips, A.N., Kiron, D., Buckley, N.: Strategy, not technology, drives digital transformation (2015)
11. Koushanfar, F., Sadeghi, A., Seudie, H.: EDA for secure and dependable cybercars: Challenges and opportunities. In: DAC Design Automation Conference 2012. pp. 220–228 (Jun 2012). https://doi.org/10.1145/2228360.2228402
12. Laney, D.: 3d data management: Controlling data volume, velocity, and variety | BibSonomy, https://www.bibsonomy.org/bibtex/742811cb00b303261f79a98e9b80bf49
13. Lankshear, C., Knobel, M.: Digital Literacies: concepts, policies and practices, vol. 30. Peter Lang Publishing
14. Liu, C., Ranjan, R., Yang, C., Zhang, X., Wang, L., Chen, J.: MuR-DPA: Top-Down Levelled Multi-Replica Merkle Hash Tree Based Secure Public Auditing for Dynamic Big Data Storage on Cloud. IEEE Transactions on Computers **64**(9), 2609–2622 (Sep 2015). https://doi.org/10.1109/TC.2014.2375190
15. Masuda, Y., Shirasaka, S., Yamamoto, S., Hardjono, T.: Risk management for digital transformation in architecture board: A case study on global enterprise. In: 2017 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI). pp. 255–262. https://doi.org/10.1109/IIAI-AAI.2017.79
16. Matt, C., Hess, T., Benlian, A.: Digital transformation strategies **57**(5), 339–343. https://doi.org/10.1007/s12599-015-0401-5
17. McGraw, G., Potter, B.: Software Security Testing. IEEE Security and Privacy **2**(5), 81–85 (Sep 2004). https://doi.org/10.1109/MSP.2004.84
18. Mohamed, I., Patel, D.: Android vs iOS security: A comparative study. In: 2015 12th International Conference on Information Technology - New Generations. pp. 725–730. https://doi.org/10.1109/ITNG.2015.123
19. Morel, B.: Artificial Intelligence and the Future of Cybersecurity. In: Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence. pp. 93–98. AISec '11, ACM, New York, NY, USA (2011). https://doi.org/10.1145/2046684.2046699, event-place: Chicago, Illinois, USA
20. Muccini, H., Francesco, A.D., Esposito, P.: Software testing of mobile applications: Challenges and future research directions. In: 2012 7th International Workshop on Automation of Software Test (AST). pp. 29–35 (Jun 2012). https://doi.org/10.1109/IWAST.2012.6228987
21. Nguyen-Duc, A., Khalid, K., Shahid Bajwa, S., Lnnestad, T.: Minimum viable products for internet of things applications: Common pitfalls and practices **11**(2), 50. https://doi.org/10.3390/fi11020050
22. Oberheide, J., Jahanian, F.: When Mobile is Harder Than Fixed (and Vice Versa): Demystifying Security Challenges in Mobile Environments. In: Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications. pp. 43–48. HotMobile '10, ACM, New York, NY, USA (2010). https://doi.org/10.1145/1734583.1734595, event-place: Annapolis, Maryland

23. Okman, L., Gal-Oz, N., Gonen, Y., Gudes, E., Abramov, J.: Security Issues in NoSQL Databases. In: 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications. pp. 541–547 (Nov 2011). https://doi.org/10.1109/TrustCom.2011.70
24. Okoli, C.: A guide to conducting a standalone systematic literature review **37**(1). https://doi.org/10.17705/1CAIS.03743
25. Penning, N., Hoffman, M., Nikolai, J., Wang, Y.: Mobile malware security challeges and cloud-based detection. In: 2014 International Conference on Collaboration Technologies and Systems (CTS). pp. 181–188 (May 2014). https://doi.org/10.1109/CTS.2014.6867562
26. Petracca, G., Sun, Y., Jaeger, T., Atamli, A.: AuDroid: Preventing attacks on audio channels in mobile devices. In: Proceedings of the 31st Annual Computer Security Applications Conference. pp. 181–190. ACSAC 2015, ACM. https://doi.org/10.1145/2818000.2818005, http://doi.acm.org/10.1145/2818000.2818005, event-place: Los Angeles, CA, USA
27. Polla, M.L., Martinelli, F., Sgandurra, D.: A Survey on Security for Mobile Devices. IEEE Communications Surveys Tutorials **15**(1), 446–471 (2013). https://doi.org/10.1109/SURV.2012.013012.00028
28. Ponemon: Cost of a Data Breach Study: Global overview. Tech. rep., IBM (2018)
29. Ren, K., Wang, C., Wang, Q.: Security Challenges for the Public Cloud. IEEE Internet Computing **16**(1), 69–73 (Jan 2012). https://doi.org/10.1109/MIC.2012.14
30. Rostami, M., Koushanfar, F., Karri, R.: A Primer on Hardware Security: Models, Methods, and Metrics. Proceedings of the IEEE **102**(8), 1283–1295 (Aug 2014)
31. Sadeghi, A., Wachsmann, C., Waidner, M.: Security and privacy challenges in industrial Internet of Things. In: 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC). pp. 1–6 (Jun 2015). https://doi.org/10.1145/2744769.2747942.
32. Sagiroglu, S., Sinanc, D.: Big data: A review. In: 2013 International Conference on Collaboration Technologies and Systems (CTS). pp. 42–47. https://doi.org/10.1109/CTS.2013.6567202
33. Sharing (LLIS), L.L.I.: FIPS Pub 199: Standards for Security Categorization of Federal Information and Information Systems (Feb 2004)
34. Singer, J., Sim, S.E., Lethbridge, T.C.: Software engineering data collection for field studies. In: Shull, F., Singer, J., Sjberg, D.I.K. (eds.) Guide to Advanced Empirical Software Engineering, pp. 9–34. Springer London
35. Sun, X., Wang, C.: The Research of Security Technology in the Internet of Things. In: Jin, D., Lin, S. (eds.) Advances in Computer Science, Intelligent System and Environment. pp. 113–119. Advances in Intelligent and Soft Computing, Springer Berlin Heidelberg (2011)
36. Teoh, C.S., Mahmood, A.K.: National cyber security strategies for digital economy. In: 2017 International Conference on Research and Innovation in Information Systems (ICRIIS). pp. 1–6. https://doi.org/10.1109/ICRIIS.2017.8002519
37. Terzi, D.S., Terzi, R., Sagiroglu, S.: A survey on security and privacy issues in big data. In: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). pp. 202–207 (Dec 2015)
38. Welch, Nina Kruschwitz, D.B.a.M.M.F.: Embracing digital technology
39. Wu, J., Ping, L., Ge, X., Wang, Y., Fu, J.: Cloud Storage as the Infrastructure of Cloud Computing. In: 2010 International Conference on Intelligent Computing and Cognitive Informatics. pp. 380–383 (Jun 2010). https://doi.org/10.1109/ICICCI.2010.119