

PLANNING

ESCUELA POLITÉCNICA NACIONAL



David Fabián Cevallos Salas

José Antonio Estrada Jiménez

Danny Santiago Guamán Loachamín

CONTENT INDEX

1	GOAL, RESEARCH QUESTIONS AND SEARCH STRING	4
1.1	Topic	4
1.2	Goal	4
1.3	Research Questions	4
1.4	Search string	5
2	CRITERIA FOR AUTOMATED INCLUSION – EXCLUSION PROCEDURE.....	9
2.1	Criteria for Inclusion	9
2.2	Criteria for Exclusion	9
3	CRITERIA AND PROCEDURE FOR MANUAL INCLUSION - EXCLUSION	10
3.1	General.....	10
3.1.1	Goal	10
3.1.2	General instructions	10
3.1.3	Inclusion criteria	10
3.1.4	Exclusion criteria.....	11
3.1.5	Possible mark options	11
3.2	Screening stage.....	11
3.2.1	Pilot Phase	12
3.2.2	Main Phase	12
3.3	Procedure for screening each paper	13
3.4	Decision trees	14
4	CODEBOOK FOR INFORMATION EXTRACTION AND CODING.....	16
4.1	Research Questions	16
4.2	Data to be extracted	17
4.3	Classification for coding	18
4.3.1	Types of Application layer protocols.....	20
4.3.2	Approaches to security provision	20
4.3.3	Security Information Goals	21
4.3.4	Types of attacks	22
4.3.5	Types of Controls	24
4.3.6	Broad domains.....	25
4.4	Coding procedure	26
4.4.1	Setting up necessary materials	26

4.4.2	Coding execution	26
4.4.3	Meeting of the coders to review results	27
4.5	General Coding validation	27

FIGURES INDEX

Figure 1	Main keywords for search string	6
Figure 2	Results using the keyword security	8
Figure 3	Results using the keywords security and protocol	8
Figure 4	Results using all the keywords	8
Figure 5	Decision tree Pilot Phase	15
Figure 6	Decision tree Main Phase	16
Figure 7	Classification scheme	19

TABLEX INDEX

Table 1	Main keywords	6
Table 2	Keywords and related terms	7
Table 3	Numbers of results applied by keyword combinations	7
Table 4	Automatic Information to be extracted	17
Table 5	Fields for extracting manual information	18
Table 6	Generalities of Types of Application Layer protocols category	20
Table 8	Descriptions of Approaches to security provision subcategories	20
Table 7	Generalities of Approaches to security provision category	20
Table 8	Descriptions of Approaches to security provision subcategories	21
Table 9	Generalities of Security Information goals category	21
Table 10	Descriptions of Security Information goals Subcategory	22
Table 11	Generalities of Types of attacks category	22
Table 12	Descriptions of Types of attacks category	23
Table 13	Generalities of Types of controls Category	24
Table 14	Descriptions of Types of controls subcategories	25
Table 15	Generalities of Broad domains category	25
Table 16	Descriptions of Broad domains subcategories	26

PLANNING

1 GOAL, RESEARCH QUESTIONS AND SEARCH STRING

1.1 Topic

Application Layer Security for Internet Communications: A Comprehensive Review, Challenges, and Future Trends

1.2 Goal

To identify contributions related to Application layer security for Internet communications, along with its associated security goals, types of attacks, types of controls, and domains of application.

1.3 Research Questions

The following research questions have been established:

RQ1: What are the current contributions aimed at securing the Application layer for Internet communications?

Reasoning

Considering the extensive attack surface of the Application layer, several contributions have been made to enhance its security. Contributions made by researchers aim to mitigate threats that cannot be addressed at lower layers of the TCP/IP architecture.

RQ2: What approaches are employed to provide security at the Application layer for Internet communications?

Reasoning

The complexity of threats encountered by the Application layer implies that, in certain scenarios, security cannot be solely ensured by the protocol itself. Consequently, some contributions have explored solutions where security is not confined to the protocol but involves external components working over it, or a combination of both.

RQ3: What security goals are pursued when securing the Application layer for Internet communications?

Reasoning

Each security objective aims to address a specific security gap. No single contribution can comprehensively and holistically cover all security gaps.

RQ4: What types of attacks have been identified when securing the Application layer for Internet communications?

Reasoning

Any technology presents weaknesses in its design or mode of operation that attackers can exploit. Moreover, the Application layer is particularly vulnerable due to its complexity, wide range of implementation technology, and close connection to software and end-user activity. Identifying the types of attacks that the Application layer faces in Internet communications will help pinpoint the weaknesses that researchers have attempted to address with their contributions.

RQ5: What types of controls have been applied to address the lack of security at the Application layer for Internet communications?

Reasoning

The diverse array of threats confronting the Application layer has led to the proposal of several controls to mitigate the associated risks. However, these controls do not operate uniformly or serve the same purpose. Identifying the types of controls suggested by contributions and the specific purposes for which they were designed enables us to comprehend the current state of Application layer security for Internet communications.

RQ6: In what broad domains is Application layer security for Internet communications employed?

Reasoning

Application layer security plays a fundamental role in various domains that operate over the Internet. Although discerning each specific domain is a complicated task due to the advancement of technology and domain overlapping, identifying the broad domains of application will contribute to a better understanding of the research's significance and its practical applications. Moreover, it aids in identifying gaps that existing literature needs to address.

1.4 Search string

In order to establish the search string three main keywords have been identified:

- Security
- Application layer
- Protocol

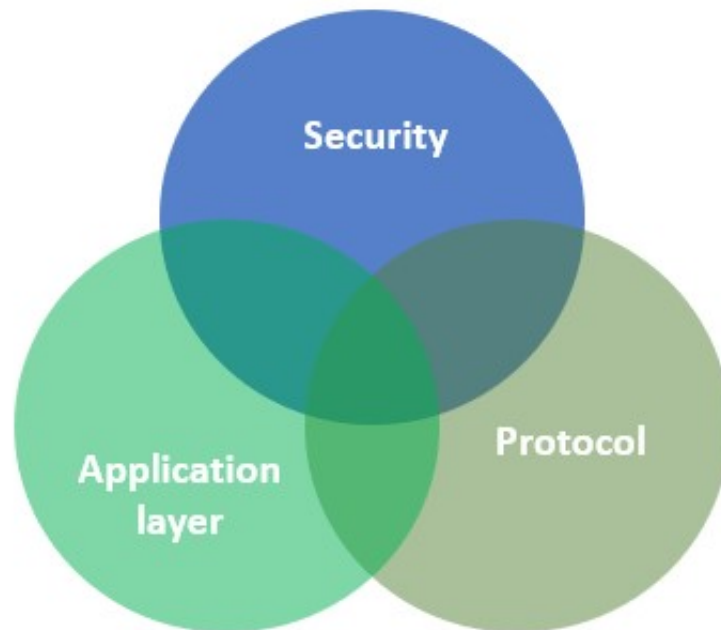


Figure 1 Main keywords for search string

Keyword	Related terms
Security	Computer security
	Secure
Application layer	Data layer
Protocol [1]	Data communication
	Communication protocol
	Communication systems
	Transit
	Connectivity

Table 1 Main keywords



Also, the following terms have been defined as possible keywords:

Possible Keyword	Related terms
Computing	Computer
Mobile	Mobility
Tenet	Principle
Vulnerability	Weakness
	Vulnerable
Control [2]	Countermeasure

Table 2 Keywords and related terms

The following search string have defined:

secur*
AND ((application W/3 layer*) OR (data* W/3 layer*))
AND ((protocol*) OR (data* W/3 communication*) OR (communication* W/3 protocol*) OR
(communication* W/3 system*) OR transist* OR mechanism* OR connect*)

-  security
-  application layer
-  protocol

The following results are obtained on February 17th, 2024, using the search string defined:

Keywords	Number of results
Security	1,272,749
Security + application layer	5,608
Security + application layer + protocol	3,159

Table 3 Numbers of results applied by keyword combinations

Security



Figure 2 Results using the keyword security

Security + application layer

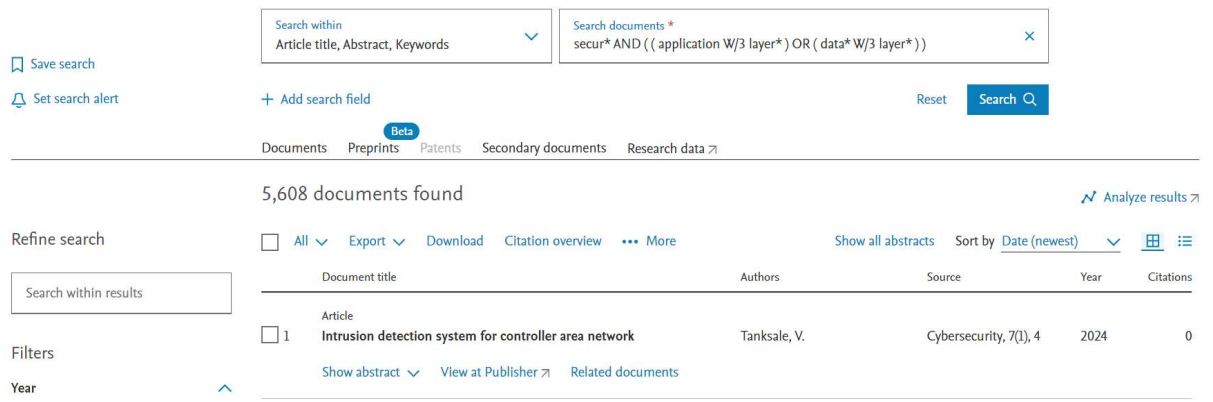


Figure 3 Results using the keywords security and protocol

Security + application layer + protocol

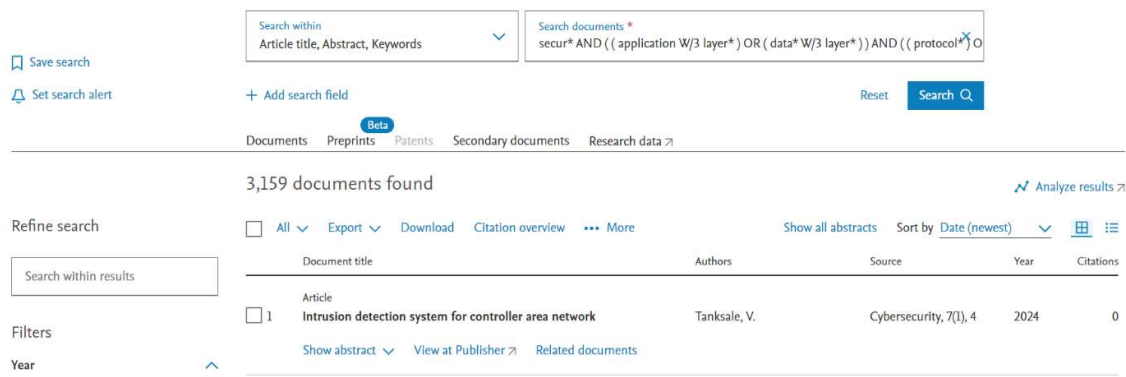


Figure 4 Results using all the keywords

2 CRITERIA FOR AUTOMATED INCLUSION – EXCLUSION PROCEDURE

The next points expose the automated inclusion and exclusion criteria that will be applied using Scopus, Web of Science and IEEE Xplore search engines.

2.1 Criteria for Inclusion

Due to the nature of the research in an engineering field, the next inclusion criteria have been established:

- **Language:** English or Spanish.

In fact, several paper and academic work written in Spanish has demonstrated to be of relevance in the fields of Security and Protocols.

- **Document type:** Conference Paper or Journal.

Conference paper will allow to determine the new pragmatic solutions in the fields, as long as journal paper will contribute with means for analyzing pragmatic and theoretical solutions.

- **Research field:** Computer Science, Engineering or Mathematics.

Research topic in strong relationship with the fields of Computer Science and Networking such as Web Programming or IoT could be included in the general Engineering field.

2.2 Criteria for Exclusion

The exclusion criteria are deduced directly from the inclusion criteria.

- **Language:** Papers not written in English nor Spanish will be discarded.
- **Document type:** If the material falls under an category different of Conference paper or Journal will be discarded. The book chapters found will be kept in order to acquire knowledge.

- **Research field:** Overall, if the field of knowledge is not Computer Science , Engineering or Mathematics the paper must be discarded.

3 CRITERIA AND PROCEDURE FOR MANUAL INCLUSION - EXCLUSION

3.1 General

3.1.1 Goal

To discard the papers obtained from the search phase that are not suitable for the purpose of the research.

3.1.2 General instructions

- The research group will be composed of the main researcher and the director. Possibly, the research group will be completed with one codirector.
- A pilot with a limit of 1% of the papers resulted from the search phased will be constituted. The inclusion and exclusion criteria will be applied over the pilot and the following iterations.
- The Krippendorff's Alpha index [2] will be used in order to establish the level of consensus between the research group members. A index of at least 0,80 has been establish as a minimum threshold for consensus between the opinions.

3.1.3 Inclusion criteria

The papers must comply with the following criteria:

- The paper is a primary contribution. Secondary contributions must be kept for analysis and acquire new ideas, but will be discarded.
- The paper contribution is related with protocols or mechanisms able to establish a communication between elements in a network.
- The paper presents a solution at the application layer.
 - Work in other layers such as transport, network, data link, physical and others is not included.
- The paper contribution depicts a work in Information Security and it can be related with at least one Information Security goal.
 - Aspects such reliability and performance are not included.
- A proof that allows to corroborate the procedure or technique used by the solution presented must be clearly identified in the paper.

Note: At this stage it will not be considered as an inclusion/exclusion criterion the percentile rank of the Thomson Reuters Indicators due to the possible reduced number of papers to obtain. However, if in the execution phase is considered necessary, this criterion also will be applied according to the results obtained.

3.1.4 Exclusion criteria

Based on the inclusion criteria, the following exclusion criteria have been defined:

- The paper is a secondary or tertiary contribution. But remember to keep and analyze the secondary contributions.
- The paper is not related to a protocol of a mechanism able to establish a communication between elements in a network.
- The paper presents a solution in a layer different than the application level.
- The paper contribution is not in the field of Information Security or cannot be related to an Information Security goal.
- The paper does not present a proof of validation of the procedure or technique used for the contribution.

3.1.5 Possible mark options

[I] The paper fulfills the inclusion criteria and none of the exclusion criteria.

[S] The paper fulfills the inclusion criteria but it is a secondary contribution. The paper is kept but is discarded.

[E] The paper does not fulfill with at least one inclusion criteria or fulfills with at least one exclusion criteria. So, the paper is discarded.

[U] A dilemma has been created of the paper analysis. So, it must be treated and discussed in depth later by the research group.

3.2 Screening stage

In order to get the main papers for the research and achieve consensus between the researcher group members, the screening stage has been divided in two phases: a pilot phase and the main phase.

3.2.1 Pilot Phase

In the pilot phase a sample of 1% the papers will be chosen randomly. Each of the papers will be analyzed, through the inclusion and exclusion criteria, for each of the research group members.

For this phase, execute Title, Abstract and Full paper screening stages. At each stage the papers some will be ruling them out and other included. Just the included and Unclear papers will be taken in the next stage.

After each stage, a Krippendorff's Alpha index of at least **0,80** must be achieved to establish a line of consensus between the members.

If the index is not achieved in the first iteration, the process will be repeated through several discussions between the research group member until achieve the desired index.

The pilot phase main goal is to unify the research criteria between the member of the research group.

3.2.2 Main Phase

The remained papers that not conformed the pilot phase will be considered in the main phase. This phase has as goal to obtain the final set of the papers for the research.

The main phase establishes the following procedure:

- **Step 1:** Firstly, each member of the research group will read just the **Title** of a group of papers individually. Under his or her understanding will classify each paper as **Included**, **Excluded** or **Unclear**.
If the paper is a secondary locate it as included in this first step.

- **Step 2:** Secondly, each member of the research group will read individually the **Title and Abstract** of the paper classified by himself or herself as Included or Unclear in the first step. Each of these analyzed papers will be then classified by the researcher as **Included**, **Excluded** or **Unclear** category.
If the paper is a secondary locate it as included in this second step.

- **Step 3:** Finally, each member of the research group will read individually the **Full paper** in order to classify each one as Included or Unclear in the second step.

Under his or her understanding, the researcher will classify each paper in the **Included**, **Excluded** category..

If the paper presents a secondary contribution fulfilling all the other inclusion criteria, it will be located in the **Secondary** group for review in order to acquire knowledge but it will be discarded.

In this step is important that the researcher takes a final decision due to the lack of subsequent iterations.

Together with the results of the other members of the research group the Krippendorff's Alpha index is calculated. Any discrepancies will be discussed and analyzed in work meetings.

3.3 Procedure for screening each paper

Depending of the phase (pilot or main) each defined section of the paper must be read carefully.

Step 1: While reading is important to take into consideration the following terms:

- **Protocol** and its related terms: communication, transmission, transit, connectivity
- **Security** and its related terms: Security Information Tenet.
- **Application layer** and its related terms: rules, top layer, mechanism.
- **Vulnerability** and its related terms: weakness, risk, exploit.
- **Control** and its related terms: countermeasures.
- **Goal:** objective, problem, dilemma.

These terms have been taken from the IEEE Thesaurus.

For Title, Abstract and Full Paper screening respond the following questions:

Step 2: Primary contribution

Question: In general terms, does the title **reflect** a primary or secondary research work in **security or protocols**?

- If **no**, mark the paper as Excluded a go to the next paper.
- If **yes** or **unclear**, being a primary contribution, continue to the following step.

Step 3: Application layer protocol related

Question: Is the **goal** of the paper to enhance the **security** of **application layer protocols** for data communication?

- If **no**, mark the paper as Excluded a go to the next paper.
- If **yes** or **unclear**, continue to the following step.

Step 4: Security goal and Proof of validation

Question: Can the work presented in the paper be **related** to a **security goal** in order to protect data communications through the use **application layer protocols** and a **proof of validation** of the procedure or technique used is presented?

- If yes but the contribution is secondary, mark it as **Secondary** in order to review it and acquire new knowledge, but the paper is discarded for the extraction and coding process.
- Select **yes**, **no**.

3.4 Decision trees

The following pictures depicts the decision trees procedures.

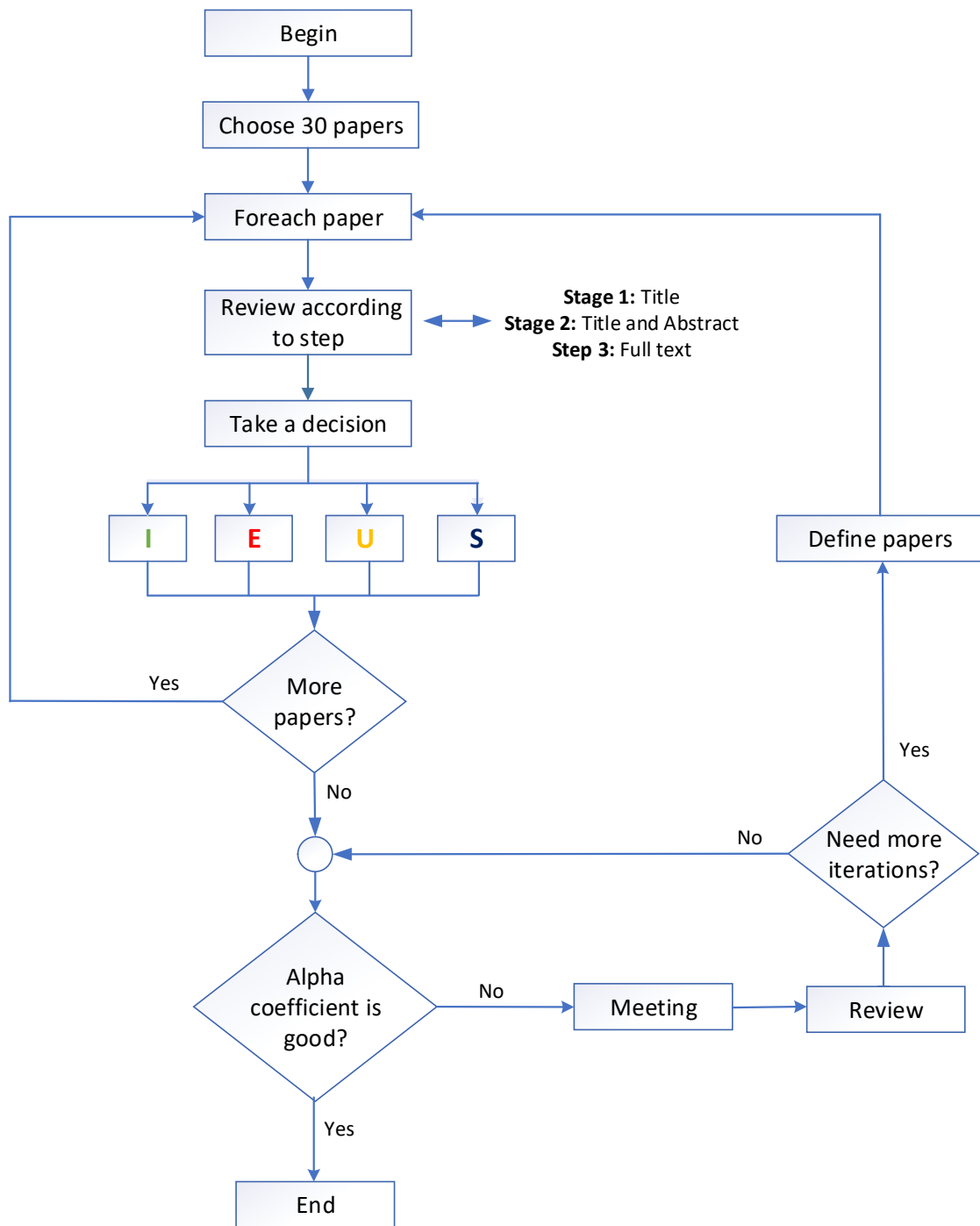


Figure 5 Decision tree Pilot Phase

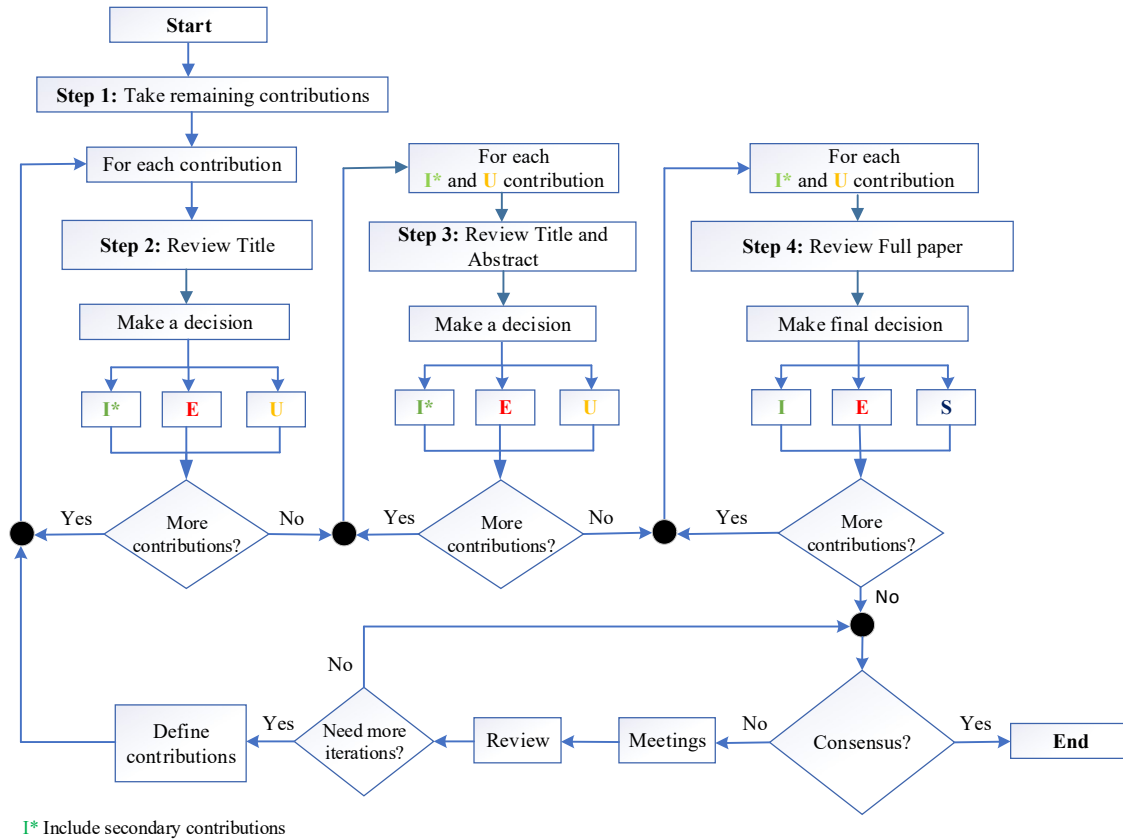


Figure 6 Decision tree Main Phase

4 CODEBOOK FOR INFORMATION EXTRACTION AND CODING

This document has as goal to present the information to be extracted from the papers after the application of the inclusion and exclusion criteria, the procedure for extracting that information and the classification scheme to be used to achieved this goal.

4.1 Research Questions

The following research questions which guide the process were defined:

- **RQ1 – Types of Application layer protocols:** What are the current contributions aimed at securing the Application layer for Internet communications?
- **RQ2 – Approaches to security provision:** What approaches are employed to provide security at the Application layer for Internet communications?
- **RQ3 – Security goals:** What security goals are pursued when securing the Application layer for Internet communications?

- **RQ4 – Types of attacks:** What types of attacks have been identified when securing the Application layer for Internet communications?
- **RQ5 –Types of controls:** What types of controls have been applied to address the lack of security at the Application layer for Internet communications?
- **RQ6 – Broad domains:** In what broad domains is Application layer security for Internet communications employed?

4.2 Data to be extracted

In order to respond to the research questions established, automatic and manual information will be extracted from the papers.

Automatic information will be extracted according to the fields explained in Table 4.

Table 4 Automatic Information to be extracted

	Field	Detail
General Information	Authors	Authors names
	ID	CADIMA Identifier
Useful Information	Year	Year of publication
	Document type	Journal or Conference
	Citation key	Key for citing the paper
	Publisher	Publisher(s) of the paper
	Journal or conference name	Name of the conference if it applies
	Affiliations	Affiliations researches belong to

Information will be extracted manually according to the details shown in Table 5.

Table 5 Fields for extracting manual information

	Title		Detail
Compulsory	Abstract		Resume of the paper. Identify the goal and the problem.
	Introduction		Corroborates what was stated in the introduction and broadens the concepts
	Conclusion		Identify the conclusion achieved by the researcher(s).
Optional	Methodology		The procedure used in order to make the contribution.
	Discussion and Analysis		Review the figures and the results obtained identifying the technique used.

The extracted information will be used for coding the paper according to the coding procedure explained in this document.

4.3 Classification for coding

In order to mark and classify and mark the paper the following classification schema has been defined.

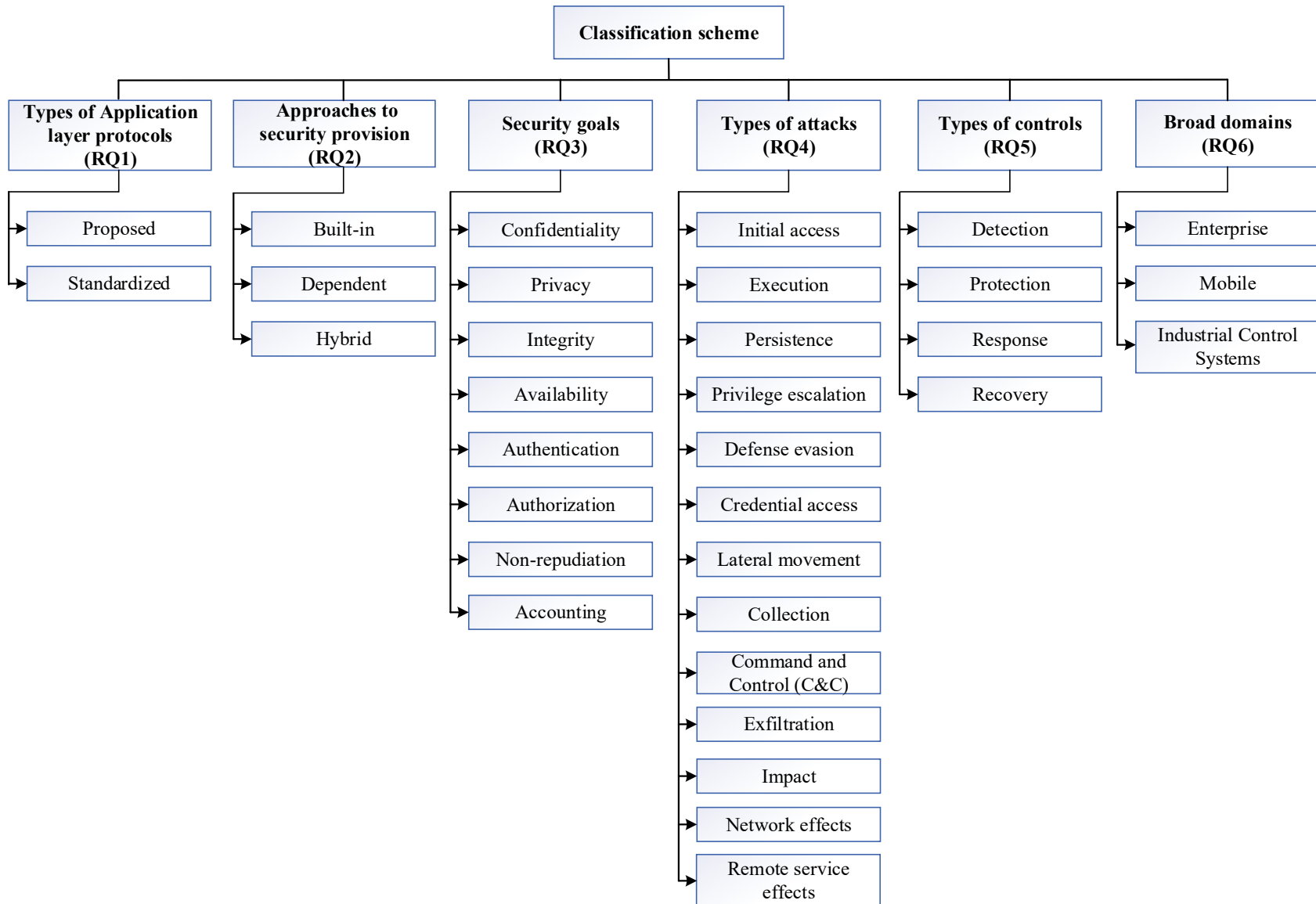


Figure 7 Classification scheme

4.3.1 Types of Application layer protocols

Under this category will be identified and located the different secured Application layer protocols found in the articles.

Table 6 Generalities of Types of Application Layer protocols category

Descriptor	Detail
Related Research Question	RQ1
Baseline Classification	Industry classification
Total of categories	2

Table 7 Descriptions of Approaches to security provision subcategories

Subcategory	Description
Proposed	It comprises a new proposed protocol
Standardized	It comprises a widely accepted protocol by the industry

4.3.2 Approaches to security provision

This category describes the approaches to security provision used by the contributions in order to apply the different types of controls to mitigate vulnerabilities.

4.3.2.1 Generalities

Table 8 Generalities of Approaches to security provision category

Descriptor	Detail
Related Research Question	RQ4
Baseline Classification	NIST SP 800-123 [3] NIST SP 800-160 (v1r1) [4]
Total of categories	3

4.3.2.2 Descriptions

Table 9 Descriptions of Approaches to security provision subcategories

Subcategory	Description
Built-in secure	The protocol is able to provide security through its own capabilities inherent to its structure or mode of operation. If a contribution proposes a new communication protocol, it can provide security without relying on other entities. If the contribution is based on a standardized protocol, it will seek an enhanced version capable of providing security independently. For instance, an Application layer protocol able to encrypt its payload before transmission, thereby preventing eavesdropping, provides a level of security through a built-in approach.
Dependent	Security for the Application layer and the protocol relies on external entities, such as Layer 7 firewalls, middlewares, frameworks, proxies, or methodologies, regardless of whether the protocol is proposed or standardized. For example, a proxy between the sender and the target able to encrypt the insecure messages of the Application layer protocol before reaching the public communication channel provides security through a dependent approach.
Hybrid	It combines the two previous approaches. The contribution offers a certain level of security through the same Application layer protocol and employs other entities to complement the achieved security level. For instance, a solution where the Application layer protocol dynamically defines the private keys and algorithms to be used in the communication, whereas a proxy is used for encrypting the messages with the defined parameters, provides security in a Hybrid approach.

4.3.3 Security Information Goals

4.3.3.1 Generalities

Table 10 Generalities of Security Information goals category

Descriptor	Detail
Related Research Question	RQ1
Baseline Classification	ISO 27001 [5] ISO 27002 [6] ISO 27005 [7]
Total of categories	8

4.3.3.2 Descriptions

Table 11 Descriptions of Security Information goals Subcategory

Subcategory	Description
Confidentiality	This goal seeks to safeguard the secrecy of the message by making it accessible only to authorized entities.
Privacy	It Seeks to protect personal data when using digital services.
Integrity	It understands the mechanisms necessary to guarantee that a message has not been tampered or modified.
Availability	It intends that the resources are available for the entities whenever they require them.
Authentication	This goal is achieved when the Application layer protocol allows to give access to an entity previously validating that the entity is what it says to be.
Authorization	Once an entity is given access to a system, an authorization goal is achieved when the entity operates and performs the action that it was just allowed to do.
Non-repudiation	This goal asserts that the source of the message of the Application layer protocol cannot deny that it was sent by itself.
Auditory	It intends to generate log messages or implement monitoring mechanisms to be able to keep track of the events that occurred and the entities that caused them.

4.3.4 Types of attacks

This category depicts the classification of the weaknesses found in the design, architecture and other features of the secure application layer protocols.

4.3.4.1 Generalities

Table 12 Generalities of Types of attacks category

Descriptor	Detail
Related Research Question	RQ2
Baseline Classification	MITRE Attack [8]
Total of categories	13

4.3.4.2 Descriptions

Table 13 Descriptions of Types of attacks category

Subcategory	Description
Initial access	The attacker aims to achieve the first access to the victim station by exploiting vulnerabilities in the Application layer used for the communication. A common example of this is an attack that mimics the Hello message required by the Application layer protocol, thereby gaining initial access to the target.
Execution	The vulnerability in the Application layer protocol allows for the delivery and execution of malicious code on the victim station. For instance, an Application layer protocol capable of embedding malicious code into its payload and running it on the target is a significant example.
Persistence	The attacker seeks to establish a constant connection to the victim station taking advantage of the flaws of the Application layer protocol. For instance, an attack might seek to transport a backdoor through the Application layer protocol in order to achieve constant access to the target.
Privilege scalation	The attacker seeks to attain higher-level access or permissions than those already achieved through exploiting weaknesses at the Application layer. An attack oriented towards exploiting software bugs through the Application layer protocol to gain more rights at the target is a common example.
Defense evasion	The attacker seeks to evade security mechanisms such as firewalls, <i>Intrusion Detection Systems</i> (IDS) and <i>Intrusion Prevention Systems</i> (IPS). For instance, malware can split it into several chunks taking advantage that the Application layer protocol is not aware of this evasion technique in order to avoid edge and host security.
Credential access	The attacker seeks to steal access credentials through deficiencies in the Application layer protocol. For instance, a cookie hijacking attack aims to steal passwords and personal data of users who access websites.
Discovery	The attack seeks to gather reconnaissance on topologies, entities, and other useful information for the attacker. For instance, the attacker might analyze the information provided by the headers of the Application layer protocol used for communication.
Lateral movement	The attack exploits weaknesses in the Application layer to move from the victim station to its neighbors. For example, a vulnerability in an Application layer protocol that allows

	for worm replication is a significant lateral movement attack.
Collection	The Application layer protocol enables the attacker to gather information through eavesdropping. A common example is a Man-in-the-Middle (MiTM) attack.
Command and Control (C&C)	The threat is controlled by the attacker through a C&C workstation. For instance, the attacker might exploit the redirection mechanisms allowed by the Application layer protocol to transmit C&C sequences and direct the attack according to the objectives pursued.
Exfiltration	The attacker can steal information by exploiting weaknesses in the Application layer protocol used in the communication. An example involves an attacker violating the Application layer protocol to transmit information to the attacker. This type of attack can also be viewed as a specific C&C attack that pursues to steal information.
Impact	Exploiting flaws in the Application layer protocol, the attack can destroy information, architectures, and even physical resources. For example, SQL injection attacks may be used for information destruction.
Network effects	Exploiting a vulnerability in the application layer protocol, the attack aims to cause damage to the target or the network, primarily by preventing service availability. Major representatives of this category include DoS or DDoS attacks, for example.
Remote service effects	The attacker exploits flaws in the Application layer protocol to establish a remote connection to the victim station or its neighbors. This attack can also be considered as the initial step in a lateral movement attack. An example involves the theft of Telnet sessions by exploiting vulnerabilities specific to this protocol.

4.3.5 Types of Controls

The subcategories of types of controls are described within this category.

4.3.5.1 Generalities

Table 14 Generalities of Types of controls Category

Descriptor	Detail
Related Research Question	RQ3
Baseline Classification	NIST Cybersecurity Framework [9]
Total of categories	4

4.3.5.2 Descriptions

Table 15 Descriptions of Types of controls subcategories

Subcategory	Description
Detection	This type of control can identify and generate alerts for other systems to implement additional countermeasures. For instance, if the control suggests a solution that can trigger an alarm upon detecting malware in the payload of the Application layer protocol, it is defined as a detection control.
Protection	This category includes controls designed to take preventive action before an attack occurs, following a proactive security approach. An example of such a control is encryption, which safeguards information from being stolen in an insecure communication channel by a Man-in-the-Middle (MiTM) attack.
Response	This category encompasses controls designed to respond when a vulnerability has been exploited, aiming to mitigate its impact and halt it at early stages. For example, if a DDoS attack is detected, the Application layer protocol might automatically reduce its volume of traffic to prevent a complete service outage.
Recovery	After damage has occurred, controls within this category contribute to resilience. For instance, an Application layer protocol that can identify malware in its payload after transmission has taken place could partially mitigate the effects of such an attack by providing details on the attack trajectory.

4.3.6 Broad domains

A broad domains classification is defined within this category.

4.3.6.1 Generalities

Table 16 Generalities of Broad domains category

Descriptor	Detail
Related Research Question	RQ5
Baseline Classification	MITRE domains [8]
Total of categories	3

4.3.6.2 Descriptions

Table 17 Descriptions of Broad domains subcategories

Subcategory	Description
Enterprise	This broad domain comprises all communication environments that does not involve mobility. For instance, cloud computing and web communications are inside this domain.
Mobile	This domain is related to all the pervasive and wireless environments, independently of its technology. Smart phones, IoT and ubiquitous systems are part of this broad domain.
Industrial Control Systems	This domain encompasses all devices, systems, networks, and controls used to operate or automate industrial processes. Examples include applications related to smart meters, traffic light systems, gas pipelines, among others. Additionally, <i>Industrial Internet of Things (IIoT)</i> and <i>Supervisory Control and Data Acquisition (SCADA)</i> domains fall within this category [10].

4.4 Coding procedure

In general, the coding procedure will be carried out in three steps which must be followed in order to classify each paper.

The process will be carried out by each coder and the results will be reviewed in meeting until reach the Alpha Krippendorff's coefficient [2].

4.4.1 Setting up necessary materials

First and foremost, the materials used for the coding phase must be prepared. These materials are:

- This codebook.
- Alpha Krippendorff's coefficient calculator.
- Software tools: Mendeley and Publish and Perish, or similar.
- Software tool for registering marking results: Cadima.

4.4.2 Coding execution

The execution process must be applied to each one of papers and for each one of the coders.

The execution process for each paper is the following:

- Extract the automatic information of the paper in order to identify it.
- Read the compulsory fields in order to extract information to classify the paper.
The proof of validation established in the Inclusion and Exclusion criteria must be considered as a baseline.
If the paper does not present a Conclusion section, try to find out something similar in another section of the paper.
- If the compulsory fields are not sufficient to mark the paper in a category, read the optional fields. Try to find out as much information as you can in order to establish a criterion for information classification.
- Mark the paper according to the work carried out in the previous steps and register the result in an software tool.

Repeat the process for each paper. The final result will be to have all the papers marked in the software tool.

4.4.3 Meeting of the coders to review results

After each paper has been codified, a meeting for reviewing the results will be carried out and the following steps must be followed for each paper:

- If an Alpha Krippendorff's coefficient of 0,80 or greater is reached between the coders according to its coding result of the paper, mark the paper in the category established.
- If there is not consensus between the coders about the coding result of the paper, additional meetings in order to achieved that agreement must be carried out until reach an Alpha Krippendorff's coefficient of 0,80.

At the end of this procedure, each one of the papers must be marked with a mutual agreement between the coders.

4.5 General Coding validation

In order to validate the coding procedure, the following general criteria must be applied:

- At least two coders must participate in the process.
- It is strongly encouraged the participation of an expert in Security if possible.
- An Alpha Krippendorff's coefficient of 0,80 has been considered as a measure of consensus.
- In order to mark the papers, the proof of validation established in the Inclusion and Exclusion criteria must be considered as a baseline.

REFERENCES

- [1] IEEE Thesaurus, “2023 IEEE Thesaurus”, 2023, Available on: <https://www.ieee.org/content/dam/ieee-org/ieee/web/org/pubs/ieee-thesaurus.pdf> Last accessed: 2023-12-11
- [2] University of Pennsylvania, “Computing Krippendorff's Alpha-Reliability”, 2011, Available on: https://repository.upenn.edu/cgi/viewcontent.cgi?article=1043&context=asc_papers, Last accessed on 2023-12-27.
- [3] NIST, “Guide to General Server Security – Recommendations of the National Institute of Standards and Technology”, 2023, Available on: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf>. Last accessed on 2023-12-12.
- [4] NIST, “Engineering Trustworthy Secure Systems”, 2022. Available on: <https://csrc.nist.gov/publications/detail/sp/800-160/vol-1-rev-1/final>. Last accessed on 2023-12-12.
- [5] ISO/IEC, “ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements”, 2023, Available on: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en>. Last accessed on 2023-12-12.
- [6] ISO/IEC, “ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection”, 2023, Available on: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en>. Last accessed on 2023-12-12.
- [7] ISO/IEC, “ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks”, 2023, Available on: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-4:v1:en>. Last accessed on 2022-12-12.
- [8] MITRE Organization, “MITRE ATT&CK”, 2023, Available on: <https://attack.mitre.org/tactics/mobile/>. Last accessed on 2022-12-12.
- [9] NIST, “NIST Cybersecurity Framework”, 2014, Available on: <https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf>. Last accessed on 2022-12-12.
- [10] TrendMicro. “Industrial Control System”, 2023. Available on: <https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system>. Last accessed on 2022-12-12.