A logo with a blue and white design

Description automatically generated with medium confidence

Academy of Economic Studies, Bucharest

Information Security Masters

An analysis of IT systems in financial institutions

dissertation

Coordinator Graduate

Prof. Univ. Dr. Cristian-Eugen CIUREA Cristian-Mihail DUMITRESCU

Bucharest 2024

Declaration regarding the originality of the content and assumption of responsibility

Through my presence, I declare that the presented results in my work are my own results except for the case where I refer to other authors. I confirm the fact that any material use from different sources (magazines, books, and websites) are as clearly as possible referenced in the dissertation and are indicated in the bibliographic references.

Contents

[**Chapter 1 – Introduction.** 1](#_Toc167042671)

[**Chapter 2 – The general structure of a financial institution’s IT system.** 2](#_Toc167042672)

[Chapter 2.1 – Structure of the critical internal systems. 2](#_Toc167042673)

[Chapter 2.2 – Ways most clients of a financial institution interact with it. 3](#_Toc167042674)

[Chapter 2.3 – Ways most employees of a financial institution interact with it. 3](#_Toc167042675)

[**Chapter 3 – Literature review of security in financial institutions.** 5](#_Toc167042676)

[Chapter 3.1 – Physical security. 5](#_Toc167042677)

[Chapter 3.2 – Network security. 6](#_Toc167042678)

[Chapter 3.3 – Software security. 6](#_Toc167042679)

[**Chapter 4 – Study and survey about trust in software data security.** 8](#_Toc167042680)

[Chapter 4.1 – Results and discussion. 9](#_Toc167042681)

[Chapter 4.2 – Research conclusion. 12](#_Toc167042682)

[**Chapter 4 – Types of possible attacks?** 13](#_Toc167042683)

[Chapter 4.1 – Third-party software and hardware security problems 13](#_Toc167042684)

[Chapter 4.2 – API problems 13](#_Toc167042685)

[**Chapter 5 – Prevention and mitigation of attacks?** 13](#_Toc167042686)

[Chapter 5.1 – Prevention and mitigation of third-party software and hardware security problems 13](#_Toc167042687)

[Chapter 5.2 – Prevention and mitigation of API problems 13](#_Toc167042688)

[**Chapter 6 – Conclusion** 13](#_Toc167042689)

[**Bibliography** 13](#_Toc167042690)

[**Annexa 1 – Figure list** 13](#_Toc167042691)

[**Annex 2 – Acronym list** 13](#_Toc167042692)

# **Chapter 1 – Introduction.**

As the title suggests, this paper presents, with examples, the possible security problems that may arise when designing, configuring, and using IT infrastructure, especially software in a financial institution.

The first thing that this paper wants to clarify is the definition of “Financial institution”: The United Stated Government through the Financial Crimes Enforcement Network [1] defines a financial institution as any person (as in individual, business, partnership, trust, or estate) doing business in one or more of the following capacities:

1. Bank
2. Broker or dealer in securities
3. Money services business
4. Telegraphy company
5. Casino
6. Card club
7. A person subject to supervision by any state or federal bank supervisory authority

For the context of this paper, I will be referring to financial institution as a business that has the capacity of a bank, a broker/dealer in securities or a money services business.

The structure of the dissertation goes as follows: presenting the general structure of a financial institution from the perspective of a bank, exposing the possible weak points of the structure from an IT perspective, and presenting possible fixes for those problems. The study will be accompanied by a project posted in the following repository: ”<https://github.com/lieautman/Dissertation>”, which will showcase a possible solution to software problems.

There are two types of threat actors: insider and outsider threats. While the outsider threat seems like a more dangerous problem, at first glance, the insider threat has received a lot of attention and is cited as a very serious problem in many studies, such as in the "Insider Threats in Cyber Security" [2].

The insider threat is very prevalent because most insiders by their role in the system may have already be in a position where some security systems are already bypassed and in the worst-case scenario, the systems now rendered useless may be relied upon when designing the rest of the security. Take for example this article [3], in which it is said that employees of Tesla entrusted with certain data, misappropriated the information to a German news outlet.

The insider problem is solved with proper background checks for all parties involved in the IT system and with proper training, these types of security problems can be reduced to a minimum.

The outsider threat is solved with well implemented security systems and protocols.

By implementing proper training within the organization, some outsider threats such as “phishing” and “malware” are neutralized.

This paper aims to study the trust of the every-day individual for the security of the systems of banks, and the care of the developers that work on them, from the security standpoint.

# **Chapter 2 – The general structure of a financial institution’s IT system.**

In this opening chapter, the paper will discuss the structure of the financial institution that it will analyze from a security perspective. It will be taking a top-down perspective, from the design of the systems to the outward facing capillaries.

## Chapter 2.1 – Structure of the critical internal systems.

In this subchapter, I will be describing the internal structure of the critical internal systems of a financial institution, mostly Databases and Networks.

Databases are a critical piece of any infrastructure. For financial institutions, reputation plays a big role in their business. Thus, client data must always be kept safe. A good rule, for any organization, is to have backups online and offline, as well as onsite and offsite. Since this paper tackles financial organizations such as banks, data stored is of high value to the institution. Such data shall always be as protected as possible. Keeping backups will lead to an easier recovery in case of emergency. They also allow for minimization of risk.

When deciding on what database to use for any organization, there are a few questions they need to ask themselves: what kind of database do we want? – structured or unstructured, SQL or non-SQL; what is the expected support for such a database? – making a contract with the creators of the database or just using a very popular database that will not be out of support soon; and what are the particular advantages of using a certain database? – some databases allow faster writes or faster reads, other databases allow greater data security through versioning and many other features.

Cloud databases may help with the security since they may implement automated backups and scalability. At the same time, they have two inherent disadvantages: the data must travel through an unsecure tunnel, the internet, which has its own solutions such as VPN’s [(annex 2)](#_Annex_2_–) and the data is now in the possession of a third party that may or may not be trusted.

Networks and their management are another key component to any organization. Having proper security on any level of the iso/osi model [4] is of upmost importance. Because most software assumes a high level of security within the organization network, incidents may arise because of network mismanagement.

When dealing with sensitive data, not only the access points, but the mode of transfer must also be secure. A secure network is not only maintained and guarded physically; it also must be maintained logically.

When discussing physical security, we can talk about maintaining proper procedures for entering restricted areas and maintaining the equipment.

On the other hand, logical security of a network has many components. There are passive security solutions such as honeypots and canaries. There are active security solutions such as intrusion detection systems.

There can also be layers of security, in the form of DMZ’s [5] [(annex 2)](#_Annex_2_–), with ever-more restrictive firewall rules. And Virtual LAN [6] solutions that will lead to a more secure network.

## Chapter 2.2 – Ways most clients of a financial institution interact with it.

As the title suggests, this subchapter will take on the task of presenting the ways in which clients can interact with the IT systems of financial institutions.

There are three main systems that are interfacing with the client of a financial institution. There is proprietary hardware facing the client, such as ATMs [(annex 2)](#_Annex_2_–) and POSs [(annex 2)](#_Annex_2_–), there is proprietary software such as websites of said financial institution and there are third party software and hardware facing the client such as network equipment in a subsidiary.

--talk about hardware facing clients such as atms – the atms and pos-es have failsafes and are monitored (ATMs are attached to a subsidiary with security personnel nearby, and pos-es should have self-destruct and monitoring measures to ensure safety.)

--talk about websites facing clients

--talk about networks facing clients (such as Wi-Fi in subsidiaries)

## Chapter 2.3 – Ways most employees of a financial institution interact with it.

Although IBM X-Force Threat Intelligence Index 2024 [7] at page 9 say the phishing attacks have come down, it reflects the continued adoption of phishing mitigation techniques. In 2016, the same research said that almost 60% of the attacks come from within a company.

To mitigate this kind of problem, there must exist protocols and training.

--protocols and training in relation to this

--talk about following protocols and training

--talk about data safety through training

--talk about accont safety through training

---make callbacks to ISO and network for dummies + audit

# **Chapter 3 – Literature review of security in financial institutions.**

The subject of security in financial institutions, especially in banks, is not a new one. There has been extensive research done to analyze and help prevent robberies and theft on any level. Some of the crime has therefore moved from the institution towards the end user, as described in the conclusion of "Banking information resource cybersecurity system modeling." [8].

The security of banking apps has therefore become a great priority, as presented by "Cybersecurity in Banking and Financial Sector: Security Analysis of a Mobile Banking Application" [9]. This paper does not focus on the user side of the equation when it comes to apps, because it is near impossible to keep the app safe, users having the ability to do as they please with their devices and data. It will discuss the API security challenges faced by the institution.

There are enough factors that top management in banks, as well as the public must understand and what should be assessed such as the ones in the conclusion of Assessing the Factors of Cybersecurity, Awareness in the Banking Sector" [10]. As the recommendations of the paper suggest, proper support and budgeting of the cybersecurity teams is a must.

The physical security and network security are also important as stated by This study about "Bank Robberies and Physical Security in Switzerland" [11] and "Security Issues on Banking Systems" [12].

## Chapter 3.1 – Physical security.

Before all the information systems and all the training required to operate them safely, the only issue that existed was physical security. In the current day and age, the physical security of a system may be overlooked when analyzing it.

The preventative measure of physical security cannot be overstated. This study about "Bank Robberies and Physical Security in Switzerland" [11] on the effectiveness of physical security on bank robberies in Switzerland, in chapter 2 and 3 emphasizes the preventive effect of physical security. The study shows that the number of attacks does not necessarily reduce, but the effectiveness does. This idea can also be applied to network and software security as well.

There are many design choices that go into the construction of a physically secure place. The book "Effective Physical Security" [13] presents some of those concepts that are important even in the context of IT security. Of all the design issues discussed there, for the context give, there are some of underlining importance:

In the chapter 3 about physical design, there is a quote about the level traffic influencing the level of crime negatively, quote of Schlomo Angel, in 1968 [14]. The author adds that the physical design may allow crime to arise through the lack of potential witnesses while providing enough victims.

This knowledge can be used when designing the physical circumstances of an information system. These circumstances should be designed with the four-eyes principle in mind.

Chapter 7, under Use of locks and in chapter 11 Access control systems and Identification badges, describe ways in which space can be separated with the use of authentication/identification. A lack of authentication at the physical level can lead to unauthorized access to information systems which can lead to a security breach.

All the issues presented above become critical when neglected. They may impact the security of any IT system if a vulnerability is found and exploited, or if the infrastructure associated becomes vulnerable to a physical attack, at network or application levels.

## Chapter 3.2 – Network security.

Physical security being established, the information transportation security can start being discussed. The chapter not only discusses transport layers, and transport equipment, but also about safety on the user machine.

This book about “Network Infrastructure Security” [15] by Angus Wong describes a lot of the attacks that may appear on a nonsecure network.

According to a study on "Evaluation of Computer and Network Security Strategies: A Case study of Nigerian Banks" [16] , in chapter 3.5, 37% of correspondents noticed some attacks and 15% experienced often attacks on their respective bank’s equipment or network. In the same publication, there are some ways to prevent and avoid attacks. The use of well implemented password management, antiviruses, firewall solutions and the use of intrusion detection or intrusion prevention systems are great ways of stopping most network attacks.

This [17] security report from the NSA-National Security Agency outlines a lot of network changes that are required to operate a network secured. Besides the changes outlined above, the report dabbles into virtual private networks, virtual local area networks, ports, proxies, and many other necessary points of interest for the security of the network.

## Chapter 3.3 – Software security.

With the mode of transport established and secured, the discussion can now move towards the software applications that run on the established infrastructure. The applications can either be made in-house or be outsourced, but all of them must have a certain level of security so no negative impact is dealt to the institution.

The cost of cybersecurity breaches in the form of software exploits or “hacks” are high, as presented in "The economic cost of cybersecurity breaches: A broad-based analysis" [18] conclusion. The paper also suggests that the software problems may affect more than the attacked entity.

Database security is at the limit between system administration and application development. The database must be secured, and the applications must be able to modify data unimpeded. This “Database Security—Concepts” [19] describes, in chapter 5, about the challenges of databases in the context of cloud.

Beside those, there are challenges about the way accounts and groups are set up in the way for apps to work properly and securely.

No SQL databases may be of help on the development side, but they are also vulnerable to such attacks, but also some of their own issues, as highlighted in the 4’th chapter of "Security Issues in NoSQL Databases" [20].

For the rest of the paper, an API is the interface between two applications, except for databases. The applications in question can be either monolith or microservice architecture in nature [21].

Over time, APIs evolved and gathered more and more importance, as described in the first 4 chapter of "Cyber Security in API Economy – Issues and Challenges" [22]. As such, the importance of their security increased.

There are many attacks that can happen at an API’s level. The “API Security in Action” [23] by N. Madden presents a big catalogue of attacks that are suitable for general purpose API’s, such as injection attacks, cross site scripting attacks and ways to prevent them through proper input validation.

The security issues of the API’s are problematic in the internal applications of the bank, but also in the external facing facilities such as ATMs and banking apps. "Understanding Security APIs" [24] describes in chapter 2 the development of security in such facilities and some attacks in chapter 3.

# **Chapter 4 – Study and survey about trust in software data security.**

Based on the literature review of this paper, the consensus is that all systems of a bank must be monitored and protected to ensure data integrity and a functional business model.

In the case of physical and network security, although not easy, the way of conducting checks on it is more transparent than in the case of software. Software often comes from a third party which restricts access to its codebase, for business-related reasons. The surveys described below aim to test the trust or distrust of the every-day person about banking software systems and for the care of developers, in the financial sector or not, for their work, from the security perspective. For such a task, there were designed a couple of surveys destined to either of the groups (every-day people and developers) to see their opinions on the subject. The surveys may be treated separately, with the results coupled together to paint a greater picture of the perceived security of the software systems.

1. The public, every-day person survey has the following question:

* Have you ever considered data protection in your life?
* Do you feel like you are a person prone to having your personal data stolen?
* Have you taken any steps to protect your data?
* Do you feel like the bank you use is protecting your data properly?
* Do you feel like your bank has a good interest in protecting your data?

2. The developer survey has the following questions and possible answers:

* Do you research security issues for the languages and apps you currently use?
* Are you involved in discussions about the level of security of the apps you develop?
* Are you interested in the security of the applications you create?
* Are you interested in the security of data for the applications you develop?

All with the following possible answers: Yes, No and Somewhat

At the end, both surveys have a section where the person has to rete their own familiarity in some security subjects:

* SQL injections
* CORS attacks
* XSS attacks
* Adware
* Spyware
* Session hijacking
* DOS/DDOS attacks
* Buffer overflow attacks
* Code injection attacks
* Impersonation

With the following possible answers:

* Unfamiliar
* Somewhat unfamiliar
* Neutral
* Somewhat familiar
* Familiar.

The population for the public questionnaire was a mixture of people from urban cities of Romania. The people surveyed had a lot of contact with banking systems and had used the services.

The population for the developer questionnaire consisted of people working as developers at different companies in Bucharest and that have finished a bachelor’s in the IT field or a master.

The public questionnaire should highlight the uninformed public opinion of the banking system for data privacy and safety, while the developer questionnaire describes the interest or disinterest in the subject of software security of the people that make it.

The restrictions and limitations of the research are given by the sample location of the survey. The problems outlined in the “Results and discussion” section may be just local problems to the surveyed region. Another possible problem may be that the developers surveyed are not necessarily working in the banking sector, so the results may not be totally representative of that sector.

## Chapter 4.1 – Results and discussion.

Based on the survey proposed above, the data shows a good interest from the public towards their own data protection and a high trust in the security of the banking system, which was to be expected, since everyday people expect reputable institutions.

A high percentage of the surveyed individuals have considered data protection and have taken steps to protect their own data with moderate success as shown in figure 1.

Figure 1:
Have you ever considered data protection in your life?
Yes: 78.9%
Somewhat: 15.8%
No: 5.3%
Do you feel like you are a person prone to having your personal data stolen?
Yes: 31.6%
Somewhat: 36.8%
No: 31.6%
Have you taken any steps to protect your data?
Yes: 52.6%
Somewhat: 31.6%
No: 15.8%

Fig. 1 Response percentages to the first 3 questions of the public survey

Figure 1 represents the data distribution for the answer of the first three questions of the public survey.

The next two questions in the public survey refer to the trust of the public in their own banking provider’s ability and desire to provide data protection for them. The answer percentages are displayed in figure 2 and display a high trust in the banking systems.

Figure 2:
Do you feel like the bank you use is protecting your data properly?
Yes: 52.6%
Somewhat:  36.8%
No: 10.5%
Do you feel like your bank has good interest in protecting your data?
Yes: 57.9%
Somewhat: 31.6%
No: 10.5%

Fig. 2 Response percentages for questions 4 and 5 of the public survey

Another good point of interest of the survey is the familiarity of the everyday person with concepts from the software security sphere of influence.

The data for this part of the survey suggests that a few everyday people were interested in some areas of security as shown in figure 3. Particularly, the area of interest consisted of mostly non-technical and broader subjects such as “Adware”, “Spyware” and “Impersonation”.

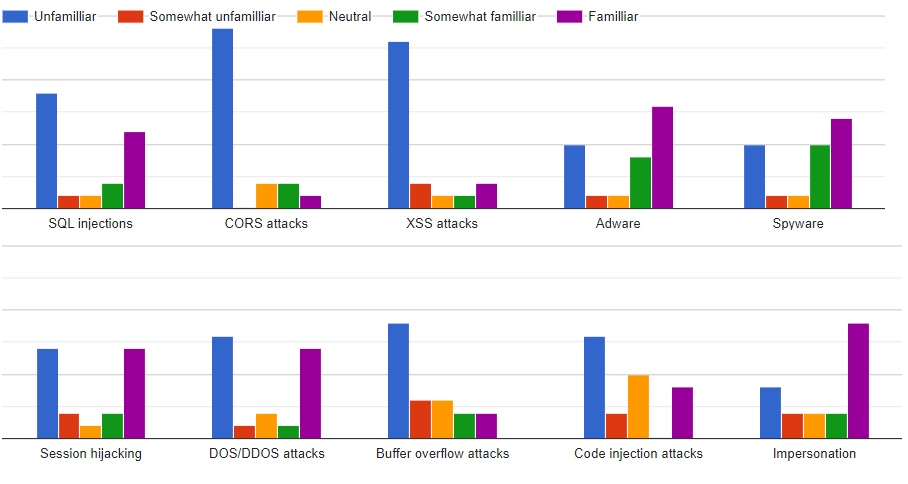


Fig. 3 Response distributions to the familiarity part of the public survey

The survey presents developers as motivated individuals with an interest in the security of the application they are developing and that are personally involved in the security level of the applications they make.

In figure 4, there are the answers to the first two questions of the developer questionnaire.

A pie chart with numbers

Description automatically generated

Fig. 4 Response percentages to the first 2 questions of the developer survey

The graphs show that developers are involved in the development of the security features of their applications, but that they mostly lack the drive to do research in this area.

The third and fourth questions, displayed in figure 5, also show that developers are interested in the security of their applications and the safety of their data.

A blue circle with a number of triangles

Description automatically generated

Fig. 5 Response percentages to the third and fourth questions of the developer survey

The interest, but lack of action determined by the first, third and fourth questions, show that developers may need help with resources about the security of the code they implement.

The last part of the survey is shown below, in figure 6. It shows that developers have more familiarity with technical subjects than the everyday person. The familiarity of them with the more mediatized subjects such as “Adware”, “Spyware” and “Impersonation” is like the general public’s.

A graph of different colored bars

Description automatically generated

Fig.6 Response distributions to the familiarity part of the developer survey

## Chapter 4.2 – Research conclusion.

As stated in the "Customers’ perception of cybersecurity threats toward e-banking adoption and retention: A conceptual study. In ICCWS 2020 15th International Conference on Cyber Warfare and Security (Vol. 270)"’s [25] conclusion, the cybersecurity threats have an impact on the customer’s decision when it comes to banking services. In this regard, the current opinion according to the survey shows good trust in the banking’s security features for software. The study can also be considered a check for "Risk Assessment of Computer Network Security in Banks" [26]’s conclusion with a public opinion survey and about software security, where the author advises banks to enhance their computer system security.

A possible remedy to the problem of developers not researching possible security issues for the systems they design would be a raise in awareness about the possible problems that may arise or the tightening of requirements for development positions.

The raise of awareness can be made by having better documentation of packages that treat security issues, better training or even an AI [(annex 2)](#_Annex_2_–) implementation that detects possible problems and warns developers, such as Copilot [27].

# **Chapter 6 – Conclusion**

-- Add conclusion

# **Bibliography**

|  |  |
| --- | --- |
| [1] | USA Gov, "financial-institution-definition," 01 01 2024. [Online]. Available: https://www.fincen.gov/financial-institution-definition. [Accessed 1 1 2024]. |
| [2] | J. H. M. B. D. G. Christian W. Probst, "Insider Threats in Cyber Security," Springer, Lyngby, Denmark, 2010. |
| [3] | D. B. Johnson, "Tesla says former employees leaked thousands of personal records to German news outlet," SC Media, 2023. |
| [4] | International Organization for Standardization, ISO/IEC 7498-1:1994, Geneva: International Organization for Standardization, 1994. |
| [5] | Department of Homeland Security USA, "Archive of "Control System Security DMZ"," Department of Homeland Security USA, 9 May 2020. [Online]. Available: https://web.archive.org/web/20200609134629/https://www.us-cert.gov/ics/Control\_System\_Security\_DMZ-Definition.html. [Accessed 2 February 2024]. |
| [6] | IEEE, "802.1Q-1998 - IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks," IEEE, 1 1 1998. [Online]. Available: https://ieeexplore.ieee.org/document/753056. [Accessed 24 2 2024]. |
| [7] | IBM, "IBM X-Force Threat Intelligence Index 2024," IBM, 1 1 2024. [Online]. Available: https://www.ibm.com/account/reg/us-en/signup?formid=urx-52629. [Accessed 25 2 2024]. |
| [8] | O. Y. I. K. M. M. I. &. N. V. Shulha, "Banking information resource cybersecurity system modeling.," Journal of Open Innovation: Technology, Market, and Complexity 8.2, Kyiv, Ukraine, 2022. |
| [9] | D. F. M. M. A. R. P. M. Biswajit Panja, "Cybersecurity in Banking and Financial Sector: Security Analysis of a Mobile Banking Application," IEEE, Flint, MI, USA; Ypsilanti, MI, USA, 2013. |
| [10] | A. I. A.-A. a. S. A. Al-Bassam, "Assessing The Factors of Cybersecurity, Awareness in the Banking Sector," -, Riffa, Bahrain, 2021. |
| [11] | C. Grandjean, "Bank Robberies and Physical Security in Switzerland," Butterworth Publishers, Lausanne, Switzerland, 1990. |
| [12] | R. V. R. L. Y. B. T. S. F. Mohd Khairul Affendy Ahmad, "Security Issues on Banking Systems," Universiti Malaysia Sabah, Kota Kinabalu, Malaysia, 2010. |
| [13] | L. J. Fennelly, "Effective Physical Security," Todd Green, Amsterdam, Holand, 2017. |
| [14] | S. Angel, "Discouraging crime through city planning," University of California Press, Berkeley, California, 1968. |
| [15] | A. Y. Angus Wong, Network Infrastructure Security, Hong Kong, PR, China: Springer, 2009. |
| [16] | Z. O. F. S. O. A. O. B. Ogunwobi, "Evaluation of Computer and Network Security Strategies: A Case study of Nigerian Banks," CoRI, Ibadan, Nigeria, 2016. |
| [17] | Cybersecurity Technical Report, "Network Infrastructure Security Guide," National Security Agency, United States, 2023. |
| [18] | K. K. R. P. T. S. Jacob Haislip, "The economic cost of cybersecurity breaches: A broad-based analysis," Workshop on the economics of information security (WEIS). Vol. 9., New York, New York, USA, 2019. |
| [19] | A. a. C. Database Security—Concepts, "Elisa Bertino, Ravi Sandhu," IEEE, 2005. |
| [20] | N. G.-O. Y. G. E. G. J. A. Lior Okman, "Security Issues in NoSQL Databases," IEEE, Changsha, China, 2012. |
| [21] | A. O. a. A. P. G. Blinowski, "Monolithic vs. Microservice Architecture: A Performance and Scalability Evaluation," IEEE Access, vol. 10, 2022. |
| [22] | S. V. Lakshmi Iyer, "Cyber Security in API Economy – Issues and Challenges," INCCOCE, Bengaluru, India, 2016. |
| [23] | N. Madden, API Security in Action, Manning, 2020. |
| [24] | M. K. Bond, "Understanding Security APIs," University of Cambridge, Cambridge, UK, 2004. |
| [25] | A. B. K. M. A. C. M. &. D. R. Jibril, "Customers’ perception of cybersecurity threats toward e-banking adoption and retention: A conceptual study. In ICCWS 2020 15th International Conference on Cyber Warfare and Security (Vol. 270)," Academic Conferences and publishing limited, Zlin, Czech Republic, 2020. |
| [26] | A. K. Singha, "Risk Assessment of Computer Network Security in Banks," IJRDO Journal, Delhi, India, 2017. |
| [27] | Microsoft, "GitHub Copilot in VS Code," Microsoft, 05 02 2024. [Online]. Available: https://code.visualstudio.com/docs/copilot/overview. [Accessed 26 05 2025]. |
| [28] | I. S. P. S. Erez Yallon, "OWASP API Security Top 10," 2023. [Online]. Available: https://owasp.org/API-Security/editions/2023/en/0x11-t10/. [Accessed 13 01 2024]. |

# **Annexa 1 – Figure list**

# **Annex 2 – Acronym list**

|  |  |
| --- | --- |
| *API* | Application Programming Interface |
| *DB* | Data Base |
| *TCP* | Transmission Control Protocol |
| *LAN* | Local Area Network |
| *SQL* | Structured Query Language (database type/language) |
| *DMZ* | De-Militarized Zone |
| *VPN* | Virtual Private Network |
| *AI* | Artificial Intelligence |
| *ATM* | Automated Teller Machine |
| *POS* | Point Of Sale |