Research methods applied to software security

María Cazares
IDEIAGEOCA
Universidad Politécnica Salesiana
Quito, Ecuador
mcazares@ups.edu.ec

Roberto Andrade
Facultad de Ingeniería en Sistemas
Escuela Politecnica Nacional
Quito, Ecuador
roberto.andrade@epn.edu.ec

***Abstract*—Research in software development is important to generate functional, adaptable, eco-friendly, and secure solutions. In the academia, there have been many discussions about the use of more engineering research methods in comparison to the ones used in social sciences (BSR) for behavioral analysis or theory construction. However, the increase of the human-machine interaction has been taking greater relevance. In the present study, we carry out a review of the most used research methods in cybersecurity, validating that the selection of the most used research methods is focused on the construction and evaluation of IT artifact/software. Such can be the case for design science research or controlled experiments.**

***Keywords*—research methods, cybersecurity, software development**

I. INTRODUCTION

In these days, many social activities have been transferred to the digital world such as work, education, relationships, entertainment among others. The growing rate of information systems and technologies such as: IoT, bigdata and cloud, have created new cybersecurity challenges [2]. In the study of cognitive Sciences Applied to Cybersecurity, a variety of cybersecurity tendencies were analyzed, of which the following, stand out [3]:

1. Attacks to smart grids
2. Attacks to smart homes
3. Attacks to IoT healthcare systems
4. Attacks to smart cities

These attacks to Information Technology (IT) and Operational Technology (OT) can be mediated through social engineering, cyber-pedophilia, fake-news, or fraud. So, to get the affectation of IT or OT, a human behavioral attack/analysis was developed first. Bernardes and Albuquerque posture the importance of studying the interaction between social science and technology [1]. In this point, is possible that a higher level of scientific development in software process could improving the opportunities of generating more secure solutions. So, if the research objective is composed by establishing cybersecurity strategies over the development of an software or IT artifact that directly interacts with a user, the research process cannot be approached on only technical aspects, rather a bidirectional bridge between technical and human behavioral aspects is required.

Having a cross-disciplinary and collaborative application is not novel, some state-of-art contributions are focus on reducing or managing antagonistic processes in both the computer science and social science research. The focus of this study is centered around the challenges faced by cybersecurity along with software solutions and the human behaviors. This context brings up the next research question: What are the most adequate social research methods to evaluate security in computer systems?

To address this question the present study is structured as the following. Section II presents the theorical background related with the research process in a general way, as well as the relevant aspects of research design in computer science. Section III introduces the method used in this study, which is based in Systematic Literature Review (SLR). Section IV presents the results about the social research methods used in cybersecurity. Section V covers the discussion about the most used social research methods in cybersecurity studies and the reason for their selection. Finally, section VI presents the conclusion of this work.

II. THEORICAL BACKGROUND

A. Social aspects in cybersecurity research

Social aspects are boarded in different research studies in the cybersecurity domain. In most recent studies, Olan's contributions, of which is engaged by a thorough data analysis, evaluates the social impact fake news provokes using a meta-framework based on a series of interviews. On the same premise, Zambrano and Sanchez contribute to the fight against cyber-pedophilia and fraud respectively with innovative artificial intelligence models, natural language processing, and the classification of psychological information. Carley defines seven core research areas in cybersecurity that include social aspects:

- Social Cyber-Forensics, related to who conducts the attack
- Information Maneuvers, analyze techniques used to engage on the attack
- Motive Identification, analyzes the attacker's motivation
- Diffusion, analyzes the impact on a campaign's influence
- Effectiveness of Information Campaigns, evaluates the effectiveness of the campaigns used in attacks
- Mitigation, understands the attack's resilience
- Governance, related to the norms and politics to be applied

The necessity to generate and validate social behaviors in cyber security strategies, such as methods, algorithms, and prototypes require an adequate research process to validate the results. Additionally, the research design needs to take in consideration the dynamic and complexity of the IT systems. Thus, it is important to evaluate the temporal, spatial, and behavioral aspects. In a computer science field, digital

979-8-3503-2759-5/23/$31.00 ©2023 IEEE
DOI 10.1109/CSCE60160.2023.00426

applications and information systems have been favored to get relevance in a similar way to other sciences, such as the humanistic social sciences. But so it is that computer science is not a new scientific approach given the following definitions that have been defined [6]:

- Computer science is the study and management of complexity,
- Computer science is the study of phenomena related to computers,
- Computer science is the study of information structures,
- Computer science is the study of algorithms.

Although logic, mathematics, natural sciences, and social sciences are included as fundamental elements of computer science; as seen in Figure 1, there has been a lot of discussion in the academic field about the research methods to be used, either in information systems or engineering solutions. One of the discussions regarding this is that many traditional research methods used in social sciences are largely focused on establishing a philosophical problem based on the research's epistemology, rather than in the development of the IT artifact itself [7]. Some authors in the engineering field have mentioned that the objective is not focused on the development or justification of theories, for the resolution of the IT problem is rather more essential. So, they have opted for suggested approaches such as Design Science Research (DSR) [8]. Table 1 shows a comparison between Behavior Science Research (BSR) used in social sciences and DSR.

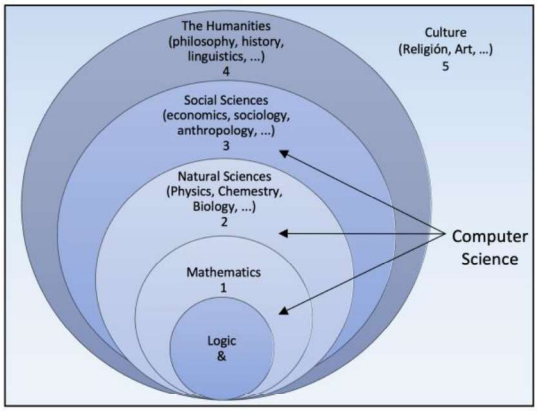

FIGURE 1. **Relationship Computer science with other sciences** [9].

However, in the computer science field, some research requires behavioral analysis, such is the case of a human behavior regarding a computer system, for that reason BSR can result in a more pertinent research method [9]. Extrapolating this aspect to the cybersecurity field as an area of a computer science research, we can consider that the traditional research methods used for behavioral analysis can be used to understand certain cybersecurity aspects in the software development process. As aforementioned, the development of new technological solutions needs to analyze the analyst's behavior when resolving a security incident or the user's interaction when is facing an attack. So, the necessity to generate and validate cybersecurity solutions (methods, algorithms, and prototypes) could require an appropriate social research process to validate the results.

B. Research process

According to [10] the types of research can be classified in function to the application, objectives, or types of information requested, as shown in Figure 2. There are different types of studies based on an application. One of them is applied research, this study is referred to the process of looking for the solution to a specific practical problem encountered by an individual, an industrial organization, a business organization, or society itself [11]. The objective of applied research isn't the creation of knowledge, rather it's the resolution of the problem along with the improvement of human conditions that motivate this kind of study. In the field of computer science, Experimental Computer Science (ECS) has been defined as a set of practices, methods, procedures, and techniques that assist computing practitioners on moving the computer sciences from its radical perception towards an applied science [12].

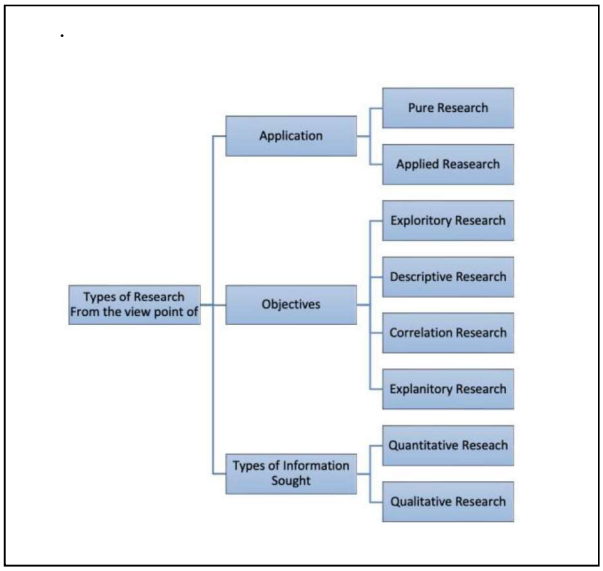

FIGURE 2. **Types of research based on the application, objectives or information sought.**

Pure research is mainly concerned with the formulation of a theory, so it generally does not have a commercial purpose as its impulse, oppositely it's the curiosity of resolving a determined scientific question that pushes the research foreword [13]. Theoretical Computer Science (TCS) has been defined in the computer science field based on a formal establishment of rules determined by both mathematics and logic. If a TCS satisfies this, its hypothesis can establish a generalization of the findings, ultimately proposing a theorem, a formal model, an algorithm, or another form of theorization, it expands the scientific background of its field in computer science [14]. The relevant aspects of Theorical CS and experimental CS are presented in Table 1.

TABLE I
RESEARCH TYPES ON COMPUTER SCIENCE

Scientific Methods	Focus on	Based on
Theoretical CS	Conceptualization, modeling, and analysis	Data models, algorithms, complexity
Experimental CS	formulate phenomena, explanations, testing	Experiments: theory testing, exploration

Based on the objective, the type of study can be exploratory, descriptive, correlational, or explanatory. An explanatory study has as an objective to study the phenomenon, situation, or problem that have not been studied previously as it pretends to profoundly analyze the relationships between its cause and effect [15]. This type of study seeks to find data that supports a predetermined hypothesis, as well as establishing knowledge that can be used for design theory, so once there is generated knowledge, prescriptions or predictions can be established. On the other hand, based on questions that help identify the best practices for this, an exploratory study's objective is to engage in a profound analysis when the problem is not clearly defined. It is very useful to be able to determine a research design, the data collection methods, and the selection of subjects [16] for the study. A comparative between exploratory or explanatory research are show in the Table 2.

TABLE II
COMPARATIVE BETWEEN EXPLANATORY AND EXPLORATORY STUDIES.

	Explanatory	Exploratory
Objective	To provide insight and understanding.	To test specific hypothesis and examine relationships.
Characteristics	Information needed is defined only loosely.	Information needed is clearly defined.
	Research process is flexible and unstructured.	Research process is formal and structured.
	Sample is small and non-represented.	Sample is large and representative.
	Dad analysis is qualitative.	Data analysis is qualitative.
Findings	Tentative.	Conclusive.
Outcome	Generally followed by further exploratory or conclusive research.	Findings used as input into decision making.

Descriptive research is based on finding facts that give forward an explanation to a specific situation. On this type of study, the researcher does not have a direct contact with the variables, as for the results are reported as an observed phenomenon under a certain set of conditions [17]. Once compared predictions with experimental data, it can be used to evaluate existing theories, including the state-of-the-art description.

Constructive research is focused on finding a solution to a determined or persistent problem [18]. This type of study is common in the development of computer science constructs. The term construct is associated with the formulation of a new theory, algorithm, software, framework, or model. It generally involves evaluating the construct under a set of indicators for predefined criteria.

Empirical research is a form of gaining knowledge in a direct or indirect way through the observations or experiences [19]. The generated evidence can be analyzed in a qualitative or quantitative form, of which is generally fundamental in the set of questions to answer and is used to obtain theories. Normative research produces the theory of design like recommendations, rules, standards, algorithms, advice, or other tools for improving the object of study [20].

The type of information sought can have a quantitative or qualitative study. For example, qualitative research is concerned with a qualitative phenomenon, for it involves looking in-depth at non-numerical data [21], so that a theory can be tested based on numerical and statistical evidence [22].

C. Research design in computer science

To resolve a research problem, it's necessary to establish a research design based on the selection of a research method in correlation to its strengths. The validity of a research design depends on how well it compensates the weakness of the research methods. Research design is the blueprint for a study [23] since both the research problem and the research questions need to be defined collectively. It's also important define units of analysis and the necessary criteria to interpret the results as well as consideration of philosophical fundaments, theories, and methods to be used. An important aspect of this is that various works are based on selecting a method without any sustenance, for this reason, it is important to previously select a method, justify the objective of the study, and then choose the type of study to perform.

There are different epistemological currents, but in computer science, research designs can generally be in two categories based on the epistemology (positivist or interpretive). Positivist are focused on theory testing and the definition of generalized patterns based on an objective standpoint. Interpretive designs are focused on theory building, based on a subjective interpretation of a social phenomenon. As mentioned before, research design requires finding questions that are aligned with both the objective and the type of study. On Table 3 some types of research questions are presented.

TABLE III
Types of research questions

In computer science the existence of questions, pretend to define the efficiency of an IT solution, an algorithm, software,

Type of question	*Sub-classification of questions*	*Research tools or source*	*Goal*	*Epistemology*
Exploratory questions	*Existence questions*	*Qualitative data*	*Build tentative theories*	*Phenomenological Constructive*
	Description and Classification questions.			
	Descriptive-Comparative questions			
Base-rate questions	*Frequency and distribution questions*	*Standard statistical distribution*	*Define the context of situation (normal or unusual).*	*Positivism*
	Descriptive-Process questions			
Causality questions	*Causality questions o*	*Standard statistical*	*Define the context of situation (normal or unusual).*	*Positivism*
	Causality-Comparative			
	Causality-Comparative Interaction			
Design questions	*Non-empirical research*	*Qualitative data*	*Build prototypes*	*Positivism*

or even hardware, meanwhile descriptive and classification questions are focused on the properties, categorized components, or measurements. Base-rate questions seek to establish normal patterns of the different causes, another subtype are the Causality-Comparative questions that investigate how the context can affect a cause-effect relationship.

D. Scientific method in computer science

The following element of a research processes is related to the foundational aspects of how knowledge is constructed. The most used scientific methods are the inductive, the deductive, and the abductive [7]. Table 4 shows a general description of scientific methods.

TABLE IV
TYPES OF SCIENTIFIC METHODS

Scientific Methods	Focus on	Goal
Deductive	Theories and laws	New knowledge
Inductive	Observation	Theoretical foundations
Abductive	Theories and experimentation	Build artefacts

The inductive method is based on a process of observation used to construct scientific knowledge [24]. In the deductive method, theories are used to explain or predict a given phenomenon [7]. By using deduction, it is possible to build new knowledge based on prior knowledge, thus explaining, and predicting the behavior of an object of study. This method is characterized by identifying a problem based on previous knowledge so that once a hypothesis is proposed, it can be tested, resulting with predictions and explanations [25].

E. Research methodology and research methods

When wanting to find a scientific approach, the research methodology can be classified as qualitative, quantitative, or a mix of both [26]. The research methodology is merely the beginning of the process for it defines the techniques to be conducted in the research for it explains the reason for the selected method. It's important to stress that it is a multi-dimensional concept that defines the systematic strategy to be used in the approach to the research's objective [27]. On the other hand, research methods focus on more suitable types of techniques used to collect and analyze data in order answer the research problem [28]. Research methods depend on research design and are a small part of the research methodology [29-30]. It is important to clearly differentiate these two elements for they are sometimes misinterpreted or approached similarly. As mentioned previously, an important relation between a research's design, methodology, and method, exists within its process.

II. METHODOLOGY

To identify the research methods to be used in the cybersecurity research study it has been decided to use a systematic literary revision based in the Prisma Guidelines [31]. Studies under scientific bases such as ACM, IEEE, Scopus, Taylor&Francis, and Google Scholar have been selected as primary sources, and then process how is show in the Figure 3 in the SLR.

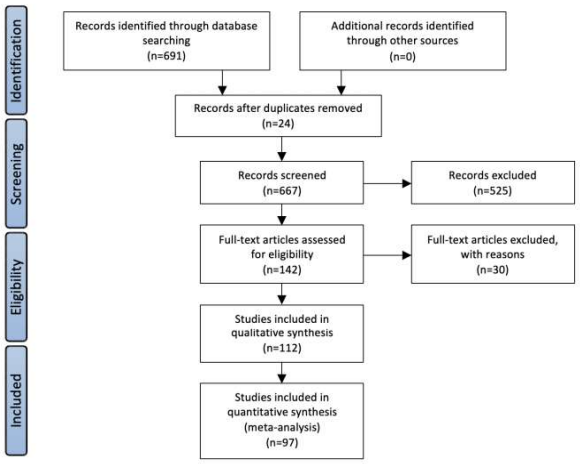

FIGURE 3. Prisma methodology for Systematic Literature Review [31].

III.

RESULTS

Based on the literary revision we can identify the following empirical methods that are used in a security context within computer science. The main characteristics are presented on Table 5.

TABLE V
TYPE OF RESEARCH METHODS USED IN IOT CYBERSECURITY

Empirical Methods	Types	Focus on	Elements	Study of	Resources
Survey research	Cross-sectional	Clear research question	Questionaries and Previous studies	Context	Structured interviews, or data logging techniques
	Longitudinal				Representative sample
	Retrospective				Past experiences and beliefs of people
Case studies	Exploratory case studies	Clear research question	Selection of cases and the types of data	Cause-effect relationships	Purposive sampling
	confirmatory case studies				Observational data
	Casual		Unit of analysis		
	Explanatory				
	Descriptive				
Controlled Experiments	Quasi experiments	Clear hypothesis	Independent and dependent variable	Cause-effect relationship	Human
	True experiments				Experiments
	time-series experiments				
Ethnography	Realism	Research question	Systematic data analysis	Study a community	Individual and group interviews
Action Research	Case study				Participant observation
	Critical				
	Technical	A problem owner	Independent and dependent variable	Design of IT constructs Theorical framework	Surveys Individual and group interviews
	Deliberative				
	Participatory				
Design Science research		A problem owner	Prototypes	Design of IT artefacts	Technical requirements
					Surveys
					Interviews

Table 6 presents a description of the objectives that make part of the application of these methods in the scope of cybersecurity. A cybersecurity gamut covers different topics that can require a social attribute evaluation, so based on the literary revision made on this study we can identify four areas: IoT security, fake news, phishing, and cyber-fraud.

TABLE VI
TYPE OF RESEARCH METHODS USED IN IOT CYBERSECURITY

Type of research method	Focus on	IoT	Fake news	Phishing	Cyber-fraud
Ethnography	Classification of the types of Relations between factors	Security, privacy, and IoT solutions [32-36]	Identification of factors utilized to identify fake news	An analysis on phishing experiences from the victims.	Fruad behavior detection
Case studies	Vulnerability assessment Security evaluation future directions	IoT solutions [37-41]	Analysis on actions to be taken to detect fake news	Simulation exercises	Fruad detection pattern analysis.
Action research	Governance	Governance	Development	Development	Development

	models or frameworks	model of IoT systems [42]	of fraud detection strategies	of phishing detection strategies	of fraud detection strategies.
Design science research	Development of security solutions	Security IoT solutions (block chain) [43-46]	Development of fraud detection strategies	Development of phishing training exercises	Development of fraud detection frameworks.
Survey search	• Establishing of actual situation. • Identification of theoric al sources • Identification of new approaches or technologies	Understanding of threats and attacks related to IoT security. Understanding of new technologies or approaches related with the security in IoT [47-50]	Methods to detect fake news	Evaluation of techniques, roles, and attack vectors.	Identification of fraud patterns.
Controlled experiments	Functionalities, and security operations	Test security of new IoT products [51-53]	Experiments to evaluate fake news	Evaluation of the increment or decrement of the capacity to detect phishing.	Experiments to evaluate fraud behavior.

Ethnography

Ethnography is focused on the generation of a theory through observation. In social sciences, its main goal is the study a community of people for the attempt of understanding their social interactions [58]. Ethnography research takes an explicit constructivist epistemology and then tries to avoid the use of any pre-existing theories.

One of the main advantages of ethnography is its ability to establish a classification and analysis of the types of relations there exists between factors or variables. In fact, it's possible to identify factors or variables in case of not being previously known for they are necessary to resolve existing research questions. For this reason, ethnography is one of the many research methods used in the scope of cybersecurity to identify elements or factors of a digital environment and establish the respective digital relationships that can exist between these computational elements as well as the relationships with its users. An example of this, is the use of ethnography allows the classification of critical industrial assets and their relationships with IoT devices [32-33], the relation between IoT and data [34], and the aspects to evaluate future data protection and the privacy user experiences in smart solution [35-36].

Cases studies

Case study is an empirical method that investigates a contemporary phenomenon within its real-life context [56]. Exploratory case studies in social sciences are used as initial investigations of some phenomena to derive new hypotheses and build theories, and confirmatory case studies are used to test existing theories. A case study is needed to define a clear research question concerned with how or why a certain phenomenon occurs. Sometimes a single case is sufficient. Choosing an appropriate unit of analysis is important to ensure that the study focuses on the intended phenomena. Case study research is more appropriate for cases where the reductionism of controlled experiments is unsuitable. In the field of cybersecurity in Computer Science, the case of studies is focus on establishing future direction for vulnerability assessment and security evaluation. For instance, in IoT security, case studies were used to highlight the risks of insecure IoT devices that are deployed in the vertical society [37]. Using case studies, a researcher is capable to analyze network and application vulnerability in IoT devices using static and dynamic analysis techniques, these techniques also permit the definition of the categories that an IoT attacks belongs, these can be: 1) physical; 2) network; 3) software; and 4) encryption [38-39]. It's also possible to evaluate the privacy of things [41] and analyze the incorporation of new technologies that may be able to improve the security in IoT devices, an example of this is Blockchain [40].

Action research

Action research is another relevant method used in computer science. It's two key criteria for judging the quality of whether the original problem of an action research is authentic and whether there are authentic knowledge outcomes for the participants. Action research is more closely associated with an epistemology called critical theory. The field of IoT security is focused on establishing a governance model [42].

Survey research

Survey research is used to identify the characteristics of a broad population of individuals. It is most closely associated with the use of questionnaires for data collection. However, survey research can also be conducted by using structured interviews or data logging techniques. Survey research is a clear research question that asks about the nature of a particular target population. Sampling bias causes problems in generalizing the survey results because the respondents to the survey may not be representative of the target population [57]. Survey research falls almost exclusively into a positivist standpoint. The desire to characterize an entire population via sampling techniques requires a belief in reductionism, and a concern with generalizable theories.

In [46], the relevant literature regarding the dimensions time and specificity are identified, categorized, and described. In [47], recent research in IoT security make an analysis. In [48], a comprehensive survey of security and privacy issues of smart cities is delineated. In [49], four different technologies, blockchain, fog computing, edge computing, and machine learning are identified to increase the level of security in IoT. In [50] the use of machine learning for IoT security is identified. These studies are based in survey research.

Controlled experiments

The hypothesis guides all steps of the experimental design, including deciding which variables to include in the study and how to measure them. The experimental method is closely tied to the positivist. The selection of the subjects to participate in the experiment, as well as the tasks to be developed, are based on the theory. Meanwhile, in quasi-experiments, the subjects are not assigned randomly. On the other hand, in time-series experiments the effect of a treatment is measured over a period.

In [51], a new method to find IoT devices on the Internet is proposed to assess this threat through a controlled experiment of 10 device models by 7 vendors. In [52], a credit-based proof-of-work (PoW) mechanism is proposed for IoT devices, which can guarantee system security and transaction efficiency. In [53], a multidimensional analysis of information exposure is conducted from 81 devices located in labs to identify potential privacy risks. These studies are based on controlled experiments.

An overview of the research methods that have been identified in the related studies to cyber security in IoT systems is presented on Table 6. The investigation methods are a key element that give way to the operation of the investigation. The general characteristics of an empirical method that has been identified in the research scope of cyber security IoT systems can be seen on the Table 7.

Design Science Research

Design science research is a method that establishes and operationalizes research when the desired goal is an artifact or a recommendation [55]. The main objective in the use of a DSR is based on the development and construction of the artifacts shown on Table 8. Concerning this aspect, it is important to mention that on the computer science domain there is an important use to the design science research method, of which is focused on problem solving [7]. Based on the understanding of the problem, this method can be used to develop and evaluate artifacts [54]. A key feature of a design science research as a method, is that it is oriented to solving specific problems, even if the solution is not optimal. Up till here, it is important to mention that the DSR method has had an extended discussion about the fundaments of epistemological base it possesses, were some say it is positivism while others say it is constructivist. As it may be, design science is the epistemological basis for the study of what is artificial.

In the field of IoT security, based on design science research, it is possible to evaluate new solutions such as blockchain-based IoT sensor data logging and monitoring systems [43]. Using DSR, the creation of physical and digital layers of IoT-enabled structures are possible [44], so is the design, implementation, and testing of an intrusion detection system for IoT systems [45].

IV. DISCUSSION

Based on the analysis of the 97 articles that have been selected through this literary revision, 6 ethnography studies, 20 case studies, 17 controlled experiments, 22 design science research, 30 survey research, and 2 action research were obtained. An overview of the types of research in IoT security are show in Figure 4. The research methods of greater selection are the ones used in the developments of IT artifacts or constructs. Most of the research methods focus on a development of security solutions rather than ones identified with theorical gaps. These methods have a positive epistemological focus while the research methods less used are of a constructive type, these are the ones that seek new theories.

This can be considered as one of the most used investigation methods for cyber security. From the analysis of these methods, we can conclude that the most utilized are the surveys focused on the types of explanatory and descriptive studies.

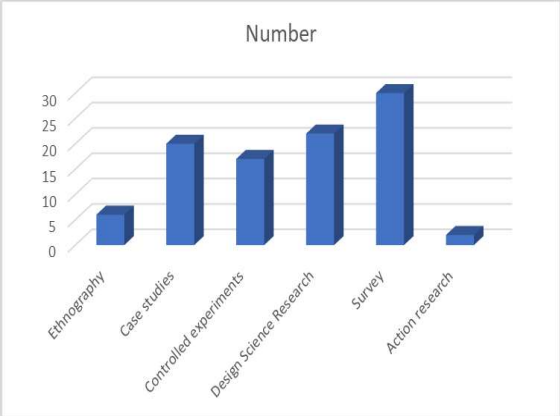

FIGURE 4. Number of research methods based on literature review

The next most used method is design science research, of which its objective is to develop an IT artifact. It has been selected in the studies to develop new encryption algorithms and an implementation of new IPS solutions. The DSR selection can be observed in the studies that have a more technical goal, of which theory analysis isn't as necessary as counting on a scientific technical process to develop and test security solutions. The third research method is one composed by controlled experiments, of which its end goal is to evaluate the behavior of a security solution, whether it is developed in the lab or in a prototype environment.

The fourth method selected is case studies, like controlled experiments, its goal is to validate the functionality of a security solution, but the difference lies that the tests are done in a real environment. The fifth selected study is ethnography, which its goal is to observe the behavior related to the user's experience of the application's security. This type of method is also used to evaluate the security and privacy of the IoT solutions thanks to the user's perspective analysis. Finally, the sixth method is action research, that is used to evaluate the behavior of the users facing an IOT system with the end goal to propose government models.

As mentioned before the methods must be selected in function to the research design, which is based in the epistemic logical principles [59]. The studies focused on the development of solutions have a positivism approach, where the research methods used are controlled experiments, surveys, and case studies. Studies with a constructivist approach use research methods such as ethnography, exploratory, case studies, and surveys. Other studies that are based on the development of frameworks have a critical theory approach that use methods such as action research and case studies. Finally, the studies that seek to solve a problem have a pragmatic approach in which we have mixed methods and the Design Science Research. A summary of the research methods and the type of epistemology are presented in Table VII

TABLE VIII
SELECTION OF RESEARCH METHODS BASED ON EPISTEMOLOGY

Empirical Methods	Drawbacks	Limitations
Survey research	Sampling bias	Hard to find appropriate case studies Hard to quantify findings Difficulty to measure changes over time.
Case studies	Research bias Interpretation	
Controlled Experiments	Behavior Effects wide ranging Effects long time	Lack external validation. Lack control over extraneous variables. Limitation of resources reduce overall testing.
Ethnography	Time consuming difficulty to choose representative sample	Avoids imposing any pre-existing theories
Action research	Biased sample	Time constraints

V. CONCLUSION

When comparing diverse investigation methods used in cybersecurity for IoT systems, we find that the scarcer amount of scientific production used in ethnographic studies and action research, indicate that constructivist strategies are less used within the field of cybersecurity in computer science. Allowing a profound understanding of the complexity and dynamic of the dynamical behaviors that are necessary to analyze in the development of IoT systems.

Most of the analyzed works are based on positivist epistemologies that are focused on the validation of IT solutions, while a smaller number of works focused on an interpretivist epistemology are evidenced. Although, the use of having a more positivism approach in computer science makes sense from a standpoint of generating a solution, theory generation is important for the understanding of new challenges, limitations and opportunities that arise from the implementation of emerging technologies such as IoT in social aspects. IoT solutions have supported the development of proposals for assisted living environments used for older adults or people with limited abilities, other solutions focus on health monitoring both for hospitals and personal care. The improvement in the quality of life and the optimization of energy resources in homes through automation and intelligence of houses (smart homes), are endpoints when generating solutions. Therefore, building theories based on the understanding of how humans interact with their environment, could support the development of preeminent security strategies. Exploratory studies based on the gathering of

information support the foundation for future works because it gives a broader insight to researchers in reference to security issues in an IoT domain.

REFERENCES

[1] R. O. Andrade, S. G. Yoo, L. Tello-Oquendo and I. Ortiz-Garcés, "A Comprehensive Study of the IoT Cybersecurity in Smart Cities," in IEEE Access, vol. 8, pp. 228922-228941, 2020, doi: 10.1109/ACCESS.2020.3046442.

[2] Andrade, R.O.; Fuertes, W.; Cazares, M.; Ortiz-Garcés, I.; Navas, G. An Exploratory Study of Cognitive Sciences Applied to Cybersecurity. Electronics 2022, 11, 1692. https://doi.org/10.3390/electronics11111692

[3] Bernardes, A., & Albuquerque, E. (2003). Cross-over, thresholds and interaction between science and technology: Lessons for less-developed countries. Research Policy, 32(5), 882

[4] Andrade, R.; Ortiz-Garcés, I.; Tintin, X.; Llumiquinga, G. Factors of Risk Analysis for IoT Systems. Risks 2022, 10, 162. https://doi.org/10.3390/risks1008016

[5] H. Shanmuganathan and A. Mahendran, "Current Trend of IoT Market and its Security Threats," 2021 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), 2021, pp. 1-9, doi: 10.1109/ICSES52305.2021.9633850.

[6] Peter Wegner. 1976. Research paradigms in computer science. In Proceedings of the 2nd international conference on Software engineering (ICSE '76). IEEE Computer Society Press, Washington, DC, USA, 322–330.

[7] Dresch, A., Lacerda, D. P., & Antunes, J. A. V. (2015). Design science research. In Design science research (pp. 67-102). Springer, Cham.

[8] Brocke, Jan vom & Hevner, Alan & Maedche, Alexander. (2020). Introduction to Design Science Research. 10.1007/978-3-030-46781-4_1.

[9] Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. BT technology journal, 19(3), 122-131.

[10] Hassani, Hosein. (2016). Research Methods in Computer Science: The Challenges and Issues. 10.13140/RG.2.2.25912.55043

[11] Hedrick, T. E., Bickman, L., & Rog, D. J. (1993). Applied research design: A practical guide. Sage Publications.

[12] Dodig-Crnkovic, G. (2002, April). Scientific methods in computer science. In Proceedings of the Conference for the Promotion of Research in IT at New Universities and at University Colleges in Sweden, Skövde, Suecia (pp. 126-130).

[13] Guthrie, G. (2010). Basic research methods: An entry to social science research. SAGE Publications India.

[14] Van Leeuwen, J. (Ed.). (1991). Handbook of theoretical computer science (vol. A) algorithms and complexity. Mit Press.

[15] Goldkuhl, G. (2004). Design theories in information systems-a need for multi-grounding. Journal of Information Technology Theory and Application (JITTA), 6(2), 7.

[16] Stebbins, R. A. (2001). Exploratory research in the social sciences (Vol. 48). Sage.

[17] Siedlecki, S. L. (2020). Understanding descriptive research designs and methods. Clinical Nurse Specialist, 34(1), 8-12.

[18] Crnkovic, G. D. (2010). Constructive research and info-computational knowledge generation. In Model-Based Reasoning in Science and Technology (pp. 359-380). Springer, Berlin, Heidelberg.

[19] Benbasat, I., & Zmud, R. W. (1999). Empirical research in information systems: The practice of relevance. MIS quarterly, 3-16.

[20] Babüroglu, O. N., & Ravn, I. (1992). Normative action research. Organization Studies, 13(1), 019-34.

[21] Fossey, E., Harvey, C., McDermott, F., & Davidson, L. (2002). Understanding and evaluating qualitative research. Australian & New Zealand journal of psychiatry, 36(6), 717-732.

[22] Gunter, B. (2013). The quantitative research process. In A handbook of media and communication research (pp. 251-278). Routledge.

[23] Akhtar, D. M. I. (2016). Research design. Research Design (February 1, 2016).

[24] Saunders, M., Lewis, P. H. I. L. I. P., & Thornhill, A. D. R. I. A. N. (2007). Research methods. Business Students 4th edition Pearson Education Limited, England.

[25] Fossey, E., Harvey, C., McDermott, F., & Davidson, L. (2002). Understanding and evaluating qualitative research. Australian & New Zealand journal of psychiatry, 36(6), 717-732.

[26] Patton, M. Q. (2005). Qualitative research. Encyclopedia of statistics in behavioral science.

[27] Gunter, B. (2013). The quantitative research process. In A handbook of media and communication research (pp. 251-278). Routledge.

[28] Williams, C. (2007). Research methods. Journal of Business & Economics Research (JBER), 5(3).

[29] Patten, M. L., & Newhart, M. (2017). Understanding research methods: An overview of the essentials. Routledge.

[30] Dodig-Crnkovic, G. (2002, April). Scientific methods in computer science. In Proceedings of the Conference for the Promotion of Research in IT at New Universities and at University Colleges in Sweden, Skövde, Suecia (pp. 126-130).

[31] Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. PLoS Med. 2009, 6, e1000097.

[32] Angelo Corallo, Mariangela Lazoi, Marianna Lezzi,Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts, Computers in Industry,Volume 114,2020,103165,ISSN 0166-3615, https://doi.org/10.1016/j.compind.2019.103165.

[33] Cayla Key, Fiona Browne, Nick Taylor, and Jon Rogers. 2021. Proceed with Care: Reimagining Home IoT Through a Care Perspective. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 166, 1–15. https://doi.org/10.1145/3411764.3445602

[34] Cayla Key, Fiona Browne, Nick Taylor, and Jon Rogers. 2021. Proceed with Care: Reimagining Home IoT Through a Care Perspective. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 166, 1–15. https://doi.org/10.1145/3411764.3445602

[35] Kraemer, M. J., Seymour, W., Binns, R., Van Kleek, M., & Flechais, I. (2019). Informing The Future of Data Protection in Smart Homes. arXiv preprint arXiv:1910.01973.

[36] George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. 2021. "It did not give me an option to decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 555, 1–16. https://doi.org/10.1145/3411764.3445691

[37] 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.

[38] G. Chu, N. Apthorpe and N. Feamster, "Security and Privacy Analyses of Internet of Things Children's Toys," in IEEE Internet of Things Journal, vol. 6, no. 1, pp. 978-985, Feb. 2019, doi: 10.1109/JIOT.2018.2866423.

[39] B. D. Davis, J. C. Mason and M. Anwar, "Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10102-10110, Oct. 2020, doi: 10.1109/JIOT.2020.2983983.

[40] M. Humayun, N. Jhanjhi, B. Hamid and G. Ahmed, "Emerging Smart Logistics and Transportation Using IoT and Blockchain," in IEEE Internet of Things Magazine, vol. 3, no. 2, pp. 58-62, June 2020, doi: 10.1109/IOTM.0001.1900097.

[41] Y. Qu, S. Yu, W. Zhou, S. Peng, G. Wang and K. Xiao, "Privacy of Things: Emerging Challenges and Opportunities in Wireless Internet of Things," in IEEE Wireless Communications, vol. 25, no. 6, pp. 91-97, December 2018, doi: 10.1109/MWC.2017.1800112.

[42] Brass, I., & Sowell, J. H. (2021). Adaptive governance for the Internet of Things: Coping with emerging security risks. Regulation & Governance, 15(4), 1092-1110.

[43] J. Lockl, V. Schlatt, A. Schweizer, N. Urbach and N. Harth, "Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications," in IEEE Transactions on

Engineering Management, vol. 67, no. 4, pp. 1256-1270, Nov. 2020, doi: 10.1109/TEM.2020.2978014

[44] J. Monteiro, J. Barata, M. Veloso, L. Veloso and J. Nunes, "Towards Sustainable Digital Twins for Vertical Farming," 2018 Thirteenth International Conference on Digital Information Management (ICDIM), 2018, pp. 234-239, doi: 10.1109/ICDIM.2018.8847169.

[45] Liang, C.; Shanmugam, B.; Azam, S.; Karim, A.; Islam, A.; Zamani, M.; Kavianpour, S.; Idris, N.B. Intrusion Detection System for the Internet of Things Based on Blockchain and Multi-Agent Systems. Electronics 2020, 9, 1120. https://doi.org/10.3390/electronics9071120

[46] Quang Do, Ben Martini, Kim-Kwang Raymond Choo,The role of the adversary model in applied security research,Computers & Security,Volume 81,2019,Pages 156-181,ISSN 0167-4048,https://doi.org/10.1016/j.cose.2018.12.002.

[47] Mardiana binti Mohamad Noor, Wan Haslina Hassan,Current research on Internet of Things (IoT) security: A survey,Computer Networks,Volume 148,2019,Pages 283-294,ISSN 1389-1286,https://doi.org/10.1016/j.comnet.2018.11.025.

[48] M. Sookhak, H. Tang, Y. He and F. R. Yu, "Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1718-1743, Secondquarter 2019, doi: 10.1109/COMST.2018.2867288.

[49] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Access, vol. 7, pp. 82721-82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[50] Syeda Manjia Tahsien, Hadis Karimipour, Petros Spachos,Machine learning based solutions for security of Internet of Things (IoT): A survey,Journal of Network and Computer Applications,Volume 161,2020,102630,ISSN 1084-8045,https://doi.org/10.1016/j.jnca.2020.102630.

[51] Hang Guo and John Heidemann. 2018. IP-Based IoT Device Detection. In Proceedings of the 2018 Workshop on IoT Security and Privacy (IoT S&P '18). Association for Computing Machinery, New York, NY, USA, 36–42. https://doi.org/10.1145/3229565.3229572

[52] J. Huang, L. Kong, G. Chen, M. Wu, X. Liu and P. Zeng, "Towards Secure Industrial IoT: Blockchain System With Credit-Based Consensus Mechanism," in IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3680-3689, June 2019, doi: 10.1109/TII.2019.2903342.

[53] Jingjing Ren, Daniel J. Dubois, David Choffnes, Anna Maria Mandalari, Roman Kolcun, and Hamed Haddadi. 2019. Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach. In Proceedings of the Internet Measurement Conference (IMC '19). Association for Computing Machinery, New York, NY, USA, 267–279. https://doi.org/10.1145/3355369.3355577

[54] March, S. T., & Storey, V. C. (2008). Design science in the information systems discipline: an introduction to the special issue on design science research. MIS quarterly, 725-730.

[55] Yin, R. K. (2011). Applications of case study research. Sage.

[56] Coon, J. J., van Riper, C. J., Morton, L. W., & Miller, J. R. (2020). Evaluating nonresponse bias in survey research conducted in the rural Midwest. Society & Natural Resources, 33(8), 968-986.

[57] Cahill, M., Robinson, K., Pettigrew, J., Galvin, R., & Stanley, M. (2018). Qualitative synthesis: a guide to conducting a meta-ethnography. British journal of occupational therapy, 81(3), 129-137.

[58] Creswell, J. W., & Miller, D. L. (2000). Determining validity in qualitative inquiry. Theory into practice, 39(3), 124-130.

[59] Figueroa, A. (2019). Science Is Epistemology. In The Quality of Society (pp. 43-82). Palgrave Macmillan, Cham.

[60] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.