Bucharest University of Economic Studies
Economic Informatics Doctoral School

HABILITATION THESIS

Using Security Analysis to Enhance
Internet of Things Solutions and Security of Mobile and Embedded Platforms

Candidate
Assoc. Prof. Marius POPA, PhD

Bucharest 2023

Summary

Industry 5.0 changes the role of the industry in society by addressing the current social and environment challenges with priority over the traditional approaches centered on efficiency and productivity. According to [8], Industry 5.0 complements the 4.0 one by adding benefits for employees and for society as results of:

- Increase the professionalism through evolved skills and training programs for employees.
- Implementation of circular production models to preserve the natural resources.
- Providing solutions to climate change.

In order to get those benefits, Industry 5.0 implies the development of research and innovation programs. According to European Commission, a digital Europe is one of the priorities to implement Industry 5.0 as [8] states. Therefore, use of digital technologies should aim:

- Well-being of the employees.
- Enhancement of employee digital skills.
- Social prosperity.

Businesses are still mostly engaged in Industry 4.0 or not event there. Approach of Industry 5.0 is still at strategical level, but there are some ways to highlight or even to demonstrate practically how that approach could look like by analyzing, investigating and touching applications proposed for the future industry.

Use of ICT (Information and Communication Technologies) knowledge and tools is a key element to get to Industry 5.0. COVID-19 pandemic has demonstrated the role of digital technology to protect employees and ensure business continuity by remote work and collaboration platforms. Materializing the benefits of Industry 5.0 will be possible on the strength of ICT and digital transformations to be done.

The thesis contains three sections with the main topic of ICT security challenges and solutions for Internet of Things (IoT) in particular to prepare implementation of the next industry version as Industry 5.0:

1. Use of Internet of Things to reveal possible applications for Industry 5.0.
2. Security issues, challenges and approaches in Internet of Things.
3. Providing security quality during the software development life cycle for a secure program coding in particular.

The common element of those three sections is security addressed both low level during the software engineering processes, and high level for various architectures and platforms.

Chapter 2 presents several solutions in the scope of Industry 5.0 as implementations for air pollution, e-voting and remote control of different devices or vehicles. The ICT knowledge and tools are used to design, develop and deploy the proposed solutions as well as security challenges

associated to those applications. The security implementations take into consideration existing guidelines, best practices and standards to ensure reliability and robustness to the proposed solutions.

The paper [5] centers on solving or mitigating the health threatening risks related to air pollution within cities. A possible real-time pollution monitoring system is investigated and a proof of concept (PoC) is designed and implemented to provide real-time countermeasures based on predictive analytics. The PoC interprets and analyzes data collected from the monitoring system deployed as IoT infrastructure. Also, the proposed solution could be integrated with existing systems to take the most appropriate decisions to reduce the air pollution to the safe thresholds. This way, the cities become smart by real-time behavior adapted to existing environmental conditions.

The author's research contributions to this topic include the following:

- Investigations regarding the air pollution affects the urban areas and population.
- Investigations of actual ICT solutions used to mitigate the air pollution causes and effects.
- Researches over the characteristic of being a "smart city" in the context of air pollution.
- Researches about the critical technologies and platforms to be used for developing a pollution monitoring ICT based solution.
- Researches related to air pollution metrics and how they are used within a smart city infrastructure.
- Defining the proposed solution architecture based on findings of actual technologies and platforms, and the targeted metrics to be used for the qualitative analysis.
- Processing and interpretation of gathered data from the proposed solution in order to effectively use the city resources.
- Analysis and interpretation of data collected from real deployed sensors and analytical comparisons performed at different times for the same date sources.

Solution proposed in [7] contributes to social stability by offering to all citizens to be part of a participatory governance model. In addition, this kind of application is used as support for making decisions within various organizations. The implementation challenges are significant regarding the voter's anonymity and end-to-end security. The proposed PoC uses a distributed and decentralized IoT infrastructure based on blind signatures and blockchain technology to implement a particular voting system.

The author's research contributions aim the following aspects:

- Analysis of existing electronic vote systems.
- Methodology of developing an ICT based solution for voting.
- Analysis of the actual cryptographic schemes being the most appropriate to be included into an electronic vote solution.
- Designing of some PoC features based on analysis of existing systems.
- Partial software development of electronic vote PoC.
- Validation of PoC by checking the functionalities, resource requirements and data synchronization throughout PoC components at both hardware and software levels.

Use of Artificial Intelligence (AI) as part of implementation of Industry 5.0 is highlighted by the paper [6]. Two PoCs are developed to get the benefits of Machine Learning (ML) technology used for IoT embedded device as particular way to design, implement and deploy Edge ML. There are several constraints and limitations regarding the IoT embedded devices to be addressed when an Edge ML-based system is developed. The PoCs refer to the following application fields:

- Edge ML-based tele-operated robot to identify the gas leaks.
- Unmanned Aerial Vehicles/Drones with Edge ML inference deployed on them for visual computing operations.

Development of such system is iterative and the most appropriate version is selected based on target performance.

In the scope of [215], the author’s research contributions are related to:

- Methodology of applying the machine learning in automated decisions and visual computing processes developed within IoT embedded devices, robots or UAVs/drones.
- Investigations over existing solutions for applying AI within IoT and UAV platforms.
- Defining requirements based on analysis performed over existing solutions.
- Validation of proposed machine learning models.
- Performance analysis of AI based learning models.

Chapter 3 highlights various security solutions applied in IoT infrastructures. The power of IoT consists of huge number of devices staying connected all the time. Security in IoT is a big challenge because of connected device number and large amounts of data sent through different communication channels and protocols. IoT devices use different hardware, chipsets, operating systems and firmware, and different protocols, communication layers, users and developers that introduce potential security issues. Besides those, still there is uncertainty about security best practices and the associated costs within IoT field. Therefore, there is no security solution fits any IoT deployment because the security risks are less well-known. Rich data collected from IoT infrastructures provides enhancements of employee’s work and life.

The paper [1] analyzes the main IoT communication protocols with Cloud infrastructures to potential security risks. Besides IoT infrastructure itself, there are other security issue sources like IoT communication protocols, the Web of Data and the access to Cloud Services. An improper IoT infrastructure deployment will lead to significant security flaws within organization. Choosing the right IoT infrastructure together with associated computing platforms is a complex process depending on financial resources allocated for that and the targeted security level. Current knowledge about IoT security introduces potential security risks due to some hidden issues or particular approaches even though the IoT infrastructure has been designed and implemented as being a robust one.

The author’s research contributions address the following points:

- Investigations of actual security challenges within an IoT infrastructure and the risks exposed to the running environments by this kind of platforms.
- Investigations over the actual security risks introduced by the communication protocols used in IoT infrastructures.

- Addressing the IoT security challenges by choosing and tuning the appropriate communication protocols for ensuring a minimal targeted security in an IoT infrastructure.
- Analyzing the complexity of an IoT infrastructure as a factor introduces new security challenges.

Payment security issues and possible solutions implemented for financial transactions are presented in [3]. The proposed architecture and implementation materialize the advantages in terms of payment security by using Oracle based technologies (e.g Java Card) blended with robust and confirmed standards provided by professional and commercial organizations (e.g EMVCo, Global Platform) and blockchain technology deployed on various hardware architectures. The paper passes through the security challenges of e-payment system implementation and offers solutions to be applied in mobile applications.

The author's research contributions to smart card based payment transaction security aim the following list:

- Investigations over actual smart card based systems having various purposes and not limited to payments.
- Investigations over different types of smart card based transactions and possible security vulnerabilities introduced by those ones.
- Analyzing ways to secure the payment transactions by using different data authentication mechanisms.
- Analyzing the robustness of existing technologies to be used for development of smart card based systems.
- Designing and implementation of components for a smart card based payment system uses the blockchain technology.

A PoC as a mobile application is provided by [11] to highlight ways of collecting and usage of valuable data related to insurance activity for market intelligence research and technical implementations. The content involves hardware and software components specific to the automotive industry to be integrated into an IoT infrastructure for collecting real-time car specific data. The security challenges are significant because the access to the car data and the control of it must be restricted to authorized parties only.

The author's research contributions related to connected cars aim the following elements:

- Investigations over the car located data monitoring and communication.
- Investigations over actual hardware and software specialized for access to car data.
- Analysis of technical opportunities for different businesses to use data collected by a car in order to optimize the operational costs of a car fleet.
- Designing the PoC architecture and functional components of a mobile application for car data management within an IoT Cloud infrastructure.
- Opening new development of future directions by adding AI components in the proposed PoC architecture.

Chapter 4 highlights the knowledge and tools needed to implement reliable and secure solutions similar to the ones presented in chapters 2 and 3. A defective solution implementation is the main cause of vulnerabilities coming from solution design, hardware and software components with security risks, communication channels, or lacks of software development as security flaws especially. A bug list becomes a vulnerability list because every time somebody wants to exploit the bugs to get software insights. Chapter 4 focuses on software engineering because the software quality sets the software security. Secure coding standards and software development principles encourage the software developers to follow a common set of rules and guidelines to improve the software quality. The software quality approach operates on two levels:

- Methods and techniques to have such a software engineering process leading to high software quality.
- Define indicators to evaluate both engineering process and software quality.

The paper [9] offers the framework to define metrics for quality of development tools or structured containers like the source code files. Some analysis are performed for orthogonality evaluation based on orthogonality measurement system. The results are used to catch possible security coding issues or to improve the quality of used utilities and tools during the software development.

The author's research contributions within system development of data quality assessment:

- Investigations over data storage containers defined as structured entities.
- Defining data quality attributes managed as structured entities.
- Identifying the key characteristics of the aggregation based metrics included into orthogonality assessment of the structured entities.
- Defining the scope of the orthogonality assessment system within the software development life cycle.
- Defining the orthogonality metrics of data stored by source code files as structured entities.
- Validation of orthogonality assessment system by analyzing the experimental results have been got for several scenarios.

Software developers who apply the best practices and coding principles over the solution requirements determine the increasing the software quality. Evaluation and improvement of the developers' technical skills are presented in [2]. Usually, a more experienced software developer adds more complexity and security to the implementation. The challenge is to enhance the human resource by transferring as soon as possible the expertise of the more experienced developers to the beginner ones. The paper presents how this software engineering education is done starting from the university studies of the future IT specialists.

The author's research contributions related to actual impact of the Industry 4.0 over the knowledge transfer cover the following aspects:

- Investigations over the impact of actual ICT knowledge and tools to the software engineering education.
- Sampling the most relevant source code indicators for assessment of code quality.
- Defining the source code assessment system by considering some constraints derived from software engineering education particularities.

- Analyzing the impact of the assessment system over the actual educational activities carried out within ICT field.

The paper [10] has a more focus on security requirements of software development process. Software developers have to be aware and to pay attention on security vulnerabilities accidentally added during the solution or program coding. The paper highlights the best practices and coding principles to be followed for an increased software security quality. In addition, it provides some starting examples where those coding techniques are applied.

The author’s research contributions in the field of source code security regard the following elements:

- Investigations over the security requirements during the software development.
- Analyzing the actual best practices regarding inclusion of source code security features into a software application.
- Providing source code vulnerabilities for software uncompliant to security, and methods and technique to solve these security risks.
- Ways to improve the software quality by eliminating vulnerabilities during the software development life cycle.

A more complex view about coding quality is provided by the paper [4]. In actual deployments, the stack of used technologies is quite large and the solution coding must adapt to the infrastructure and rules of those technologies. The solution architecture is heterogeneous and different components and technologies must be synchronized. An implementation of a secure communication channel is provided as example at the industrial level.

The author’s research contributions to coding quality result from:

- Investigations over actual ICT trends in the scope of Industry 4.0.
- Analyzing the requirements of Industry 4.0 to be implemented into an IoT solution for a very specialized industry having particular information and technological approaches.
- Defining the IoT based solution prototype architecture with many particularities regarding the technical equipment and challenging production environment.
- Providing security improvements to the proposed solution to improve the communication between physical production equipment and production specific data managed by an ioT Cloud infrastructure.
- Defining the security methodology to target the solution security as much as possible together with effective data management related to the production activities.
- Implementations related to the proposed solution security to proof the feasibility.

The above research topics improve skills, experiences, knowledge and processes within areas such as education, research and innovation, and professional skills and competencies improvements.

Regarding the education area, the technological transfer is improved by continuous update of the teaching topics, using actual electronic teaching resources, stimulating the students’ feedback and the teaching process transparency, activating learning and stimulating the academic climate.

Research, innovation and technology transfer involve building strong relationships among different research and development interdisciplinary teams in order to facilitate the technology transfer in different areas interested in applying the research results. Participation within highest academic degree programs like PhD stages ensures increasing of human resource quality in ITC field.

Professional knowledge and skills are improved by following high quality of academic degrees and professional training programs based on curricula according to the new market trends and technologies implemented by the industry.

All above points contribute to professional development ensuring a high quality of the professional background and technical skills expected by the ITC industry.

References

[1] Alin ZAMFIROIU, Bogdan IANCU, Cătălin BOJA, Tiberiu GEORGESCU, Cosmin CARTAS, Marius POPA, Cristian TOMA, *IoT Communication Security Issues for Companies: Challenges, Protocols and The Web of Data*, Proceedings of the International Conference on Business Excellence, Vol. 14, Issue 1, 2020, pp. 1109–1120, WOS 000556549000104, EISSN 2558-9652, https://doi.org/10.2478/picbe-2020-0104

[2] Cătălin BOJA, Mădălina ZURINI, Marius POPA, Cristian TOMA, *Code Quality Metrics Evaluation Platform in Software Engineering Education*, Proceedings of the 16th International Conference on Informatics in Economy (IE 2017), 2017, ASE Publishing House, Bucharest, pp. 283 – 290, WOS 000418463600046, ISSN 2284-7472, ISSN-L 2247-1480

[3] Cristian TOMA, Marius POPA, *EMV/Bitcoin Payment Transactions and Dynamic Data Authentication With Smart Java Cards*, Proceedings of the 14th International Conference on Informatics in Economy (IE 2015) – Section 3: Mobile-Embedded and Multimedia Solutions, 2015, ASE Publishing House, Bucharest, pp. 141 – 151, WOS 000362796900024, ISSN 2284-7472, ISSN-L 2247-1480

[4] Cristian TOMA, Marius POPA, *IoT Security Approaches in Oil & Gas Solution Industry 4.0*, Informatica Economica, Vol. 22, Issue 3, 2018, pp. 46 - 61, ISSN:1453-1305

[5] Cristian TOMA, Marius POPA, Alin ZAMFIROIU, Andrei ALEXANDRU, *IoT Solution for Smart Cities' Pollution Monitoring and the Security Challenges*, Sensors, Vol. 19, Issue 15, 2019, Article Number 3401, WOS 000483198900156, ISSN 1424-8220, https://doi.org/10.3390/s19153401

[6] Cristian TOMA, Marius POPA, Bogdan IANCU, Mihai DOINEA, Andreea PASCU, Filip IOAN-DUTESCU, *Edge Machine Learning for the Automated Decision and Visual Computing of the Robots, IoT Embedded Devices or UAV-Drones*, Electronics, Vol. 11, Issue 21, 2022, Article Number 3507, WOS 000883410100001, EISSN 2079-9292, https://doi.org/10.3390/electronics11213507

[7] Cristian TOMA, Marius POPA, Cătălin BOJA, Cristian CIUREA, Mihai DOINEA, *Secure and Anonymous Voting D-App with IoT Embedded Device Using Blockchain Technology*, Electronics 2022, Vol. 11, Issue 12, Article Number 1895, WOS 000818504700001, EISSN 2079-9292, https://doi.org/10.3390/electronics11121895

[8] Industry 5.0, European Commission, available on-line https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/industry-50_en

[9] Ion IVAN, Daniel MILODIN, Marius POPA, *Orthogonality Metrics of the Structured Entities*, Proceedings of the Romanian Academy, Series A: Mathematics, Physics, Technical Sciences, Information Science, vol. 11, Issue 3, 2010, pp. 269 – 276, WOS 000208624600011, ISSN 1454-9069

[10] Marius POPA, *Security Characteristics of the Program Coding*, Conference Proceedings – The 11th International Conference on Informatics in Economy – Section: Audit and Project Management, 2012, ASE Publishing House, Bucharest, pp. 211 – 215, WOS 000313136800040, ISSN 2284-7472, ISSN-L 2247-1480

[11] Marius POPA, Cosmin CARTAS, *OBD2 IoT Device Proof of Concept for the Insurance Companies Connected Cars*, Proceedings of the 15th International Conference on Informatics in Economy (IE 2016) – Section 2: Mobile-Embedded and Multimedia Solutions, 2016, ASE Publishing House, Bucharest, pp. 103 – 107, WOS 000386192300017, ISSN 2284-7472, ISSN-L 2247-1480