Designing Testing Framework with the context of prioritizing security Testing



**Addis Abeba Science and Technology University School of Electrical and Mechanical Engineering Department of Software Engineering**

A research Proposal for Research Methodology

By Yaregal T.

March 2022

Contents

[Introduction 3](#_Toc99739150)

[Problem Statement 4](#_Toc99739151)

[Objectives 5](#_Toc99739152)

[General Objective 5](#_Toc99739153)

[Specific Objective 6](#_Toc99739154)

[Research Questions 6](#_Toc99739155)

[Methodology 6](#_Toc99739156)

[Significance of the Research 7](#_Toc99739157)

[Literature Review 7](#_Toc99739158)

[Literature Summery 9](#_Toc99739159)

[Time Schedule 10](#_Toc99739160)

[Cost Break Down 11](#_Toc99739161)

[References 12](#_Toc99739162)

# Introduction

the Internet of Things (IoT) is "a system of interrelated computing devices, mechanical and digital machines, objects, animals, or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction". The IoT encompasses a large range of devices ('things'), among which everyday household electronics, such as dishwashers, fridges, smart cameras, smartwatches, smart glasses, smart TVs, and smart light bulbs. Wearable devices can monitor heart rate, steps, and spent calories to name just a few 'smart' features introduced by IoT devices

Security in IoT software is not a joke anymore since the IoT systems are improving day-to-day life in a way that our day-to-day life depended on it. In this rise of the Internet of Things (IoT), where billions of devices are expected to be integrated into horizontal applications [4][5]. Security problems are massively increasing because the amount of linked smart devices constantly grows with their use of different standards, the heterogeneity of the devices, their different implementation way [6]- [8], making the security testing operations daunted. imagine your smart TV is hacked by someone and its record audio in your Salone or bedroom, imagine your IoT connected car is hacked, or imagine an intruder successfully hacked your IoT supported door, from these simple cases you can imagine the consequence that successful penetration of security holes in an IoT supported devices will case to the society in a variety of aspects. Since every device such as your watch, washing machine, your doorbell, your ovens, etc. is being able to connect to the internet which increases your vulnerability to security. Since the vulnerability of these devices cause a series of impact, securing IoT devices is a must done task

The main cause of many software attacks is a flow in the software that happened during development which will produce a vulnerability in the system of course it's impossible to develop a 100% flow free system but minimizing the flows in the system have high contribution to reducing the possible vulnerabilities in the system and the best time to capture those flows and fix them before they cause any damage is done during testing, unfortunately, the attacks that happen in IoT software level are mostly caused by software flows in the system. In this regard research has been done focusing on developing IoT security testing methodology, framework and techniques have been developed [3]. But they didn't start by analyzing the cause and move towards finding a solution to the cause they just developed a methodology, a framework, or a technique to perform IoT security testing and the problem still exists. In this paper I will develop a framework that helps to identify known vulnerabilities by giving higher attention to security during all phases of Software testing Lifecyle’s.

# Problem Statement

Over the last few years, IoT devices and IoT-enabled solutions have become significantly popular both for consumers and industries. IoT is not just about embedded devices, but also comprises an ecosystem of device hardware, system integration, connectivity, data storage, security, IoT platform providers, IT and communication service providers, and application development. Currently, there are more IoT devices connected to networks than the number of human beings on the earth. These IoT devices carry a lot of sensitive data which remains insecure. IoT security has become the subject of strong consideration after several high-profile incidents where a common IoT device was used to infiltrate and attack a larger network, hacking of internet-connected devices, surveillance concerns, and privacy.

The main cause of a security problem is a flaw or bug in the design and implementation of the program that runs the IoT system and these flaws and bugs have to be detected and fixed before the system is delivered to customers this is done through testing in which security tested doesn’t get the attention it deserves due to this the security problems are causing a lot of problems not only on the IoT system in which the flaw or the bug is found but also big systems I which this buggy IoT system is communicating.

As said in the introduction part IoT security is still a sensitive issue several studies have been made in the last time which focuses on developing a testing strategy, their main focus is on prevention and mitigation. Since the traditional testing mechanisms are not suitable for IoT systems because of their Heterogeneity, distributed-ness, resource-constrained environment, and use of different platforms. So, using the old software testing didn’t fit the IoT for this reason adapting or developing a new testing framework is mandatory. In this perspective, a lot of studies have been made [list the papers on security testing and frameworks] and different frameworks and methodologies have been designed. but still, the problem existed and IoT systems still have a lot of vulnerabilities after these all-testing methodologies have been adopted and new frameworks are developed [21-25].

Whatever a great testing methodology, framework, tool, or techniques have developed they are embedded inside the general IoT testing methodology which also includes another testing like interoperability testing, conformance testing, Scalability testing and platform independence testing and of course security testing. So, if this general testing methodology didn’t give enough emphasis on the security testing all the methodology, technique, or tool we use have small affect because the problem is not on the methodology, technique, or tool rather on the general testing methodology.

So since even after several studies have been made on security testing and security methodology, technique, tool, and frameworks are developed still the problem is not solved [26,27] in this study we will answer the question. are the general testing frameworks give enough emphasis to security testing? if not? what is the solution to make them give higher emphasis to the security of the IoT system and if yes? what measures have to be taken to strength the security will be answered in this paper.

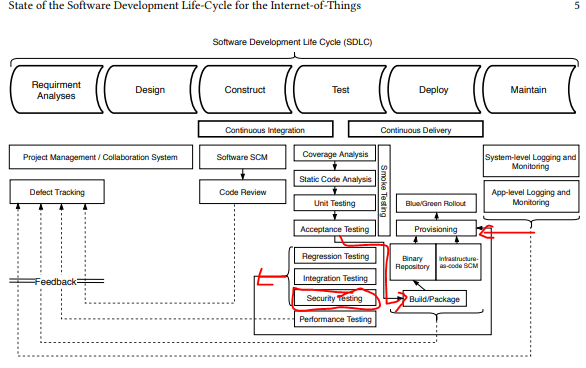


Figure development Life cycles of IoT systems

As shown in the figure since the regular software development phases are not applicable for developing IoT systems because IoT systems are different from regular system by their distributed Ness, heterogeneity, the devices work in a constrained environment so they proposed a new development phase for IoT systems with the detail to each phase. As shown in the figure on the testing phase the security testing is performed after other testing like coverage analysis, static code analysis, unit testing, system testing and acceptance testing are performed so after this testing are performed which needs an additional Time, human power, resource and cost.

# Objectives

## General Objective

Design an IOT testing framework which gives higher emphasis to Security testing of the IOT system

## Specific Objective

* Study state-of-the-art IoT system testing methodologies in the context of security testing by following systematic mapping study (SMS).
* Design IoT testing framework that can add the capability of Security testing.
* Implement a real IOT system and test my framework and other frameworks performance in terms of their ability the reduce cost, Time and unveiling as many vulnerabilities
* Comparison of my framework with other frameworks will be performed

# Research Questions

* Did the current IoT system Testing methodologies give emphasis to testing the security of the system?
* If the answer to the 1st question is no, I will design a IoT system Testing framework that can unveil possible security flows.
* If the answer to the above question is yes so why is the known security problem still a problem?

# Methodology

In the first stage I will analyze the existing state of the art IoT testing methodology and examine if they give enough emphasis to the security testing and the amount of time and cost, they require during testing of the IoT system to achieve this I will perform a systematic mapping study (SMS). Based on the study I will designing a framework that gives higher emphasis to the security of the IoT system and also reduces the amount of time and cost it requires which works a long side the testing methodologies so that everything will be tested once. And then I will develop a real IoT system to evaluate the performance of my framework and other existing frameworks so that a comparison will be performed between them in terms of their cost, time and their effectiveness in unveiling security vulnerabilities

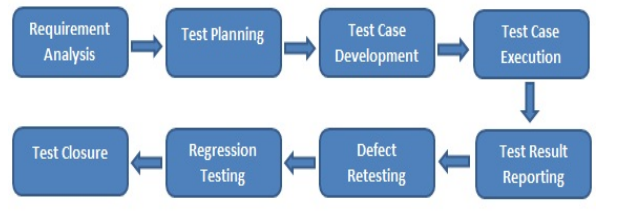


Figure Testing Life Cycle of IoT systems

As shown above the IoT testing life cycle for testing IoT system is proposed by[20] for the testing operations mentioned on figure 1 so on current testing operation which is performed after this phase is performed for testing integrity, conformance, scalability, unit test, system test and integration test are performed by following the phases stated on figure 2 after these testing is completed security testing will be performed during or after deployment by analyzing by analyzing vulnerabilities at shown on figure 1 so we are bringing security testing operations along with each phase of the testing life cycles mentioned on figure 2 above. I will study what have to be performed in each phase of the IoT testing lifecycle in order to include security in each phase and perform test everything once.

Since our research is motivated to solve security problems in the IOT softeare during the stages of testing by unveiling as many vulnerabilities as possible and analysis the IoT testing methodologies are analyzed using the systematic mapping study (SMS) and a designing of new IoT testing framework which will have the additional capability to discover as many security vulnerabilities as possible during the testing stage in addition to unveiling other flows in which the testing is required to discover for this reason the methodology used I may use qualitative approaches to gather data but the general approach will be more on Design Science research approach.

# Significance of the Research

# Literature Review

G. Murad et.al[9] examines the trends in software testing approaches using different types of IOT environments and uncovers various issues that must be to enhance testing in IOT environment

Abbas Ahmad et al[3] an IOT-TaaS(Internet of Things Testing as a Service ) frame work that aims to solve problems such as the scalability of traditional software testing, the heterogeneity of IoT devices increases costs and the complexity of coordination of testing due to the number of variables which arises due to The amount of IoT devices and their collaborative behavior. The aim of the testing framework is to resolve constraints regarding coordination, cost and scalability issue of traditional software testing in the context of standard based development of IOT devices. It is composed of distributed interoperability testing, scalable automated conformance testing and semantic conformance testing.

Pedro Martins Pontes et al[11] in their papers named IZinto a pattern based IOT Testing framework they stated that there are several solutions for testing IOT systems which follows different testing approaches and focus different focus level(),u it, integration and acceptance) covering different layers(cloud layer, fog layer, edge layer) however they have their own limitations such as failing to account for the heterogeneity of the IOT field by focus on specific platform, language, or standards and lack the possibility of improvement or functionality extension, and also not providing out of box functionality by mentioning this limitations they proposed a pattern based test automation framework for integration testing. This framework also have limitation since it only solves the integration testing which didn’t solve other testing’s like interoperability, scalability and security

Brian Ramprasad et al[12] have also discussed the challenges of IOT testing they stated the main challenges with heterogenous IOT network is maintaining the quality of service(QOS) because of the fluctuation in the number of active devices and the data they produce [13-15]. Fluctuations occur because IoT devices may operate under different time of use policies to save energy, IoT devices may fail in the network or their up link to the Internet may be temporarily down. Being able to reliably predict resource utilization in a dynamic heterogeneous IoT environment can help overcome some of the QoS challenges associated with scaling IoT networks. Prediction with high accuracy allows us to plan ahead in preparing for changes in demand on the IoT network. In this paper, they develop a novel resource utilization prediction engine for IoT applications based on a Smart Testing Framework for Adaptation. This allows to execute repeatable experiments to learn about IoT device resource utilization so that we can trigger adaptations to add or remove computing resources.

On paper “Secure SDLC Using Security Patterns 2.0”paper written in 2022[18] they proposed “Secure SDLC using **Security Patterns 2.0 (SSDLC using SPs2.0)**”, and this framework enhances security by minimizing the known vulnerability. Identifying the security requirements using security discoverer process, selection of security pattern for security requirements, design security requirements using security building blocks, creating test templates to support pattern implementation during development stage, vulnerability scanning

Large Scale IoT Security Testing, Benchmarking and Certification(07\_chapter\_07)[20] describes the challenges in IOT security testing and presents a model based approach solution here what they want to solve is what are the challenges when security testing of IoT system is performed or what are the challenges during the implementation of any selected testing strategy then the proposed a model based approach to solve the challenges(read the methodology part)

Consumer IoT: Security Vulnerability Case Studies and Solutions [19] in this paper the researchers try to describe the common attacks to the consumer IOT devices and suggests their mitigation strategy which helps to reduce the severity of the attack

Artorias: IoT Security Testing Framework in this paper the researchers introduce the IoT Security Testing Framework named Artorias which is an automated testing tool to test the TOP 10 security issues identified by OWASP then they show how it tests those areas, how to setup and run Artorias and how Artorias should be used. As we see above this paper selected top 10 OWASP selected security issues, introduces an automated testing tool named Artorias and show how this tool is used to test those security problems. (Read The Methodology part)

The Open Web Application Security Project, or OWASP, evaluated and derived a list of the top 10 vulnerabilities associated with IoT devices in 2014; insecure web interfaces, insufficient authentication or authorization, insecure network services, lack of transport encryption, privacy concerns, insecure cloud interfaces, insecure mobile interfaces, insufficient security configuration, insecure software or firmware and poor physical security [2].

Improving Software Testing, Verification and Reliability in the Software Development Life Cycle (ImprovingSoftwareTesting.pdf) make a detail methodology review on this paper

# Literature Summery

* A range of techniques from utilization of machine learning [30] and deep learning [31] to the development of novel key generation methods [20] and intrusion detection mechanisms [32] were suggested for securing IoT environments. However, still software defects such as buffer overflows, logic flaws, inconsistent error handling, SQL injections are the major source of security issues in IoT [33].
* In this regard Software quality assurance plays a key role, especially in IoT environment where a device might not be updated for considerably long time [35] or devices are deployed in the safety critical environments [34].
* All the papers I have reviewed focuses on the following
  1. Most of the frameworks are about testing the devices security
  2. They all focuses about discovering vulnerabilities after the system have been tested
  3. They don’t Provide methodological approach which can test everything once
  4. They focus on identifying and defending attacks

# Time Schedule

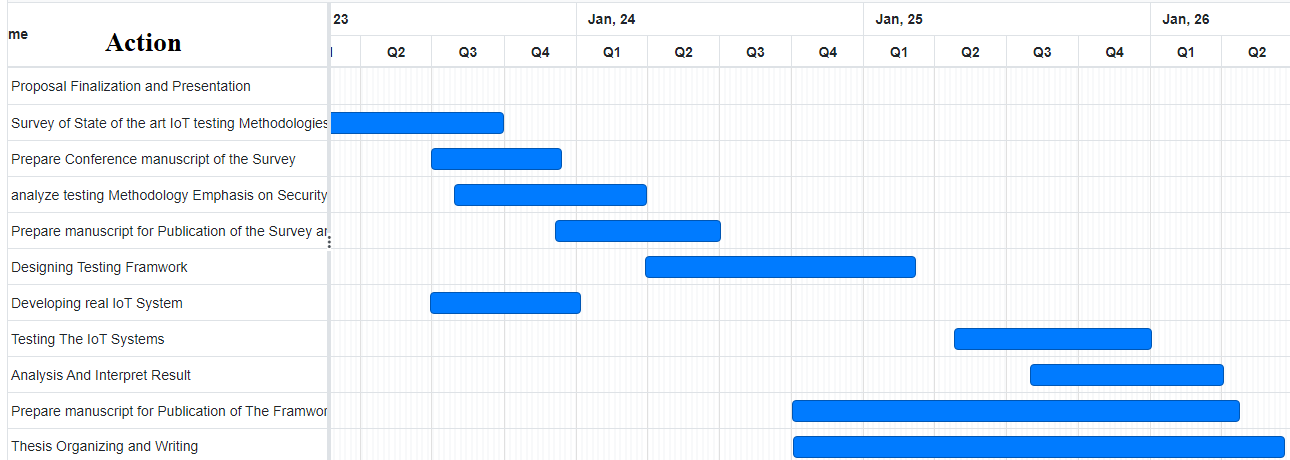
I have provided the time schedule in to forms the first one is using Gantt diagram which will show graphically the actions and the time those actions will be performed to show the overlaping tasks graphically as shown in the figure 3 below. The years are classifed in quarter forms so one year will have four quraters the first, second, third and forth for example Q1 is the first quarter of the year which is the first three months of the year

Figure 3 Research Schedule Diagrammatic view

The secondone as shown on figure 4 below one using a text verson which is In tabular form that describes in detail the start and end date in textual form I prpare it to make the start and end dates vissible..

# Cost Break Down

Figure Research Schedule of the research

|  |  |  |
| --- | --- | --- |
| No | Item | Cost |
| 1 | Data Collection and preparation Cost | 30,000 |
| 2 | Conference and journal publication cost | 36,000 |
| 3 | Hardware Cost/Simulation Software Cost | 200,000/For simulation Tool 100,000 |
| 4 | Human Labor Cost | 20,000 |
| 5 | Transport and communication cost | 10,000 |
| Total | | 296,000 or if simulation is used 196,000 |

# References

1. C.H.R.I.S.T.O.P.H.E.R.S.Y.O.O. (n.d.). article on IOT. Cigionline.Org. Retrieved January 31, 2022, from https://www.cigionline.org/articles/emerging-internet-things/?utm\_source=google\_ads&utm\_medium=grant&gclid=Cj0KCQiArt6PBhCoARIsAMF5wagddds86MyMXi-niFl-yx3swGYbPzhqvyGooatrEBmvZdKB-NKO\_jQaAneLEALw\_wcB
2. B.L.E.G.E.A.R.D. (2019, March 25). Security Testing of IoT systems. In C.V.I.H.O., B.O.U.Q.U.E.T.F.A.B.R.I.C.E., & F.L.E.G.A.L.L. (Eds.), Model-Based Testing for IoT Systems - Methods and Tools (1st ed., Vol. 1, pp. 24–32).
3. Ahmad, A., Baqa, H., Hwang, J., & le Gall, F. (2018, February). IoT-TaaS: Towards a Prospective IoT Testing Framework. 10.1109/ACCESS.2018.2802489, IEEE Access, 1, 1–14.
4. L. Ericsson, “More than 50 billion connected devices,” White Paper, 2011
5. S. Ziegler, C. Crettaz, L. Ladid, S. Krco, B. Pokric, A. F. Skarmeta, A. Jara, W. Kastner, and M. Jung, “IoT6–moving to an ipv6-based future IoT,” in The Future Internet Assembly, pp. 161–172, Springer, 2013.
6. D. Bandyopadhyay and J. Sen, “Internet of things: Applications and challenges in technology and standardization,” Wireless Personal Communications, vol. 58, no. 1, pp. 49–69, 2011.
7. J. Song et al., “Connecting and managing m2m devices in the future internet,” Mobile Networks and Applications, vol. 19, no. 1, pp. 4–17, 2014.
8. P.V. Lingala Thirupathi, N. Rao, Developing a multilevel protection framework using EDF, Intern. J. Advanced Research Eng. Technol. (IJARET) 11 (10) (2020) 893–902.
9. G. Murad, A. Badarneh, A. Qusef. and F. Almasalha, “Software testing techniques in IoT,” in 8th Int. Conf. on Computer Science and Information Technology (CSIT), Amman, Jordan vol. 1, no. 1, pp. 17–21, 2018.
10. Ahmad, A., Baqa, H., Hwang, J., & le Gall, F. (2018, February). IoT-TaaS: Towards a Prospective IoT Testing Framework. 10.1109/ACCESS.2018.2802489, IEEE Access, 1, 1–14.
11. Pontes, P., Lima, B., & Pascoal Faria, J. (2018b). Izinto: a pattern-based IoT testing framework. Conference: Companion Proceedings for the ISSTA/ECOOP 2018 Workshops, 1(1). https://doi.org/10.1145/3236454.3236511
12. Ramprasad, B., Mukherjee, J., & Litoiu, M. (2018). A Smart Testing Framework for IoT Applications. Conference: 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion), 1(1), 1–7. https://doi.org/10.1109/UCC-Companion.2018.00064
13. A. Javed, K. Heljanko, A. Buda, and K. Frmling, “CefIoT: A fault-tolerant IoT architecture for edge and cloud,” in IEEE WF-IoT, 2018.
14. H. F. Atlam, A. Alenezi, A. Alharthi, R. J. Walters, and G. B. Wills,“Integration of cloud computing with internet of things: Challenges and open issues,” in 2017 IEEE International Conference on Internet of Things, 2017.
15. A. Botta, W. de Donato, V. Persico, and A. Pescap, “On the integration of cloud computing and internet of things,” in 2014 International Conference on Future Internet of Things and Cloud, 2014.
16. W. Shi and S. Dustdar, “\*e promise of edge computing,”Computer, vol. 49, no. 5, pp. 78–81, 2016.
17. X. Xia, F. Chen, Q. He, J. Grundy, M. Abdelrazek, and H. Jin,“Cost-effective app data distribution in edge computing,”IEEE Transactions on Parallel and Distributed Systems, vol. 32,no. 1, pp. 31–44, 2020.
18. Aruna, E. & Reddy, A. & Sunitha, K.V.N.. (2022). Secure SDLC Using Security Patterns 2.0. 10.1007/978-981-16-3945-6\_69.
19. T. Alladi, V. Chamola, B. Sikdar and K. -K. R. Choo, "Consumer IoT: Security Vulnerability Case Studies and Solutions," in IEEE Consumer Electronics Magazine, vol. 9, no. 2, pp. 17-25, 1 March 2020, doi: 10.1109/MCE.2019.2953740.
20. Ahmad, Abbas & Baldini, Gianmarco & Cousin, Philippe & Matheu Garcia, Sara Nieves & Skarmeta, Antonio & Fourneret, Elizabeta & Legeard, Bruno. (2017). Large Scale IoT Security Testing, Benchmarking and Certification.
21. Nguyen Duc, Anh & Jabangwe, Ronald & Paul, Pangkaj & Abrahamsson, Pekka. (2017). Security challenges in IoT development: a software engineering perspective. 1-5. 10.1145/3120459.3120471.
22. Krichen M., Lahami M., Cheikhrouhou O., Alroobaea R., Maâlej A.J. (2020) Security Testing of Internet of Things for Smart City Applications: A Formal Approach. In: Mehmood R., See S., Katib I., Chlamtac I. (eds) Smart Infrastructure and Applications. EAI/Springer Innovations in Communication and Computing. Springer, Cham. <https://doi.org/10.1007/978-3-030-13705-2_26>
23. B. Jeannotte and A. Tekeoglu, "Artorias: IoT Security Testing Framework," 2019 26th International Conference on Telecommunications (ICT), 2019, pp. 233-237, doi: 10.1109/ICT.2019.8798846.
24. Yu, Miao, Jianwei Zhuge, Ming Cao, Zhiwei Shi, and Lin Jiang. 2020. "A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices" *Future Internet* 12, no. 2: 27. <https://doi.org/10.3390/fi12020027>
25. Lally G., Sgandurra D. (2018) Towards a Framework for Testing the Security of IoT Devices Consistently. In: Saracino A., Mori P. (eds) Emerging Technologies for Authorization and Authentication. ETAA 2018. Lecture Notes in Computer Science, vol 11263. Springer, Cham. <https://doi.org/10.1007/978-3-030-04372-8_8>
26. Khujamatov, Halim; Reypnazarov, Ernazar; and Lazarev, Amir (2021) "MODERN METHODS OF TESTING AND INFORMATION SECURITY PROBLEMS IN IoT," Bulletin of TUIT: Management and Communication Technologies: Vol. 4 , Article 4.
27. M. A. Jamil, M. Arif, N. S. A. Abubakar and A. Ahmad, "Software Testing Techniques: A Literature Review," 2016 6th International Conference on Information and Communication Technology for The Muslim World (ICT4M), 2016, pp. 177-182, doi: 10.1109/ICT4M.2016.045.
28. S. N. Matheu, J. L. Hernández-Ramos, S. Pérez and A. F. Skarmeta, "Extending MUD Profiles Through an Automated IoT Security Testing Methodology," in IEEE Access, vol. 7, pp. 149444-149463, 2019, doi: 10.1109/ACCESS.2019.2947157.
29. A. Azmoodeh, A. Dehghantanha, and K.-K. R. Choo, “Robust Malware Detection for Internet Of (Battlefield) Things Devices Using Deep Eigenspace Learning,” IEEE Trans. Sustain. Comput., pp. 1–1, 2018.
30. N. Milosevic, A. Dehghantanha, and K.-K. R. Choo, “Machine learning aided Android malware classification,” Comput. Electr. Eng., vol. 61, 2017.
31. G. Epiphaniou, P. Karadimas, D. K. B. Ismail, H. Al-Khateeb, A. Dehghantanha, and K. R. Choo, “Non-Reciprocity Compensation Combined with Turbo Codes for Secret Key Generation in Vehicular Ad Hoc Social IoT Networks,” IEEE Internet Things J., 2017.
32. G. Mcgraw, “Software security,” IEEE Secur. Priv. Mag., vol. 2, no. 2, pp. 80–83, Mar. 2004.
33. A. Azmoodeh, A. Dehghantanha, M. Conti, and K.-K. R. Choo, “Detecting crypto-ransomware in IoT networks based on energy consumption footprint,” J. Ambient Intell. Humaniz. Comput., pp. 1–12, Aug. 2017.
34. S. Walker-Roberts, M. Hammoudeh, and A. Dehghantanha, “A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure,” IEEE Access, 2018.
35. System vulnerability is a deficiency in the implementation of an application, which could be an implementation flaw or a design flaw that enables an attacker to inflict harm on the end user of the application and gain extra privileges (Owasp 2015)
36. Stewart, H. (2021), "The hindrance of cloud computing acceptance within the financial sectors in Germany", Information and Computer Security, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/ICS-01-2021-0002