symmetry

MDPI

Review

A Survey on Threat-Modeling Techniques: Protected Objects and Classification of Threats

Anton Konev, Alexander Shelupanov *, Mikhail Kataev, Valeriya Ageeva and Alina Nabieva

Faculty of Security, Tomsk State University of Control Systems and Radioelectronics, 40 Lenina Prospect, 634050 Tomsk, Russia; kaa@fb.tusur.ru (A.K.); kmy@asu.tusur.ru (M.K.); avs1@fb.tusur.ru (V.A.); nav@fb.tusur.ru (A.N.)

* Correspondence: saa@tusur.ru; Tel.: +7-(3822)-70-15-29

Abstract: Information security is one of the most important attributes of distributed systems that often operate on unreliable networks. Enabling security features during the development of a distributed system requires the careful analysis of potential attacks or threats in different contexts, a process often referred to as «threat modeling». Information protection should be comprehensive, but it is also necessary to take into account the possibility of the emergence of threats specific to a certain information system. Many public and private organizations are still trying to implement system models and the threats directed at them on their own. The main reason for this is the lack of useful and high-quality methodologies that can help developers design system models. This review explores a variety of the literature on confidentiality- and integrity-aware system design methodologies, as well as threat classification methods, and identifies key issues that may be referenced by organizations to make design system processes easier. In particular, this article takes a look at the extent to which existing methodologies cover objects of protection and methods of classifying threats, as well as whether there are such models of systems in which the object itself and the threats directed at it are described. This includes whether the compiled models exhibit symmetry or asymmetry. This literature research shows that methodologies appear to be heterogeneous and versatile, since existing methodologies often only focus on one object of protection (a system). Based on the given analysis, it can be concluded that the existing methodologies only relate superficially to the description of system models and threats, and it is necessary to develop a more complete abstract model of the protected object and threats aimed at it in order to make this model suitable for any organization and protect it against most threats.

Keywords: information security; threat; unauthorized; object; model; system; confidentiality; integrity; threat classification methods; attack; symmetry; asymmetry

check for updates

Citation: Konev, A.; Shelupanov, A.; Kataev, M.; Ageeva, V.; Nabieva, A. A Survey on Threat-Modeling Techniques: Protected Objects and Classification of Threats. *Symmetry* **2022**, *14*, 549. https://doi.org/10.3390/sym14030549

Academic Editor: Jeng-Shyang Pan

Received: 19 December 2021
Accepted: 1 March 2022
Published: 8 March 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

Information protection should be comprehensive, but it is also necessary to take into account the possibility of threats specific to a particular information system. Many public and private organizations are still trying to implement system models and threats aimed at them independently. The main reason for this is the lack of useful and high-quality methodologies that can help developers model system models.

The problem of data security threats in the 21st century is relevant, since the leakage of a small amount of information can lead to significant reputational or financial losses of organizations. For more than 20 years, human everyday life has been tied to the Internet and the digital environment; nowadays, a much larger amount of personal and confidential information is stored in the virtual world, and not on paper. With the increase in the volume of this data on networks, the number of unscrupulous people who want to acquire someone else's information, constituting state, commercial or professional secrets, is also growing.

Nowadays, cyberspace is increasingly quickly becoming the main source of information transfer from one node to another, with all its charms and problems. Cyberspace serves as an important source of access to an infinite amount of information and resources around the world. In 2017, the level of Internet use was 48% in the world; later, it increased to 81% in developing countries [1].

Cybersecurity is a widely used term, the definitions of which vary greatly, are often subjective, and sometimes uninformative. The lack of a concise, broadly acceptable definition reflecting the multidimensionality of cybersecurity hinders technological and scientific progress, reinforcing a predominantly technical view of cybersecurity, separating disciplines that must act in concert to solve complex cybersecurity problems [2].

There is no doubt about the need to protect information, and any system designed and commissioned should carry adequate protection functions regarding existing threats. Information protection should be comprehensive, but it is also necessary to take into account the possibility of threats specific to a particular information system. At the analysis stage it is important not to miss significant details, but also not to overestimate some of them, since this may entail unjustified financial and material costs. At the system design stage it is necessary to determine what level of security the final system should have, and at the testing stage to be able to evaluate the security parameters of the final system and compare them with the initial security task.

With the development of technology, it is becoming easier for an attacker to gain access to confidential data, which is why the security of information systems has become a serious problem.

The amount of information processed in automated systems is continuously increasing, which leads to the need to store large amounts of information that can become the target of an attacker's attacks. Additionally, according to experts, the number of attacks that jeopardize the confidentiality, availability and integrity of information has increased significantly.

The urgency of the problems of information protection is generally recognized; this is confirmed by high-profile trials of illegal actions with protected information. The losses incurred by companies due to information security violations amount to trillions of dollars. At the same time, the analysis of violation statistics indicates the presence of serious problems in this area, which are largely due to shortcomings in the design and operation of protective equipment.

Threats aimed at information require careful attention in order to protect confidential data. Previously, the task of providing information was solved with the help of cryptographic protection, the establishment of firewalls and access control. These technologies are no longer enough, because nowadays the number of threats to information has increased, from which it needs to be protected [3].

This review examines various examples of the literature on system design methodologies that take into account their confidentiality and integrity, as well as that on threat classification methods, and also identifies the main problems that need to be solved in order to make it easier for organizations to design systems.

In particular, it examines to what extent existing methodologies cover protection objects and methods of threat classification, in addition to whether there are such models of systems that describe the object itself and the threats directed at it.

The above literature study shows that the methodologies look heterogeneous and versatile, since existing methodologies often focus only on one object of protection (a system). Based on the above analysis, it can be concluded that the existing methodologies relate only superficially to the description of system models and threats, and it is necessary to develop a more complete abstract model of the object of protection and threats directed at it, so that this model fits any organization and protects against most threats.

The purpose of this work is to determine the most promising classification methods and structural models used to formalize the description of information security systems.

To achieve this goal, it is necessary to solve the following tasks:

- Analyze publications related to information systems;
- Select suitable publications;
- Formulate questions that are answered in the reviews of the reviewed publications;
- Analyze the sources of the selected publications;
- Carry out statistical processing of the selected publications (% of articles that answer the questions posed; % of articles that match the topic).

2. Research Methodology

This section describes general concepts related to system modeling and the classification of threats, taking into account the integrity and confidentiality of the information stored in any system.

This review aims at studying the models of confidentiality and integrity preservation in various systems, as well as the classification of threats. For example, what types of confidentiality and integrity models are more relevant in the market? What are the security requirements for maintaining confidentiality and data integrity? What vulnerabilities help to compromise data confidentiality and thus lead to security threats? What vulnerabilities should be addressed to improve system performance in terms of maintaining confidentiality? Qualitative research is used to find answers to these pressing questions.

In addition, in this review publications will be evaluated with the criterion of symmetry. This is due to the fact that there is a hypothesis that has not yet been officially confirmed. The hypothesis is as follows: if the components of a protected object are symmetrical, then the classification of threats for them will also be symmetrical. For example, the processes of storing information in a physical or virtual space (in a paper document or a file) are symmetrical; therefore, many threats will be similar. For example, saving data to an unauthorized data carrier, destroying the data carrier, etc. A detailed consideration of the dependence of the list of threats on the presence of symmetry in the object of protection is one of the directions of further research. Due to the models used by the authors, it was decided to limit ourselves only to considering symmetry/asymmetry within the framework of models.

Qualitative research helps to collect innovative information about models for maintaining the confidentiality and integrity of information in systems. However, the evaluation method in conducting the survey is not completely systematic, and the evaluations try to cover completely blind and peer-reviewed scientific articles on maintaining the confidentiality and integrity of information. These articles are focused on 2010–2021. The source of information collection is extremely clear, and is based on peer-reviewed research articles, books, conferences and published sources. These sources include various databases. These sources support a collection of articles devoted to the current state of the system models that preserve their confidentiality and integrity, as well as the information stored in it.

2.1. Brief Overview of Used Articles

This review included studies that address any cybersecurity system model and threat, including intrusion detection, spam and malware detection, discussion of performance evaluation and threat modeling.

This section includes those articles that do not provide an opportunity to classify them separately for the protection object, threat classification methods or formal linking of the protection object and the threat model, since most of the articles describe attacks on protection systems, and attacks are not considered in this review.

The following keywords were used to search for articles: cyber–physical systems, threat modeling, system model, information security, computer security, data security, security analysis and security policies.

The following databases with scientific journals and articles were selected: Scopus, Research Gate, eLibrary, Publons, SJR and ACM Digital Library.

Previous insights and review articles have been used in addition to these included articles to provide a comprehensive assessment of effectiveness.

Anton V. Uzunov and Eduardo B. Fernandez, in [4], combined threat libraries and taxonomies, and proposed an extended two-level taxonomy based on templates for distributed systems. These authors claim that the taxonomy is designed to classify a wide range of more abstract, systemic and technological threats, which allows you to control the number of threats that require consideration; this property of the taxonomy makes it more practical and useful for information security. In the end, the authors proposed a simple and effective method for constructing a threat taxonomy based on templates for specific types of systems—for peer-to-peer systems. The authors of this article have built a conceptual model linking various security patterns; analyzing it, we can conclude that the scheme is asymmetric, since it has ring loops, and that there is also a hierarchical relationship of blocks following each other.

Blake D. Bryant and Hossein Saiedian, in [5], described the structure of cyber threat modeling using a kill chain, as well as the practical application of threat modeling in criminology. The constructed structure, according to the authors, effectively solved the problem of incomplete or inadequate information about alarms by responding. The above kill chain model has an asymmetric character, since everything in it depends on the sequence of steps, that is, the sequence of proposed blocks: prehack, hack, compromise and theft.

Ye Zhu, Xinwen Fu, Byran Gramham, Riccardo Bettati and Wei Zhao, in [6], considered attacks that use the temporary behavior of TCP and other protocols as well as applications in anonymous networks with low latency. In this article, the authors focused on a specific class of traffic analysis attacks—correlation flow attacks, with which an attacker tries to analyze network traffic and compare the flow traffic on the input channel with the traffic on the output channel. When constructing the model, the authors positioned the system elements (users, encoder and servers) symmetrically relative to each other. In this paper, the authors considered mixed networks and carried out certain attacks on them, and then concluded that mixed networks using traditional batch-processing strategies, regardless of the implementation scheme, are vulnerable to attacks with flow correlation.

R. N. Dahbul, C. Lim and J. Purnama, in [7], considered a honeypot (bait), which is designed to distract intruders from computer resources. In addition, the bait tracks the actions of intruders and helps researchers learn about the schemes of their attacks. The authors of this article used threat modeling to identify potential threats that detect intruders in order to make the bait the most effective. However, there is no clearly described or constructed model in this publication, so there is no way to determine symmetry or asymmetry.

Geric Sandro and Zeljko Hutinski, in [8], analyzed various types of and criteria for classifying risks (threats) to the security of information systems. These authors identified a common set of criteria that can be used to classify threats to the security of information systems, which makes it possible to further compare and evaluate various security threats from different classifications of security threats. Geric Sandro and Zeljko Hutinski built a hybrid model of classification of information system security threats, which is presented in the form of a cube. This model is symmetrical with respect to two categories: insiders (persons/employees who are authorized users of the system, who use the system daily to perform everyday work tasks) and outsiders (persons who are not authorized users of the system).

Adham Albakri, Eerke Boiten and Rogerio De Lemos, in [9], presented a specific and detailed risk analysis of the exchange of information about cyber incidents, with a detailed consideration of what information may be contained in incident reports and what specific risks are associated with its disclosure. For each included data field, the threats associated with its disclosure were identified and evaluated, including the extent to which it identifies organizations and individuals. The main result of this analysis was a detailed understanding of what information in cyber incident reports requires protection from specific threats with an assessed severity. Since the information for analysis is different in most cases, it is not possible to build a generalized model; therefore, this article has neither symmetry nor asymmetry.

Threat modeling is recognized as one of the most important activities in the field of software security. When modeling threats, it is important to first identify assets before listing threats in order to diagnose threat targets and identify protection mechanisms.

Nan Messe, Vanea Chiprianov, Nicolas Belloir, Jamal El-Hachem, Regis Fleurquin and Salah Sadou, in [10], strove to structure the asset identification stage by offering a systematic asset identification process based on a reference model. The authors illustrated the proposed process by example, and demonstrated the usefulness of their process for supporting threat enumeration and improving existing threat-modeling processes, such as Microsoft SDL. The given reference model of the authors has an asymmetry, since one block of the model is included in another; there are also ring connections that are supplemented with each iteration.

Jan Meszaros and Alena Buchalcevova, in [11], proposed a new structure for managing the security risks of online services, which can be used by both service providers and service consumers. The key components of the proposed structure were a threat model and a risk model. These models were designed while taking into account the specific features of online services and the cyberspace environment. The above OSSF threat model of the authors has an asymmetry, since the blocks in the model have a hierarchical structure.

Laurens Sion, Koen Yskout, Alexander van den Berghe, Riccardo Scandariato and Wouter Joosen, in [12], proposed a new MASC notation: modeling architectural security concerns for modeling security problems at the architectural level. It was developed as an extension of UML, and is based on recurring security concepts that were taken from well-known security principles, goals and patterns. Using the given notation system, the system developer has the opportunity to more clearly express security problems in the documentation at the architectural level. The authors for their model are based on the DFD social network, which demonstrates the connection between the user and the database server. The above model shows symmetry with respect to services (servers).

John Patrick Barrowclough and Rameez Asif, in [13], identified the threats to which the cloud «hypervisor» is exposed, conducted an in-depth analysis and identified cloud security problems. For the in-depth analysis, a fully functional private cloud infrastructure running on CloudStack for software management was demonstrated and a real hack was organized. For the analysis, the authors proposed a schematic diagram of a basic laboratory implementation based on CloudStack, in which there is a nesting of structures; hence, it follows that this model is asymmetric.

Farahmand F., Navathe S.B., Enslow P.H. and Sharp G.P., in [14], developed a scheme for the probabilistic assessment of the impact of security threats and proposed a risk management system consisting of a five-step approach. The goal was to assess the expected damage from attacks as well as manage the risk.

Ambalavanan V., in [15], described some strategies for the effective detection of cyber threats. One of the critical disadvantages of a security system is that the level of the reliability of the security of computing resources is usually determined by an ordinary user who does not have technical knowledge about security. Malware detection training methods should be cost-effective. Malware analysts should also be able to understand malware detection techniques at the expert level.

Another threat to computer resources is a spam message. Spam messages are unwanted and unrequested messages that consume a lot of network resources, as well as memory and computer speed. Machine learning methods are used to combat such threats. Machine learning methods make a significant contribution to the detection of spam messages on a computer [16,17], SMS messages on mobile devices [18], spam tweets [19] or images/videos [20,21].

Cyberattacks planned in advance cause the greatest damage to users of information systems. Such attacks can last a very long time and require significant financial and human resources. Early detection requires the detailed monitoring of network and system parameters in order to be able to accurately identify the early stages of an attack when it is still possible to destroy the attack chain. Jusas V., Japertas S., Baksys T. and Bhandari S., in [22], proposed considering a chain of attacks consisting of nine stages, as well as a method for detecting cyberattacks at an early stage based on an analysis of the chain of attacks using hardware implementation of logical filters. The authors' experiment confirmed the possibility of detecting an attack at an early stage.

Xin Y., Kong L., Liu Z., Chen Y., Li Y., Zhu H., Gao M., Hou H. and Wang C., in [23], described key literature reviews on machine learning (ML) and deep learning, training methods (DL) for network intrusion detection analysis and provided a brief training description of each ML/DL method. In this article, the authors gave an example of a decision tree, the structure of the RN and CN models, to describe various models. These examples represent a hierarchical structure, which is an asymmetry.

Gandotra E., Bansal D. and Sofat S., in [24], examined modern malware that poses a serious threat to the Internet and computer systems. The authors highlighted the existing methods of the analysis, detection and classification of malware. The authors also analyzed traditional and advanced malware, and compared them with each other.

Dharamkar B. and Singh R.R., in [25], presented various methods of detecting and classifying cyberattacks based on data mining and a neural network approach, as well as criteria for evaluating identifiers and the dataset used to verify identifiers.

Hodo E., Bellekens X., Hamilton A., Tachtatzis C. and Atkinson R., in [26], classified intrusion detection systems (IDS). In addition, they presented a systematization and review of intrusion detection systems in shallow and deep networks. This article discusses machine learning methods and their effectiveness in detecting anomalies. The choice of functions that affect the effectiveness of machine learning IDS (ML) is discussed in order to explain the role of function selection at the stage of classification and training of ML IDS. The authors, using various schemes, showed the work of ML algorithms that are built hierarchically, also explained the essence of the work of these algorithms and eventually demonstrated a three-layer neural network.

Eder-Neuhauser P., Zseby T. and Fabini J., in [27], discussed three types of malware and central worlds that are extremely necessary to overcome security threats. They suggested that cybercrime could be reduced by constantly updating cybersecurity policies, reducing reaction times and reliable segmentation. The authors arrived at this conclusion by modeling various situations. A subsalt structure of the modeling environment was built, which has a certain nesting, that is, some objects are nested in others. This network structure is symmetric with respect to the mesh network.

Ndibanje B., Kim K.H., Kang Y.J., Kim H.H., Kim T.Y. and Lee H.J., in [28], presented a classification method for detecting obscure malware using an API call as malicious code. They applied similarity-based machine algorithms to extract features, and claimed to have effective results for obscure detection methods. The authors obtained these conclusions after performing many experiments, using a platform for analyzing and classifying malware. The authors have given the scheme of this platform in their work. It has a hierarchical structure, which helps to quickly understand the idea of the authors and understand the work of malware.

Richard White, Terrance Boult and Edward Chow, in [29], presented an asset vulnerability model (AVM) designed to solve problems and provide a strategic risk measure. This model is based on the probability of an attacker's failure, based on earlier work on game theory. The AVM supports baseline analysis, cost–benefit analysis and the development of decision support tools that reflect current risk levels, evaluate alternative protections, demonstrate risk reduction across multiple assets and measure as well as track improvements over time. The authors in their work presented a simulation model of the AVM investment strategy, which is a symmetry with respect to DSC, which helps to evaluate alternative risk reduction strategies. Then, the authors considered each object of this model and considered its risk. After this, the authors concluded that an investment strategy that reduces the risk for infrastructure assets with the greatest potential consequences provides the greatest protection over time.

Mark Yampolskiy, Peter Horvath, Xenofon D. Koutsoukos, Yuan Xue and Janos Sztipanovits, in [30], proposed a taxonomy for describing cyber–physical attacks based on CPS. The proposed taxonomy is capable of presenting both conventional cyberattacks and cross-domain attacks. Several possible applications of the proposed taxonomy are discussed in detail. Among other things, it can be used to create a knowledge base about attacks on CPS that are known in the literature. Then, using UML diagrams, the authors began to describe cyber–physical attacks, linking some groups together and using CP-ADL language to describe them. This language supports structured descriptions of conventional cyberattacks, as well as new cross-domain attacks on cyber–physical systems.

Benedikt Lebek, Jorg Uffen, Markus Neumann, Bernd Hohler and Michael H. Breitner, in [31], presented an overview of the theories used in the field of employee behavior in the field of information systems security (IS) over the past decade.

Guifre Ruiz, Elisa Heymann, Eduardo Cesar and Barton P. Miller, in [32], proposed a new and automated approach to the analysis of software projects to determine the risk rank of and mitigate potential threats to the system. A new data structure has been developed for detecting threats in software projects, called the «Identification Tree». A new method of describing measures to counter threats, called «Mitigation Trees», has been defined. This automated approach is based on identification trees and mitigation trees to integrate the managed risk assessment process throughout the development lifecycle. The general architecture scheme of the authors' approach was modeled in data flow diagrams. All the main approaches and implementations were constructed in the form of graphs (trees). The authors claim that their approaches allow companies to achieve the desired balance between software usability and security; that is, as a result, the authors have developed software that helps to identify certain risks for organizations, taking into account the completed requirements from the organizations themselves.

Risk analyses of critical infrastructures, such as electricity or telecommunications, are complicated by the fact that such infrastructures are interdependent. Gyrd Braendeland, Atle Refsdal and Ketil Stolen, in [33], offer a modular approach to modeling and analyzing risk scenarios with dependencies. This approach can be used to determine the risk level of a common system based on previous risk analyses of its constituent systems. The authors proposed various fault and threat trees, and then compiled a threat model for a composite system. However, this article contains only threats and attacks, but there are no counteractions to them. Additionally, the proposed model has an asymmetry, since each attack depends on specific actions; therefore, the model is constructed in the form of a graph with a choice of actions.

To improve the understanding of security threats, Brij Gupta, Dharma P. Agrawal and Shingo Yamaguchi, in [34], proposed a security threat classification model that allows us to study the impact of a threat class rather than the impact of a threat, since the threat changes over time. This article discusses the problem of threat classification and its motivation. Various criteria for classifying information system security risks are also considered, and an overview of most threat classification models is given.

Mouna Jouini, Latifa Ben and Arfa Rabai, in [35], consider threat classification models that help managers determine the characteristics of threats and then protect their assets from them. The existing threat classification models are not complete, and represent nonorthogonal threat classes. The purpose of this article is to offer a scalable and complete approach that classifies security threats in an orthogonal manner. This classification is given in the form of a hierarchy of threat classification. There is no symmetry in the scaled model shown.

A. A. Khristolyubova, A. A. Konev, A. A. Shelupanov and M. L. Solovev, in [36], describe the implementation of an information security threat-modeling method using the IDEF0 functional modeling methodology to solve the problems of the formalization of specific threat models. The formulation of the information security threat-modeling method takes into account various means of transmitting information and its carriers. The authors of this article gave examples of data conversion operations for each protection purpose, that is, they formally showed the information carrier—the information transmission medium—the information carrier. This publication is aimed at protecting information from integrity threats; therefore, the above approach can be used, but needs to be refined from the point of view of the confidentiality and availability of information.

U. Lindqvist and E. Jonsson, in [37], presented the classification of intrusions using taxonomies. The taxonomy is intended to be used in incident reports, statistics, intrusion detection systems, etc. The above approach is based on data from a realistic intrusion experiment, which confirms the practical applicability of the scheme. The authors throughout the work cite certain methods of computer misuse, intrusion methods through the description of taxonomies and the results of intrusions. After this, the authors developed a classification scheme for computer security intrusions, but only theoretically; the researchers do not show a practical application of the scheme.

The new paradigm of cloud computing poses a serious security threat to its adherents. To cope with these risks, an appropriate taxonomy and classification criteria for attacks on cloud computing are needed. N. Gruschka and M. Jensen, in [38], presented a taxonomy based on the concept of attack surfaces of participants in the cloud computing scenario.

Florian Sommer, Jurgen Durrwang and Reiner Kriesten, in [39], showed that the existing taxonomies were not intended for use in the development of cars, and therefore do not provide sufficient detail to support the development stages, such as threat analysis or security testing. In order to be able to use the information that security attacks can provide to develop security concepts and test automotive systems, a comprehensive taxonomy with a degree of detail has been proposed that solves these tasks.

It can be noted that most review articles do not contain a comprehensive and complete description of system modeling and the classification of threats aimed at it. Moreover, no document provides an assessment of the effectiveness of known models of systems.

Therefore, further publications will be considered that mention specific objects of protection or methods of threat classification. Their thorough analysis will be carried out, which will help to assess the current situation and draw certain conclusions from the subject area under consideration.

2.2. Overview of Articles Related to the Description of Protected Objects

This section contains publications by authors who, in their articles, described the objects of protection (or at least mention them) for further use in the classification of threat models.

In all the articles below, there is not enough of a description of the threats that would be directed at the described object of protection. The authors of subsequent publications did not consider threats and attacks on their objects of protection in the aggregate, so that it is possible to use their developments in subsequent studies. In addition to the fact that the authors only described objects, there is no way to understand which methods of protection would be suitable for the above objects. From this, it can be concluded that most authors in their research rely on only one element of information security, namely the object of protection. In order to fully ensure the security of the system, it is also necessary to indicate both the threats directed at it and the methods of protection against directed threats.

Andrey Koltays, Anton Konev and Alexander Shelupanov, in [40], considered the main methods used in constructing a mathematical model for assessing the reliability of a counteragent; identified the main difficulties in assessing the accuracy and completeness of the model; and the use of cross-validation is described. The developed model, using machine learning methods, provides an accurate result with a small number of counterparties being compared, which corresponds to the order of checking the counterparty in a real system.

Yosef Ashibani and Qusay H. Mahmoud, in [41], described the security of cyber–physical systems, that is, their object of protection is cyber–physical systems. These systems are a combination of closely integrated physical processes, networks and computing.

K. I. A. James and R. Prabakaran, in [42], compiled a threat-modeling structure for SCADA electrical distribution networks, that is, these authors have SCADA electrical distribution networks as their object of protection. The SCADA system was the basis of industrial automation. These systems are used to control and monitor critical functions of industrial infrastructure, such as electricity, gas, water, waste, railways and transport. In the field of power supply, SCADA systems are widely used for the automation of substations.

Shams Zawood, Amit Kumar Date and Rage Hasan, in [43], analyzed threats in the activity logs of cloud users, taking into account collusion between users, vendors and investigators. Based on the threat model, the authors proposed Secure-Logging-as-a-Service (SecLaaS), which saves various logs running in the clouds and ensures the confidentiality and integrity of such logs. In this article, the object of protection is the cloud.

M. O. Kalinin and A. S. Konoplev, in [44], considered a grid system as an object. Grid systems, as a type of memory of distributed computing systems, have become a leading technology that is used to solve time-consuming and resource-intensive tasks in the scientific and commercial fields. Due to the high value of the information processed by grid hosts, grid systems are focused on aspects of information security.

Olawumi Olayemi in [45] considered security problems in smart homes and mobile healthcare systems; hence, it follows that the objects of protection are a smart home and a mobile healthcare system. Smart homes provide opportunities for a comfortable and safe life, and can also help elderly and disabled people improve their quality of life as well as prolong their independent life at home. Such technologies provide an excellent infrastructure for medical purposes, which will allow the elderly and disabled to receive some affordable medical services comfortably at home.

Rimsha A.S. and Rimsha K.S., in [46], discussed the problem of choosing information security tools for one of the varieties of cyber–physical systems—automated control systems of a gas-producing enterprise. Several classes of solutions have been studied, taking into account their application in automated systems.

As you can see from a small analysis, all the authors are focused on various systems, be it an automated system, a cyber–physical system, a grid system or a smart home system. This analysis confirms the formulated relevance in Section 1, that it is necessary to create a single system that will fit any goals and objectives. In addition, the analysis proves that most researchers rely only on the description of the objects of protection, without thinking about the description of threats and methods of protection against them.

2.3. Overview of Articles Related to Threat Classification Techniques

This section introduces various threat-modeling techniques. These methods can be divided into subgroups, in which they:

- Are used separately from everyone;
- Are used in combination with others;
- Are examples for combining different methods.

To choose which method is best for a project, you need to think about specific areas in which the goal needs to be determined, such as risk, security or privacy, how much time there is for threat modeling, what experience of threat modeling is available, stakeholders' degree of involvement, etc. Some threat-modeling features of each method are shown in Table 1.

Table 1. Features of threat-modeling methods.

Threat-Modeling Method	Features
STRIDE	- Accounts for six threat categories: spoofing identity, tampering with data, repudiation of threats, information disclosure, denial of service and elevation of privileges; - Can be used as a framework in ensuring secure application design [47]; - Is the most reliable and time-tested; - Is easy to use but requires large amounts of time.
PASTA	- Application threat-modeling methodology [48]; - Promotes risk management; - Is laborious; - Has rich documentation.
LINDDUN	- Supports analysts in systematically eliciting and mitigating privacy threats in software architectures [49]; - Is laborious and time-consuming; - Finds suitable solutions to tackle the uncovered threats.
CVSS	- Used for assessing the severity of computer system security vulnerabilities [50]; - Has score calculations to prioritize responses and resources according to threat; - Has automated components.
Attack trees	- Used to understand threats to physical systems; - Used in computer control systems [51]; - Are conceptual diagrams showing how an asset, or target, might be attacked; - Are easy to use.
Persona non Grata	- Helps think about the kinds of mischief a malicious user might attempt [52]; - Detects only some subgroups of threats; - Promotes risk management.
Security Cards	- Research using this method is carried out with 42 cards in 4 categories: motivation of the enemy, resources of the enemy, methods of the enemy and human influence [53]; - Targets offbeat threats; - Many false positives.
hTMM	- Consists of SQUARE (Security Quality Requirements Engineering method), Security Cards and Persona non Grata [54]; - Contains threat mitigation prioritization; - Encourages stakeholders' collaboration; - Provides consistent results on repetition.
Quantitative TMM	- Addresses several issues with threat modeling for cyber–physical systems that contain complex interdependencies in their components [55]; - Some components are automated; - Has consistent results when repeated.
Trike	- The core of this threat-modeling methodology is the «requirements model». These requirements ensure that the specified level of risk for each asset is «acceptable» to the various stakeholders [56]; - Promotes risk management; - Has automated components; - Has unclear, insufficient documentation.
OCTAVE	- Driven by operational risks and security practices, not technology [57]; - Promotes risk management; - Easily scalable; - Time-consuming; documentation is unclear.
VAST modeling	- Requires the creation of two types of models: application threat models and operational threat models [58]; - Promotes risk management; - Some components are automated; - Easily scalable; - Documentation is not easily publicly available.

It can be seen from the above table that all methods are similar in some parameters, but that they are still different from each other. To understand how exactly they differ and where they are used, it is necessary to refer to the publications of various authors who consider these methods.

When people identify threats and do not consider the context of the underlying element, this leads to threat duplication or redundancy. Kim Wuyts, Laurens Sion, Dimitri Van Landuyt, Wouter Joosen and Koen Yskout, in [59], provided a detailed breakdown of this problem, with threat detection based on an element in the context of LINDDUN.

Nancy R. Mead, Dan Shoemaker and Jeffrey A. Ingalsbe, in [60], discussed organizations' decisions affected by megatrends, and then showed how one can use STRIDE threat modeling to manage associated risks.

Vulnerabilities are the main reason for security risks in E-learning systems. Therefore, Babita Pandey and Aditya Khamparia, in [61], proposed a threat model that identifies threats in the system and puts them into categories according to STRIDE.

In [62], M. Sukmana, K. Torkura, F. Cheng, Anne Kayem, Michael Meinig, H. Graupner and C. Meinel analyzed security threats and risks for a cloud service broker (CloudRAID). Moreover, they propose a technique for combining Common Vulnerability Scoring System (CVSS) and Common Configuration Scoring System (CCSS) base scores in probabilistic attack graphs to eliminate vulnerabilities based on configuration, which are often used to attack cloud storage systems.

D. Simopoulos, Andreas Wolf, Patrick Schwaiger and Luca D'Avino, in [63], introduced an approach to classify security threats by applying the PASTA threat model to the IoT domain. By adapting PASTA, the authors optimized the threat analysis based on domain knowledge and specific needs of the IoT. With the inclusion of the PASTA results into the designing process and the IoT software development lifecycle, they reduce security risks.

Hassan Reza and Darren Seifert, in [64], investigated the accessible architectures for cyber–physical systems to decompose them, according to STRIDE, to find security problems and ways of solving them.

In [65], Tang Zhi-Wei presented risk evaluation factors for information systems of E-government based on OCTAVE, because this is the most important aspect in government administration and services.

Rando Tonisson, Raimundas Matulevicius and A. O. Affia, in [66], used the OCTAVE allegro method of assessing critical threats, assets and vulnerabilities to identify and evaluate assets protected by autonomous vehicles (AVs), security risks and countermeasures.

In [67], Jordi Forne, Javier Parra-Arnau and Antonio Robles-Gonzalez investigated a LINDDUN extension that allows for a robust and systematically reproducible PTA (privacy threat analysis) of custom IA (identification and authentication) processes.

As you can see from the brief overview, STRIDE is the most common method. The STRIDE approach to threat modeling was invented by Lauren Confelder and Praerith Garg. This structure and mnemonic were designed to help people who develop software to identify the most devastating types of attacks for said software.

3. Research Questions and Assessment Criteria

The main purpose of this study is to understand the current state of affairs in the field of formulating system models and threat classification, taking into account confidentiality and integrity, and to identify trends in the literature. To achieve this goal, existing methodologies for the development of models and threats that take into account confidentiality and integrity will be investigated, where the following research questions are solved.

RQ1: Are there models that allow you to form the structure of the system for the further modeling of threats, attacks and protection measures?

The purpose of this study is to determine whether the development methodology takes into account the principles of the confidentiality and integrity of the information security system and supports their implementation throughout the entire lifecycle of the system's development.

In other words, this question means the formalization of the application of systems.

RQ2: To what extent do the existing formal approaches fully describe the system models and threat classifications, and do these models demonstrate their suitability for this purpose?

The goal is to understand the scope of the methodologies and whether they are «fit for purpose». The scope depends on various aspects, including the degree of specificity of specific assumptions, support for continuous evaluation and verification. Domain-independent methodologies can facilitate the cross-use of concepts and ultimately lead to common indicators and standards of confidentiality at the system level.

At the same time, in clarifying abstract concepts or transferring them from one area to another, various problems may arise. The validation of case studies can illustrate the feasibility, limitations and strengths of approaches, as well as provide additional information for adoption and future developments.

It is also worth determining to what extent the methodology supports continuous assessment of confidentiality and integrity, as well as whether it takes into account changes in threats. These aspects can help practitioners and researchers choose the right methodology based on their needs.

This question implies how existing models show their suitability (for what purposes they exist and for which organizations they are suitable).

RQ3: Is there a connection between formal system models and formal threat models?

Companies must collect and process confidential information. Therefore, it is extremely important that the model helps companies understand what threats may arise in their system and what measures of protection against them can be implemented in their systems.

In other words, this issue will analyze threats aimed at systems, as well as protection measures aimed at countering threats.

Six criteria were formulated to evaluate the identified description methodologies.

These criteria directly relate to research issues. In particular, methodologies for describing security objects, modeling threats and attacks were investigated, since these techniques include issues of confidentiality and system integrity.

In order to study the advanced methods of forming system structures (RQ1), two criteria were formulated:

CR1: Principles of the described models. This criterion evaluates which models are covered by existing methodologies. Publications that describe various systems can help other authors identify the necessary functions of the described systems, as well as the confidentiality and integrity functions that should be maintained by the system.

CR2: Principles of confidentiality and integrity. This criterion is aimed at determining whether the implementation of confidentiality and integrity is maintained throughout the entire development lifecycle of the system. This indicates whether and to what extent practices have been taken into account in the system development process.

To characterize the «compliance with the purpose» of the above methods (RQ2), the following criteria are defined:

CR3: Constant evaluation. Organizations should have the means to identify confidentiality and integrity risks, to assess their impact. This criterion examines to what extent existing methodologies support the continuous assessment of confidentiality and integrity, and, therefore, whether they can be used to model various systems.

CR4: Domain specificity. This criterion is aimed at assessing whether the methodology has been developed and applied to a specific area or whether it is independent of the area, since excessive attention to a specific area may prevent its transfer to another context [68].

CR5: Check. This criterion is aimed at assessing the level of maturity of the methodology by checking whether it has been tested and confirmed on real case studies.

In order to characterize the existing methodologies from the point of view of linking the formal description of the system model and the formal description of threat and attack models (RQ3), the following criterion was considered:

CR6: Levels of system model design problems and their relationship with threat models. The levels of problems associated with the design of the system model help to maintain an ongoing review of how each component of the system contributes to meeting the needs of stakeholders.

4. Selection of Articles

For this review, the focus is on the latest developments over the past eleven years (2010 to 2021). A total of 267 articles were retrieved. The titles and abstracts have been checked to identify potential articles. The full text of 200 studies was assessed for compliance with the inclusion criteria. The selected articles were categorized according to several criteria:

- Articles related to the description of protected objects;
- Articles related to the description of threat and attack modeling. This aspect only includes methods (models) for describing the classification of threats, that is, only how threats can be described;
- Articles related to linking formal system models and formal threat models. These articles include a description of the object of protection, as well as threats that are described for this object of protection, that is, a short list of threats for this object of information protection.

As a result, 133 studies were selected for data extraction.

4.1. Complete Overview of Articles Related to Protected Objects

In this section, the objects of protection that are found in various authors of publications will be considered in more detail. Based on the analysis of publications, a list of objects of protection that were mentioned in the authors' articles was compiled; after analysis, all objects were classified according to the purpose of their use. This selection is presented in Table 2. The table contains those publications that answer the research question from Section 3, namely R1. In addition to answering the research question, publications should fit the selection criteria, which were also formulated in Section 3, namely, for Table 2, these are the CR1 and CR2 criteria.

Table 2. Selection of publications related to protected objects.

Name of the Property	Publication	A Brief Description
Smart grid	[69]	The authors proposed a new method for solving cybersecurity problems to detect malicious activity directed at the levels of the distributed network protocol (DNP3) in dispatch control and data acquisition (SCADA) systems. In this paper, a system model was built for the proposed solution, which includes a data entry system, a data analysis system and a classification as well as detection system. Additionally, the authors in this article described some attacks on the smart grid, but the experiments were not successful. The authors pointed out that it was necessary to refine their method, and that in the future it will be possible to use it. The constructed model is asymmetric and hierarchical, since one object is nested in another, and then the general structure passes into the next structure.
Process-oriented systems	[70]	Model-based architecture is an approach to improving the quality of complex software systems based on the creation of high-level systems and the automatic creation of system architectures from models. The authors showed how this paradigm can be adapted to what is called model-driven security. In this work, several models were formed: the structure and control of the flow of the order process, a meta-model, a model for designing processes and an access control policy model for the order process. All these models are asymmetric, as they have a step-by-step structure until the first action is performed, the second is not performed, etc. Ultimately, the authors proposed a design model (process models) and a security model that can be used in process-oriented systems.

Table 2. *Cont.*

Name of the Property	Publication	A Brief Description
Computer networks	[71]	The structure of software-defined networks (SDNs) is subject to serious threats. The authors reflected the need to introduce a new approach to the consideration of cybersecurity in the framework of SDNs. They also presented a model for protecting information from cyber threats in the SDN global network connected to the Internet.
	[72]	The authors proposed a new stochastic model for quantifying cybersecurity by combining time and probability. The proposed model is based on the indicators of «Markov Chains» and «Attack Graphs». Since the authors used Markov chains, their proposed model is symmetric. The authors described all the elements that can be included in their stochastic model, and also calculated the probability of some threats to their model, but they did not describe these threats.
	[73]	The authors systematically studied methods, algorithms and system designs that used machine learning (ML) in the fields of security. We studied generalized system designs, underlying assumptions and measurements, and gave examples of their use in active research. The researchers built a matrix showing the intersection of ML paradigms and three different taxonomy structures for classifying security areas, providing tables describing protocols, system components and possible vulnerabilities, as well as which ML methods can be used in a certain attack on a computer network.
Computer networks	[74]	In this article, the authors analyzed machine learning methods used to detect intrusions, malware and spam. We set ourselves the following tasks: to assess the current maturity of these solutions and identify their main limitations that prevent the immediate implementation of machine learning cyber distribution schemes. The authors' results indicate that existing machine learning methods are still subject to a number of disadvantages that reduce their effectiveness in the field of cybersecurity. All approaches are vulnerable to enemy attacks and require constant retraining as well as the careful adjustment of parameters, which cannot be automated.
	[75]	This review aimed to provide a description of how machine learning has been used so far in the context of malware analysis in Windows environments, that is, to analyze portable executable files. The authors presented a new concept of the economics of malware analysis, concerning the study of existing trade-offs between key indicators, such as the accuracy of analysis and economic costs.
Healthcare (medical institutions)	[76]	Very few studies have systematically examined cybersecurity threats in healthcare. The authors investigated the main types of cybersecurity threats to healthcare organizations and explained the roles of four main players (cyberattacks, cyber defenders, developers and end users) in cybersecurity. As a result, the authors proposed recommendations for healthcare organizations to strengthen cybersecurity in their organizations.
Executable files	[77]	This publication discussed and highlighted various applications of machine learning in cybersecurity. This research covers: detection of phishing, network intrusions and spam in social networks; authentication with keystroke dynamics; cryptography; and evidence of human interaction.
Wireless sensor networks	[78]	In this article, the authors investigated and proposed a theoretical hypothetical model of wireless sensor networks as an effective method for creating an energy-efficient green routing model that can overcome the limitations of traditional green routing methods. For comparison, the authors built several wireless sensor networks and tested attacks on them, after which they applied machine learning to determine the probability of attacks.
	[79]	The authors proposed a taxonomy consisting of the security properties of a sensor network, a threat model and a security design space. An attempt was made to understand the purpose of the sensor network at the application level. In this article, only the taxonomy for the security of sensor networks was considered, but the authors claimed that in the future they will conduct a systematic analysis of the threat model and link it to security.
Network intelligent transport systems	[80]	The authors developed a threat model for an attack scenario, and also investigated LVS performance in terms of mutual input/output information. The practical advantages of the new information-theoretic scheme in comparison with more traditional verification systems are discussed. The authors have constructed a symmetric information-theoretic LVS model using mutual information between the input and output LVS data as an objective optimization criterion.

Table 2. *Cont.*

Name of the Property	Publication	A Brief Description
IoT	[81]	This article highlights several machine learning (ML) methods, such as k-nearest neighbors (KNN), support vector machines (SVM), decision trees (DT), naive Bayes (NB), random forests (RF), artificial neural networks (ANN) and logistic regression (LR), which can be used in IDS. This article compares ML algorithms for both binary and multiclass classification in both Internet of things datasets.
	[82]	This document provides an overview of the Internet of things security recommendations proposed by various organizations, in addition to an assessment of some existing technologies used to ensure the security of the Internet of things in accordance with these recommendations.
	[83]	In this article, the authors proposed a platform that implements a reputation-based trust mechanism and an extended application-level firewall to solve the security problems of Internet of things applications. The proposed platform provides minimal resource consumption at the node level, as well as an integrated overview and control of the system status using a cloud component and a smartphone management application.
	[84]	This article proposes a solution for anomaly detection based on the use of unsupervised deep learning methods to detect the actions of an Internet of things botnet.
	[85]	This article proposes a Hadoop-based framework for detecting malicious Internet of things traffic using a modified Tomek switchable channel, resampling, integrated with auto-coupled hyper parameters setting-up machine learning classifiers. The novelty of this article is the use of a big data platform for benchmarking IoT datasets to minimize computation time.
Enterprise applications	[86]	The authors of this article tested the method of the visualization and measurement of the architecture of corporate applications. The method was developed to reveal the hidden internal architectural structure of software applications. To achieve this goal, a test was carried out to see if this method could reveal new facts about applications and their relationships in the enterprise architecture, that is, whether the method could reveal a hidden external structure between applications.
Cloud storage	[87]	The article presents a systematic review of the literature in the field of cloud computing, with an emphasis on risk assessment. This will help future researchers and cloud computing users/business organizations gain an understanding of the risk factors in the cloud environment.
	[88]	In this article, the authors presented the current state of the privacy preservation (PPM) models of cloud computing based on TPA. Moreover, TPA privacy models were comprehensively analyzed and divided into different classes, with an emphasis on their dynamism. Finally, the limitations of the models were discussed.
Distributed systems	[89]	This source describes more fully the lifecycle processes of the secure development of distributed systems. An overview of typical security development processes is given, and important recommendations for the development of the security of distributed systems are given.
	[90]	The authors investigated and critically analyzed modern security methodologies based on some form of abstract modeling for distributed systems. A number of criteria were proposed that reflected the characteristics that security methodologies should have, which should be adopted in real industry scenarios. The authors' results help to assess risks and indicate the direction of future research.
	[91]	The authors proposed a comprehensive approach to engineering safety methodologies. This approach is embodied in three interrelated parts: the structure of interrelated models of security processes; a security-specific meta-model; and a meta-methodology that will help engineers use the model in stages. The article proposes a new template-oriented approach to the modeling, construction, adaptation and integration of security methodologies, which is the very first and currently the only such approach in the literature.

This table shows the points of view of the description of objects by various authors over a long period of time. The collected publications displayed in the table show that, despite the large number of scientific articles in this subject area, there are no articles that considered the whole system together, and not just its individual parts.

Based on the above, this table clearly shows the objects of research by various authors, which are parts of the system. That is, based on the analysis of this table, it can be seen that the authors do not describe the totality of the objects of the system, but describe only the objects of interest to them. This analysis justifies the usefulness of this table as well as its application by other researchers for their own scientific purposes in the description and construction of a model of the system and objects.

Analyzing the sources of the above table, we can say that in [69,78,80,83,85,86] the authors built schematic models to demonstrate their usefulness, and in [71,73–77,81,82,84, 87–90] the authors cited models either existing, described in words or only mathematically. This approach may not be clear to everyone, and may also cause difficulties. However, in [70,72,79,91], the authors described the models both schematically and mathematically, which makes it possible to use their developments for their systems.

The usefulness of this table is as follows: It contains a brief analysis of the selected articles. In turn, this table will be useful for other scientific researchers due to the brevity and usefulness of the information provided in the table, which significantly reduces the time spent on researching articles that are fixed in the table.

The following articles that will be presented confirm the usefulness of the table, as well as how the above studies are beneficial for the scientific community.

For example, in [69] the authors described a scheme for the SCADA/DNP3 communication protocol through several modules that play a role in building a holistic cybersecurity solution in an IoT-based smart grid environment. The proposed model can be used in any company dealing with oil/gas and water supply networks, as well as electrical devices, since DNP3 is easily configurable and is an open protocol. This study helps to understand the structure of the DNP3 protocol, and therefore helps to use these developments in future research on this topic. If scientific researchers want to build a smart-grid-based system model using the DNP3 protocol, then this article provides a complete structure and can be very useful for formalizing the model in oil/gas and water supply networks.

In [72], the authors described the system mathematically in the form of a graph in which there are a set of protected components, a set of failed components and a set of edges that show the relationship between a safe transition and failure. The relationship between the components of the system and the impact of threats can mathematically take the form of a matrix. This study uses a mathematical description of the system, which has a number of advantages:

- Identification of elements that affect security;
- Identification of critical components;
- Measurement of the security system.

Since the model is described mathematically, its main advantage is that the model constructed by the authors can be used as a template, that is, researchers can substitute elements of their system and use the calculated attack probabilities to determine the security of the system.

This description also has a drawback, insofar as the system components used by the authors are only those related to cloud computing: browser, proxy server, router, etc., that is, it will be harder to apply this model to the physical level than to the cyber–physical level. However, despite this, the proposed model is useful for a computer network security engineer and can be used to build a computer network model.

In [91], the authors described the structure of interrelated process patterns as well as a meta-model for research in the field of software development. In this article, security in the model is considered as separate objects. In addition to comparing existing methodologies, the authors proposed their own meta-methodology, which consists of several steps (stages), thereby presenting a step-by-step guide to achieve their goals. The proposed approach is intended for the development of secure software. This publication will help researchers who want to understand the structure of software and existing technologies.

4.2. Overview of Articles Related to Threat Classification Methods

Based on the analysis of publications, a list of threat classification methods that were mentioned in the authors' articles was compiled. This selection is presented in Table 3. This table contains those publications that answer the research question from Section 3, namely RQ2. In addition to answering the research question, publications should fit the selection criteria, which were also formulated in Section 3. The criteria used for this table are CR3, CR4 and CR5.

Table 3. Selection of publications related to threat classification methods.

Method Name	Publication	Brief Description
STRIDE	[92]	In this paper, the authors used STRIDE to identify vulnerabilities in a cyber–physical system and decide which appropriate component-level security measures to use at the stage of system design, because it is a light and efficient methodology of threat modeling.
	[93]	This article evaluates STRIDE, namely, the number of suitable threats usually created per hour, the correctness of the analysis results by considering the average number of false positives, i.e., invalid threats, and the fullness of the assay results by considering the average number of missed threats.
	[94]	In this paper, the authors added security solution elements to data flow diagrams (DFD) and used them together for more accurate threat detection. Their approach is confirmed on the example of a STRIDE analysis of an industrial solution for video conferences. The DFD additions presented are a key element for the development of the continuous and dynamic modeling of threats.
	[95]	The paper examines three different approaches for connecting the CWE weakness database and STRIDE, and discusses the results.
	[96]	In this paper, the authors investigated the threat-modeling method STRIDE, which is often used in the IT industry, and assessed its applicability for a connected car. The authors used STRIDE for investigating the software architecture of the system.
PASTA	[97]	The authors identified suitable security monitoring within the 5GCN through threat identification and decomposition in line with the threat analysis step of the PASTA framework.
	[98]	The authors used PASTA to model threats for a generic cyber–physical system (CPS) to prove its efficiency and report results. They also included strategies for mitigation that were identified in the process of modeling threats for CPS owners to apply.
LINDDUN	[99]	The authors presented a study based on the real application of LINDDUN. This study includes a total of 122 home automation system threat models. This study's main focus is explaining the role of assumption making in the process of modeling threats, dividing the information types into categories and matching them to the threat categories of LINDDUN.
	[100]	This paper proposes a systemic approach for using LINDDUN to determine the privacy requirements of systems that are software-intensive and select technologies for enhancing privacy accordingly.
CVSS	[101]	In this paper, the authors used the CVSS to quantitatively estimate the attack sequence, which is the attack tree leaf host in distribution automation systems.
	[102]	The authors of this paper evaluated the reliability of the CVSS scoring data found in five leading databases: CERT-VN, Cisco, OSVDB, NVD and X-Force. It was concluded that the CVSS is quite reliable, except for a few dimensions.
	[103]	The main focus of this paper was to explore the application of the CVSS to quantitatively assess and estimate the project participants' vulnerability, in addition to the application of this information as the groundwork for finding vulnerabilities in the security of construction networks.
Attack trees	[104]	Attack trees are a technique for security modeling that use logic gates to predict the chances of malicious actions. However, they do not consider attack progression over time. To solve this issue, one can use the formalism of Boolean-logic-driven Markov processes (BDMP) to extend AT where triggered transitions connect the subtrees pertaining to the hierarchy.
	[105]	This paper's focus was the application of attack tree analysis to assess the vulnerabilities of a CubeSat. The authors built an architectural model of an operational CubeSat. Then, they created a series of attack trees for the abstracted architecture to illustrate a series of potential attack vectors for small satellites.

Table 3. *Cont.*

Method Name	Publication	Brief Description
Persona non Grata	[106]	The authors of this paper wrote about crowdsourcing the creation of Persona non Grata, which can model the actions and goals of potentially malicious unwanted users. In their research they took a collection of various potentially redundant Persona non Grata and formed a single set out of it. This approach is a combination of visualization and machine learning techniques.
hTMM	[107]	This paper is about threat modeling using a hybrid techniques framework designed to help secure software against SQL injection attacks. By focusing on the most exploited vulnerabilities, security experts can determine the best methods through which to make software invulnerable to SQL injection attacks.
Quantitative TMM	[108]	In this paper the authors proposed a quantitative threat-modeling methodology (QTMM) that can help to determine privacy-related attacks that might be a threat to a service. This methodology has been successfully tested in the context of the EU project ABC4Trust, which required the end users to elicit the security and privacy requirements of the privacy attribute-based credentials.
OCTAVE	[109]	The authors of this paper described the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), an approach for dealing with information security risks. This document is an overview of the OCTAVE approach and a brief description of two OCTAVE-consistent methods developed by the Software Engineering Institute.
Trike	[110]	This document is a sufficiently detailed report on the current version of the Trike methodology. It can be used by a security auditing team for a complete and accurate depiction of the high- and low-level security characteristics of a system.
VAST modeling	[111]	The authors of this paper described the structure and implementation of a tool for assessing security risks. The tool supports a security risk evaluation method VAST which is specific threat. This method allows cloud providers the opportunity to estimate the security risk of their tenants based on threats specific to them.

Threat-modeling approaches are practice-oriented, but do not allow researchers to adapt to a specific system structure and provide a more detailed analysis of the actual threats to it.

This table lists publications that used threat classification methods. Based on these publications, it can be concluded that the authors preferred to use commonly encountered methods, such as STRIDE and PASTA. Due to the fact that these methods have extensive documentation available for development, they are often used in the description of threat models.

The usefulness of this table is that it collects the most common methods of classifying threats, which will be useful to system builders in the future.

What follows is a more detailed analysis of the articles supporting the usefulness of the table, as well as how the above studies are useful to the scientific community.

Article [92] reflects, very beneficially, how system vulnerabilities are identified using the STRIDE method. This positive moment can help developers of cyber–physical systems at the design stage. In addition, works [93,95] can be used to detect invalid threats and vulnerabilities.

In the process of modeling system threats using STRIDE, designers can only rely on abstract threats, while they do not have well-structured data about its current weaknesses and vulnerabilities. Article [94] may be useful for filling this gap.

In [96], the authors investigated the threat-modeling method STRIDE, which is often used in the IT industry, and assess its applicability for the connected car. The authors use STRIDE for investigating the software architecture of the system. This publication will assist connected car researchers in their choice of threat classification method.

In [97], the security-monitoring approach in 5GCN is described in detail, which allows researchers to analyze the threats to this technology and draw a conclusion about the advisability of using the PASTA method.

In [98], the authors used PASTA to model threats for a generic cyber–physical system (CPS), to prove its efficiency and report results. They also included strategies for mitigation that were identified in the process of modeling threats for CPS owners to apply. The usefulness of this publication is in what is observed when modeling the threat of a cyber–physical system, allowing researchers to understand whether the PASTA method is suitable for their system.

This work will be useful for developers of secure software for their IoT-based home automation systems when designing a threat model, since the LINDDUN method used can very successfully detect privacy-related errors [99].

This paper proposes a systemic approach for using LINDDUN to determine the privacy requirements of systems that are software-intensive and select technologies for enhancing privacy accordingly [100]. The practical significance of surveillance lies in the ability of users to increase privacy in the system. If users, after reading the publication, consider this method inappropriate for maintaining confidentiality, then there is an opportunity to study and use the possibilities offered.

The use of these articles will help researchers in their systems and networks to evaluate the sequence of threats, as well as to identify vulnerabilities [101–103].

Attack trees are typically used to assess vulnerabilities. Article [104] can be used to extend this method. The authors in [105] successfully applied attack trees to the CubeSat. The practical significance of this work is that designers of small satellites can use the information presented in the article to identify increased vulnerability. It can also help AI planners to evaluate the use of consumer resources.

When developing software, you can refer to this article to protect your code from SQL injection attacks. Additionally, security experts will be able to choose the appropriate method for this [107].

Works [106,109–111] describe the structure and implementation of a risk assessment process based on specific threats, which can allow designers to create models. However, unfortunately, parts of the methods used in these articles are currently experimental, which can complicate the process of threat modeling.

4.3. Overview of Articles Related to Threat Classification Techniques

In this section, publications describing models of protection objects and classifying threats will be considered in more detail. As a result, articles will be analyzed for their completeness of descriptions of both the objects of protection themselves and the classifications of threats to these objects. This selection is presented in Table 4. The table contains only those publications that answer the research question from Section 3, namely RQ3. In addition to answering the research question, publications should fit the selection criteria, which were also formulated in Section 3; for Table 4 this is the CR6 criterion.

Table 4. Selection of publications that describe threat models and classifications.

Publication	Brief Description
[112]	The authors described the need for software security testing in the lifecycle of a web application before it enters the market. The method of threat modeling used in security testing is defined. The proposed method lists threats that are interesting, highlights operations and areas that need to be protected and generates test measures used to test security checks in web applications.
[113]	This article presents the basic theory of Cloud-COVER (tools for managing and ordering vulnerabilities and risks), a threat-modeling tool developed to identify threats to cloud computing systems. Cloud-COVER simulates the observed system and determines the priority of threats using a system of relative preferences provided by the user of the instrument. The Cloud-COVER model is abstracted in such a way that it is extensible, which allows users to change the perspective of the model according to their own circumstances.
[114]	The authors proposed a model that can detect and quantify attacks. It has a rich set of agent actions with appropriate probability and cost. A threat model is also presented. The actions of the attacker have an appropriate cost and are forced to be realistic. Comparison of a model with a probabilistic means of checking symbolic models and expression of patterns of security properties in the logic of the probabilistic computing tree.
[115]	This paper describes an approach to developing threat models for attacks on control systems. These models are useful for analyzing the actions taken by an attacker who gains access to the assets of the management system, and for assessing the impact of the attacker's actions on the controlled physical process. Models of integrity attacks and denial-of-service (DoS) attacks are proposed, and the physical and economic consequences of attacks on the chemical reactor system are evaluated.

Table 4. *Cont.*

Publication	Brief Description
[116]	The authors described a structure for modeling the security of a cyber–physical system, in which the attacker's behavior is controlled by a threat model that covers cyber aspects (with discrete values) and physical aspects (with continuous values) of a cyber–physical system. The framework identifies cyber–physical features defined by security policies that need to be protected, and can be used to formally prove the security of cyber–physical systems.
[117]	The article discusses security issues in aviation and presents the application of a realistic cyber–physical system for the introduction of a threat-modeling method with the support of tools that can be used to analyze the security of unmanned aerial vehicles.
[118]	The authors proposed a new threat model called Process Memory Captor (PMCAP) in the Windows operating system, which threatens the data of the energy-dependent memory of a real process. Compared to existing technologies, PMCAP can extract valuable data at a lower cost; some methods in the model are also suitable for memory analysis and malware analysis.
[119]	This report presents a methodology for assessing threats to the information security of the National Airspace Management System (NAS) and Infrastructure Management System (NIMS). Specific vulnerabilities are discussed in the accompanying Legacy NIMS Vulnerability Study (FOTO) report. This report is an improved version of MITRE.
[120]	The article proposes an integrity threat model for an information system model based on the attributive nesting of metagraph three. This threat model includes threats at the level of software, operating system and network. The model can be used within the framework of the methodology for assessing the quality of computer network security, and can be used to develop a model of the system and threats of an automated system for commercial accounting of energy consumption.
[121]	The authors of this publication discussed three key security issues of cyber–physical systems: (1) understanding the threats and possible consequences of attacks, (2) identifying the unique properties of cyber–physical systems and their differences from traditional IT security and (3) analyzing the security mechanisms applicable to cyber–physical systems. In particular, we analyze security mechanisms for the prevention, detection and recovery, resilience and deterrence of attacks.
[122]	Creating a secure cyber–physical system is a very difficult task, since it involves the comprehensive elimination of vulnerabilities in cyber systems and their impact on physical systems. The general approach to solving this problem is to analyze the spread from cyber vulnerabilities to corresponding impacts on the physical system, or vice versa.
[123]	The authors investigated how threat modeling can be used as a basis for the specification of security requirements. They explained the differences between modeling software products and complex systems, and described an approach to identifying threats to network systems. Three case studies of threat modeling were presented: software-defined radio, a network traffic monitoring tool (VisFlowConnect) and a cluster security monitoring tool (NVisionCC).
[124]	This review examines all the most important research issues related to strengthening the cybersecurity of SCADA networks. The general architecture of SCADA networks and the properties of some widely used SCADA communication protocols are described. Common security threats and vulnerabilities in these networks are discussed, followed by a review of the research challenges facing SCADA networks. The authors discussed current work in several areas of SCADA security: improving access control, firewalls and intrusion detection systems, analysis of SCADA protocols, cryptography and key management and the security of devices and operating systems.
[125]	The author described in detail how to ensure security from the very beginning when designing systems, software or services. The book describes various approaches to threat modeling. Additionally, how you can test a system for threats and find out effective ways to eliminate threats that have been tested in Microsoft and other leading companies.
[126]	The article discusses methods for constructing threat models of information systems and computer networks. The disadvantages of existing approaches are highlighted. The authors propose an approach to the construction of a computer network model, as well as to the description of information and system threats. The proposed approach takes into account the identified shortcomings of existing solutions, and is aimed at reducing the influence of subjective expert opinion when compiling lists of threats.
[127]	In this article, the authors presented a new ICS security metric based on graphs and/or hypergraphs, which can effectively identify a set of critical ICS components and security measures that should be compromised, with minimal cost (effort) for an attacker, in order to disrupt the operation of vital assets of the automated process control system.

Table 4. *Cont.*

Publication	Brief Description
[128]	The article highlights the problem of identifying threats to the information security of computer networks. The analysis of computer network models used to identify threats, as well as approaches to the construction of such models, was carried out. The shortcomings that need to be corrected are highlighted. Based on the mathematical apparatus of attributive metagraphs, a computer network model has been developed that allows for describing the software components of computer networks and all possible connections between them. Based on elementary operations on metagraphs, a model of threats to the security of computer network software has been developed, which makes it possible to compile lists of threats to the integrity and confidentiality of computer network software. The proposed constructed model is symmetric with respect to the server.
[129]	This article discusses one of the fundamental problems of information security—building a threat model. The article discusses a new method for identifying typical threats to information confidentiality based on the information flow model. The above description was based on the formulation of the system. A review of the subject area revealed several approaches used to describe the system in terms of circulating information flows. The information flow model proposed in this paper reduces the description of any information system to an eight-digit alphabet. The analysis of the structure of the elementary information flow revealed four typical threats to privacy; the Cartesian product of a set of threats and a set of flows is a complete model of typical threats to the confidentiality of information processed in cyberspace.
[130]	This article analyzes telemedicine applications to assess security threats. This research focuses on identifying and presenting significant security threats in telemedicine. The study shows that in a strictly controlled environment, the security risks created by telemedicine applications are significant, and that using the threat table approach provides an easy-to-use and effective method of managing these threats.
[131]	With the spread of research in the field of intelligent networks, Advanced Metering Infrastructure (AMI) has become the first ubiquitous and fixed computing platform. However, due to the unique characteristics of the AMI, such as a complex network structure, smart meters with limited resources and sensitive security data, it is particularly challenging. To solve this problem, the authors have identified the basic security requirements that the AMI must meet. The authors proposed a developed accounting infrastructure, which is a hierarchical structure.

This table shows the points of view of the description of objects and threats directed at them by various authors over a long period of time. The collected publications displayed in the table show that, despite the large number of scientific articles in this subject area, there is only a small percentage of publications that describe both the object (system) and the threats (attacks) directed at it.

Based on the above, this table clearly shows the totality of the description of the system and threats, that is, based on the analysis of this table, it can be seen that a small percentage of authors describe the systems (objects) of interest to them and the threats directed at them. This analysis justifies the usefulness of the above table, as well as its application by other researchers for their own scientific purposes when describing and constructing a model of the system and the threats directed at it.

Analyzing this table, we can conclude that in [112,113,117,122,125] the authors described the model in general terms, and the threats to it were given in the form of diagrams; this approach allows the scientific community to better and more quickly understand what the authors wanted to convey to readers. In [114,116], the authors, in addition to schematically constructing a model of the system, developed attacks on this system that occur with a calculated probability and cost. The above development helps to assess threats to the system, since mathematical formulas are given, and by substituting your system values you can obtain the probability of an attack from intruders on the model being developed. Additionally, in [115,119,123,130,131], the authors described these actions verbally, without mathematical calculations, which will cause further difficulties for scientific researchers since it is impossible to use this experience in their research. However, in addition, the authors described in great detail two types of threats: attacks on the integrity of the system and DoS-type attacks, which will allow researchers to better understand these attacks. In addition to the fact that many authors have described the system model and threats to it in sufficient detail, there are also publications in which the system model was described in general terms and the authors placed more emphasis on the threat model. For example, in [118] the authors focused on the description of threats to the operating system (OS) without describing the OS itself, since it does not need a description according to the authors. It is difficult to agree with this statement, since it is not known what is included in the OS, what parameters it has and what functions it performs, and this is a necessary measure for threat analysis.

The authors of [120,126,128,129] described, in detail, the models of the system and threats in both verbal and mathematical forms, which allows them to be used as a basis for further scientific research in this field.

In [121], the authors, as in [118], emphasized the description of attacks and threats, without a detailed description of the model to which these threats and attacks can be applied. Additionally, in [127], on the contrary, the authors placed more emphasis on the description of the model than on the description of threats.

The usefulness of this table is as follows: It contains a brief analysis of the selected articles. In turn, this table will be useful for other scientific researchers due to the brevity and usefulness of the information provided in the table, which significantly reduces the time spent on researching articles that are fixed in the table.

The following articles will be presented that confirm the usefulness of the table, as well as how the above studies are beneficial for the scientific community.

For example, in [117] the authors described approaches to threat modeling in cyber–physical systems. To begin with, a model of the system was built, for which it was possible to determine its attack surface for further analysis—in this article, such a model of the system was a cyber–physical system. The authors considered only vulnerabilities related to the network communication protocol, and identified four types of threats: false message, message deletion, message corruption and flood message. The usefulness of this article lies in the fact that it can be used to apply a description of a cyber–physical system and identify types of threats in network protocols if difficulties arise in the process of formalizing their own models.

In [128], the authors analyzed existing models of computer networks that use threat detection, as well as existing approaches to building threat models for computer networks. Based on the analysis, a computer network model based on the mathematical apparatus of attributive metagraphs was developed. The constructed model makes it possible to describe the software components of computer networks and the connections between them. After that, a model of threats to the security of computer network software was developed, which allows for the countering of threats to the confidentiality and integrity of computer network software. These models are described mathematically, which allows them to be used in any research, only substituting their elements and their description. It follows that the usefulness of this study is that scientific researchers, in their work and for their own purposes, can use the described models. Additionally, based on this study, you can use a simulated system for computer networks as a basis, but with the addition of a list of threats to this system from their scientific papers, since the authors considered only the software elements of computer networks and the connections between them.

In [129], a model of information flows is presented, thanks to which the description of any information system is reduced to an eight-digit alphabet. In addition to the system model, the article describes a method for identifying typical threats to information. After analyzing the information flow model, the authors proposed four types of privacy threats to information. The developed model of the system allows you to build a scheme of information flows, in which, in addition to the permitted flows, all possible occurrences of prohibited ones will be included. This makes it possible to formulate a list of permitted and prohibited flows (access control), as well as to track unauthorized actions of violators in time. After forming the system model and threat model, the authors described typical threats to the information flow, but these threats relate only to threats to the confidentiality of information. These models are described mathematically using graphs, which allows them to be used in other studies. The models described by the researchers can be used as a basis for building a system that works with information flows. Based on the above threat model and typical threats, it is possible to describe threats to the integrity and accessibility of information flows, since the authors only considered threats to confidentiality. From all of the above, it follows that the usefulness of the publication is that these models can help the scientific community to understand the system of information flows faster and more efficiently, since the above publication described this system in sufficient detail.

5. Discussion

As a result of this study, the current state of the art in the formulation of system models and threat classification, taking into account confidentiality and integrity, was assessed.

As a result of writing the review, 267 sources were analyzed, from which 133 articles were selected that were directly related to our review. Forty-two articles were used to write the introductory section, thirty were related to the description of models of protection objects, forty-one articles were associated with methods of threat classification and twenty articles were used for formal linking with the description of models and methods of threat classification.

The study shows that the existing publications are incomplete, and that some methodologies only partially take into account descriptions of protection objects and methods of threat classification aimed at the system. Moreover, verification is often underestimated in the process of system development. This requires proven methodologies that provide specific, systematic as well as holistic guidelines.

Based on the above research, based on the research questions and criteria from Section 3, it was found that all articles can be divided into several aspects, namely:

- Articles describing attacks;
- Articles describing incomplete systems (only some parts of it);
- Articles describing the objects of protection in various ways;
- Articles describing methods of threat classification;
- Articles that formally link the description of models with threats directed at them, but without methods of protection against them.

As a result, it can be concluded that, in the 21st century, the relevance of information protection remains unchanged, since there are no specifically formulated objects of protection (if they are formulated, they are not fully described); there is also no universal classification of threats and methods of protection against them.

Due to the fact that there is no complete description of the system, threats and methods of protection, attackers penetrate into many systems, steal valuable information and use it for selfish purposes. Therefore, in further research, we wish to formulate a single model of the system, describe the threats directed at it, and also formulate methods of protection against the described threats, so that any organization can use this model and protect the stored information with the proposed methods of protection. Only by creating a unified model of the protection system is it possible to avoid the current shortcomings that were identified during the analysis of this study.

The usefulness of the given review is as follows: it can be used as a brief description of the cited publications throughout the text of the review, that is, researchers do not need to reread the entire text of the article in order to understand its essence, but it is enough to read a brief description that was interpreted in the written review.

The applicability of this review is that it can be used for future research, which will formulate a generalized system, threats aimed at it and protective measures. It is worth noting that, in the above articles, none of the authors considered protection measures against the formulated threats. For researchers, this review will help to understand the current subject area, which objects (systems) are described by various authors, which methods are used in the formulation of threat models as well as how to link the system model and the threat model together so that it is used in their research.

Figures 1 and 2 show diagrams showing the percentage and quantitative ratio of the analyzed sources. Additionally, Figures 3 and 4 show a diagram of the ratio of articles according to the criterion of symmetry.

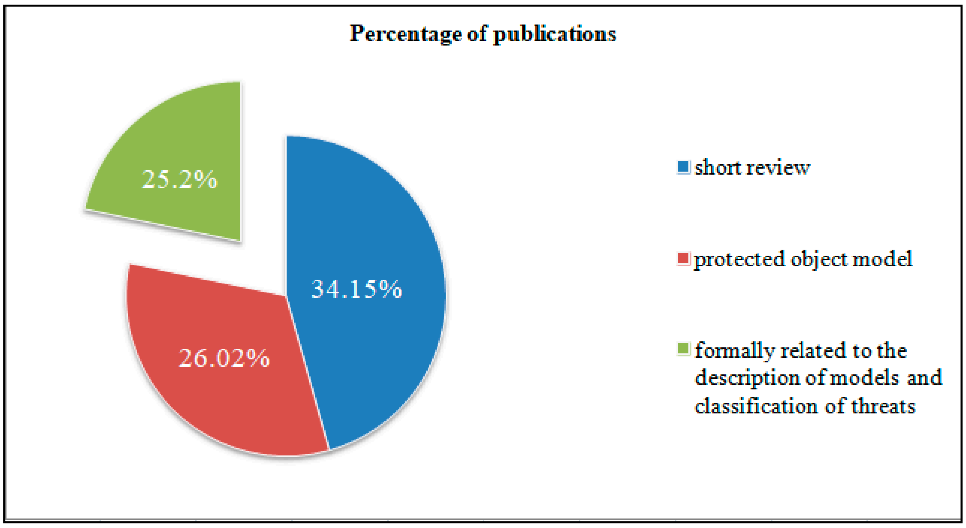

Figure 1. Percentage of publications.

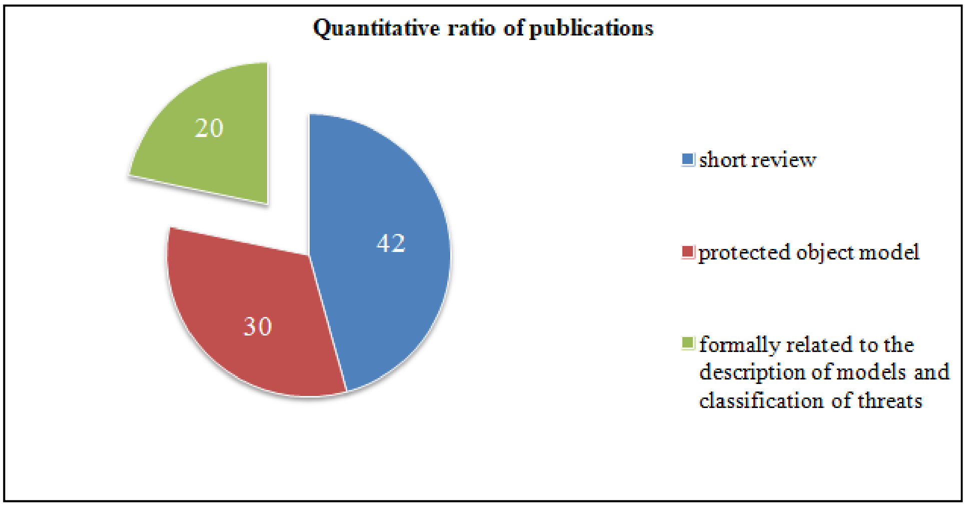

Figure 2. Quantitative ratio of publications.

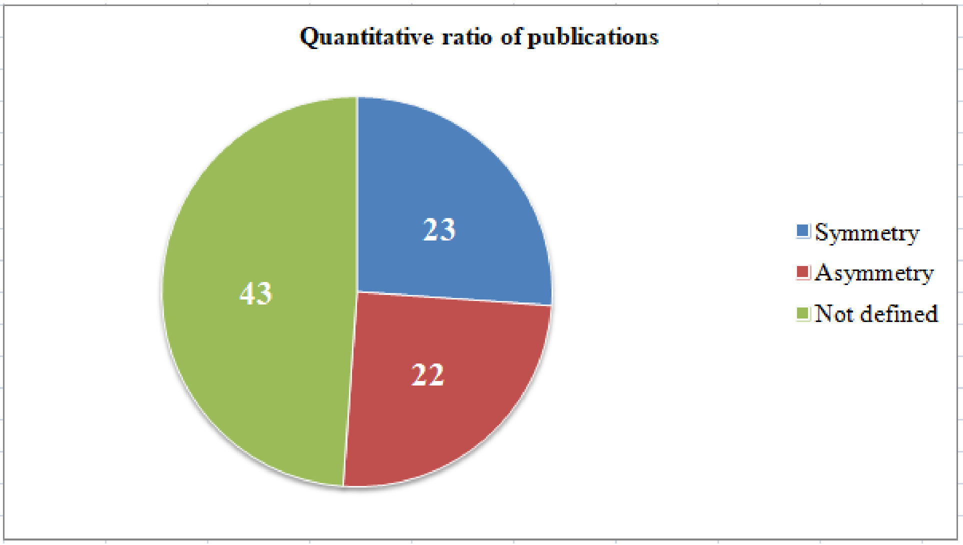

Figure 3. Quantitative ratio of publications according to the criterion of symmetry.

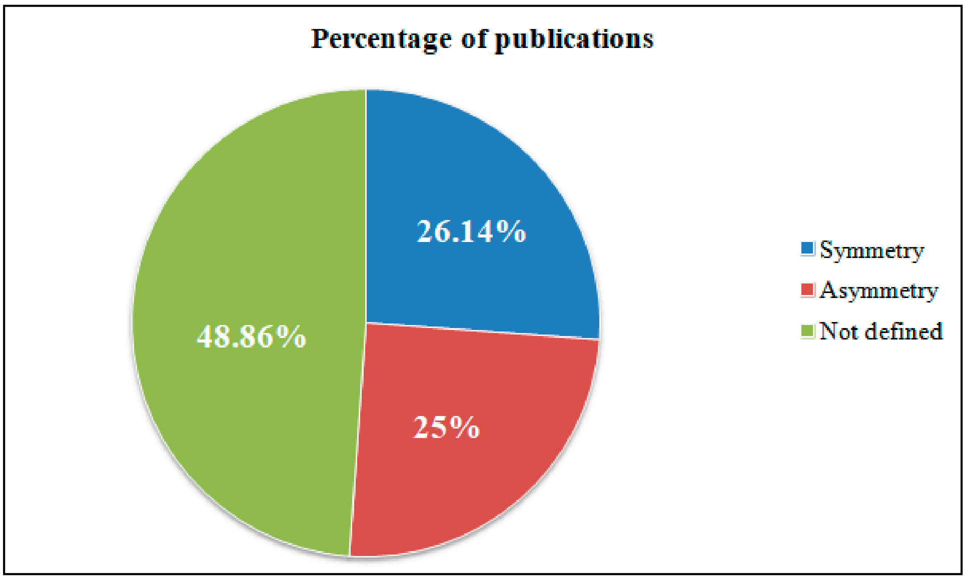

Figure 4. Percentage of publications according to the criterion of symmetry.

As can be seen from the figures, only a small percentage of authors considered the description of the system model in correspondence with the threat models aimed at it.

In order to fully describe a system, it is necessary to describe its protected object model and suitable methods for classifying threats or a threat model.

The study showed that only 20 publications considered both the formal description of the protected object and the threat model. It is worth noting that, in these articles, the models of the protected object were narrowly focused, that is, there was no abstract model that would fit any organization.

In other sources, the authors only considered either the protected object with a full description or methods of classifying threats, not combining these attributes. In particular, for the most part, only one method of threat classification was considered—STRIDE, since it is more advanced.

The different formulations of objects of protection and methods of threat classification, covered by the studied methodologies, are caused by the fact that each organization tries to implement its own model of the system and the model of threats aimed at it for further use, since there is no single formally described model that would fit any organization.

Thus, it can be concluded that, due to the lack of a universal system model and a threat model aimed at the system, many organizations neglect the protection of information, and, therefore, lose confidential data. If not handled with care, the direct application of incomplete methodologies can result in a failure to fully comply and demonstrate compliance, leading to large fines and losses.

The definition of a unified and comprehensive structure for describing a system model opens up new opportunities for research and use by many organizations. First, it will help organizations better configure and use their system. Secondly, this model will help prevent the leakage of confidential data.

The above conclusions do not only apply to IT systems, but also to systems engineering in general. This formulation can be summarized in two aspects. First, IT systems use software intensively (this means that «software has a significant impact on the design, construction, deployment and development of the system as a whole» [132]). Additionally, secondly, all systems correspond to the definition of the system as a whole, that is, there are artificial solutions with equipment, software, data, people, processes, procedures, means, materials and natural objects [133].

6. Conclusions

This overview covered, in detail, the protected object models and the most recent threat classification methods, as well as models that combine both the protected object model and the threat model.

In the course of this study, various objects of protection and common methods of classifying threats were identified. After the analysis of the publications, a detailed conclusion was made that, at the moment, there is no single formally described model of the system and the model of threats aimed at this system.

System designers need practically written methodologies to design systems with confidentiality and integrity in mind. This review shows how the existing methodologies do not take into account the principles of constructing various systems, as well as their problems. The analysis in Section 4 highlighted key deficiencies in existing research. Today, the existing methodologies cannot be categorized into any clearly defined categories that would focus on the confidentiality and integrity of the system. The absence of these categories does not lead to specific confidentiality and integrity issues being addressed in the system development process. This is one of the main obstacles to the development of system model formulation.

Author Contributions: Conceptualization, A.K.; methodology, A.S.; investigation, A.K., V.A. and A.N.; resources, A.S.; writing—original draft preparation, V.A. and A.N.; writing—review and editing, A.K. and M.K.; supervision, M.K.; project administration, A.K.; funding acquisition, A.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Ministry of Science and Higher Education of Russia, Government Order for 2020–2022, project no. FEWM-2020-0037 (TUSUR).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. ICT Facts and Figures 2017. Available online: https://www.itu.int/en/ITUD/Statistics/Pages/facts/default.aspx (accessed on 13 November 2021).
2. Craigen, D.; Diakun-Thibault, N.; Purse, R. Defining cybersecurity. *Technol. Innov. Manag. Rev.* **2014**, *4*, 13–21. [CrossRef]
3. Romashkina, N.P.; Zagorskii, A.V. *Information Security Threats during Crises and Conflicts of the XXI Century*; IMEMO: Moskow, Russia, 2016; p. 133.
4. Uzunov, A.V.; Fernandez, E.B. An extensible pattern-based library and taxonomy of security threats for distributed systems. *Comput. Stand. Interfaces* **2014**, *36*, 734–747. [CrossRef]
5. Bryant, B.D.; Saiedian, H. A novel kill-chain framework for remote security log analysis with SIEM software. *Comput. Stand. Interfaces* **2017**, *67*, 198–210. [CrossRef]
6. Zhu, Y.; Fu, X.; Graham, B.; Bettati, R.; Zhao, W. Correlation-Based Traffic Analysis Attacks on Anonymity Networks. *IEEE Trans. Parallel Distrib. Syst.* **2010**, *7*, 954–967. [CrossRef]
7. Dahbul, R.N.; Lim, C.; Purnama, J. Enhancing Honeypot Deception Capability Through Network Service Fingerprinting. *J. Phys. Conf. Ser.* **2017**, *801*, 012057. [CrossRef]
8. Sandro, G.; Hutinski, Z. Information System Security Threats Classifications. *J. Inf. Organ. Sci.* **2007**, *31*, 51–61.
9. Albakri, A.; Boiten, E.; de Lemos, R. Risks of Sharing Cyber Incident Information. In Proceedings of the ARES 2018: Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 27–30 August 2018; Volume 58, pp. 1–10.
10. Messe, N.; Chiprianov, V.; Belloir, N.; El-Hachem, J.; Fleurquin, R.; Sadou, S. Asset-Oriented Threat Modeling. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December–1 January 2021; pp. 1–11.
11. Meszaros, J.; Buchalcevova, A. Introducing OSSF: A framework for online service cybersecurity risk management. *Comput. Stand. Interfaces* **2017**, *65*, 300–313. [CrossRef]
12. Sion, L.; Yskout, K.; van den Berghe, A.; Scandariato, R.; Joosen, W. MASC: Modelling Architectural Security Concerns. In Proceedings of the 2015 IEEE/ACM 7th International Workshop on Modeling in Software Engineering, Florence, Italy, 16–17 May 2015; pp. 1425–1432.

13. Barrowclough, J.P.; Asif, R. Securing Cloud Hypervisors: A Survey of the Threats, Vulnerabilities, and Countermeasures. *Secur. Commun. Netw.* **2018**, *2018*, 1681908. [CrossRef]
14. Farahmand, F.; Navathe, S.B.; Enslow, P.H.; Sharp, G.P. Managing vulnerabilities of information systems to security incidents. *J. Manag. Inf. Syst.* **2008**, *25*, 241–280.
15. Ambalavanan, V. Cyber Threats Detection and Mitigation Using Machine Learning. In *Handbook of Research on Machine and Deep Learning Applications for Cyber Security*; IGI Global: Hershey, PA, USA, 2020; pp. 1–18.
16. Shah, N.F.; Kumar, P. A comparative analysis of various spam classifications. In *Progress in Intelligent Computing Techniques: Theory, Practice, and Applications*; Springer: Singapore, 2017; pp. 265–271.
17. Chandrasekar, C.; Priyatharsini, P. Classification techniques using spam filtering email. *Int. J. Adv. Res. Comput. Sci.* **2018**, *9*, 402–410. [CrossRef]
18. Shafi, M.A.; Latiff, M.S.A.; Chiroma, H.; Osho, O.; Abdul-Salaam, G.; Abubakar, A.I.; Herawan, T. A review on mobile SMS spam filtering techniques. *IEEE Access* **2017**, *5*, 15650–15666.
19. Chen, C.; Zhang, J.; Xie, Y.; Xiang, Y.; Zhou, W.; Hassan, M.M.; AlElaiwi, A.; Alrubaian, M. A performance evaluation of machine learning-based streaming spam tweets detection. *IEEE Trans. Comput. Soc. Syst.* **2015**, *2*, 65–76. [CrossRef]
20. Biggio, B.; Fumera, G.; Pillai, I.; Roli, F. A survey and experimental evaluation of image spam filtering techniques. *Pattern Recognit. Lett.* **2011**, *32*, 1436–1446. [CrossRef]
21. Kumar, A.D.; Vinayakumar, R.; Soman, K. DeepImageSpam: Deep Learning based Image Spam Detection. Available online: https://www.researchgate.net/publication/328189401_DeepImageSpam_Deep_Learning_based_Image_Spam_Detection (accessed on 17 November 2021).
22. Jusas, V.; Japertas, S.; Baksys, T.; Bhandari, S. Logical filter approach for early stage cyber-attack detection. *Comput. Sci. Inf. Syst.* **2019**, *16*, 491–514. [CrossRef]
23. Xin, Y.; Kong, L.; Liu, Z.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.; Wang, C. Machine learning and deep learning methods for cybersecurity. *IEEE Access* **2018**, *6*, 35365–35381. [CrossRef]
24. Gandotra, E.; Bansal, D.; Sofat, S. Malware analysis and classification: A survey. *J. Inf. Secur.* **2014**, *5*, 56–64. [CrossRef]
25. Dharamkar, B.; Singh, R. A review of cyber-attack classification technique based on data mining and neural network approach. *Int. J. Comput. Trends Technol. (IJCTT)* **2014**, *7*, 100–105. [CrossRef]
26. Hodo, E.; Bellekens, X.; Hamilton, A.; Tachtatzis, C.; Atkinson, R. Shallow and Deep Networks Intrusion Detection System: A Taxonomy and Survey. Available online: https://www.researchgate.net/publication/312170608_Shallow_and_Deep_Networks_Intrusion_Detection_System_A_Taxonomy_and_Survey (accessed on 17 November 2021).
27. Eder-Neuhauser, P.; Zseby, T.; Fabini, J. Malware propagation in smart grid networks: Metrics, simulation and comparison of three malware types. *J. Comput. Virol. Hacking Tech.* **2019**, *15*, 109–125. [CrossRef]
28. Ndibanje, B.; Kim, K.H.; Kang, Y.J.; Kim, H.H.; Kim, T.Y.; Lee, H.J. Cross-method-based analysis and classification of malicious behavior by api calls extraction. *Appl. Sci.* **2019**, *9*, 239. [CrossRef]
29. White, R.; Boult, T.; Chow, E. A computational asset vulnerability model for the strategic protection of the critical infrastructure. *Int. J. Crit. Infrastruct. Prot.* **2014**, *7*, 167–177. [CrossRef]
30. Yampolskiy, M.; Horvath, P.; Koutsoukos, X.D.; Xue, Y.; Sztipanovits, J. A language for describing attacks on cyber-physical systems. *Int. J. Crit. Infrastruct. Prot.* **2015**, *8*, 40–52. [CrossRef]
31. Lebek, B.; Uffen, J.; Neumann, M.; Hohler, B.; Breitner, M.H. Information security awareness and behavior: A theory-based literature review. *Manag. Res. Rev.* **2014**, *37*, 1049–1092. [CrossRef]
32. Ruiz, G.; Heymann, E.; Cesar, E.; Miller, B.P. Automating Threat Modeling through the Software Development Life-Cycle. Available online: https://research.cs.wisc.edu/mist/papers/Guifre-sep2012.pdf (accessed on 17 November 2021).
33. Braendeland, G.; Refsdal, A.; Stolen, K. Modular analysis and modelling of risk scenarios with dependencies. *J. Syst. Softw.* **2010**, *83*, 1995–2013. [CrossRef]
34. Gupta, B.; Agrawal, D.P.; Yamaguchi, S. Threats Classification: State of the Art. In *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*; IGI Global: Hershey, PA, USA, 2016; pp. 368–392.
35. Jouini, M.; Rabai, L.B.A. A Scalable Threats Classification Model in Information Systems. In Proceedings of the SIN '16: Proceedings of the 9th International Conference on Security of Information and Networks, Newark, NJ, USA, 20–22 July 2016; Association for Computing Machinery: New York City, NY, USA, 2016; pp. 141–144.
36. Khristolyubova, A.A.; Konev, A.A.; Shelupanov, A.A.; Solovev, M.L. Modeling threats to information security using IDEF0 methodology. In Proceedings of the IOP Conference Series Materials Science and Engineering, Tomsk, Russia, 23–26 April 2019; pp. 1–6.
37. Lindqvist, U.; Jonsson, E. How to systematically classify computer security intrusions. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 4–7 May 1997; pp. 1–10.
38. Gruschka, N.; Jensen, M. Attack surfaces: A taxonomy for attacks on cloud services. In Proceedings of the IEEE 3rd International Conference on Cloud Computing, Miami, FL, USA, 5–10 July 2010.
39. Sommer, F.; Durrwang, J.; Kriesten, R. Survey and Classification of Automotive Security Attacks. *Information* **2019**, *10*, 148. [CrossRef]
40. Koltays, A.; Konev, A.; Shelupanov, A. Mathematical Model for Choosing Counterparty When Assessing Information Security Risks. *Risks* **2021**, *9*, 133. [CrossRef]

41. Ashibani, Y.; Mahmoud, Q.H. Cyber physical systems security: Analysis, challenges and solutions. *Comput. Stand. Interfaces* **2017**, *68*, 81–97. [CrossRef]
42. James, K.I.A.; Prabakaran, R. Threat Modeling Framework for Electrical Distribution Scada Networks. *Middle-East J. Sci. Res.* **2015**, *23*, 2318–2325.
43. Zawoad, S.; Dutta, A.K.; Hasan, R. Towards Building Forensics Enabled Cloud Through Secure Logging-as-a-Service. *IEEE Trans. Dependable Secur. Comput.* **2016**, *13*, 148–162. [CrossRef]
44. Kalinin, M.O.; Konoplev, A.S. Formalization of Objectives of Grid Systems Resources Protection against Unauthorized Access. *Nonlinear Phenom. Complex Syst.* **2014**, *17*, 272–277.
45. Olayemi, O. Security issues in smart homes and mobile health system: Threat analysis, possible countermeasures and lessons learned. *Int. J. Inf. Technol. Secur.* **2017**, *9*, 31–52.
46. Rimsha, A.S.; Rimsha, K.S. The Problem of Selecting APCS' Information Security Tools. In *Cyber-Physical Systems: Industry 4.0 Challenges*; Springer: Cham, Switzerland, 2019; pp. 211–223.
47. STRIDE Threat Modeling: What You Need to Know. Available online: https://www.softwaresecured.com/stride-threat-modeling/ (accessed on 4 January 2022).
48. Real World Threat Modeling Using the PASTA Methodology. Available online: https://owasp.org/www-pdf-archive/AppSecEU2012_PASTA.pdf (accessed on 4 January 2022).
49. LINDDUN Privacy Engineering. Available online: https://www.linddun.org/ (accessed on 4 January 2022).
50. Common Vulnerability Scoring System. Available online: https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System (accessed on 4 January 2022).
51. Attack Tree. Available online: https://en.wikipedia.org/wiki/Attack_tree (accessed on 4 January 2022).
52. How Well Do You Know Your Personae Non Gratae. Available online: https://www.infoq.com/articles/personae-non-gratae/ (accessed on 4 January 2022).
53. Denning, T.A.; Friedman, B.; Kohno, T. The Security Cards. Available online: https://securitycards.cs.washington.edu/ (accessed on 10 December 2021).
54. The Hybrid Threat Modeling Method. Available online: https://insights.sei.cmu.edu/blog/the-hybrid-threat-modeling-method/ (accessed on 4 January 2022).
55. What is Threat Modeling: Process and Methodologies? Available online: https://www.simplilearn.com/what-is-threat-modeling-article (accessed on 4 January 2022).
56. Stride, VAST, Trike, & More: Which Threat Modeling Methodology is Right for Your Organization? Available online: https://threatmodeler.com/threat-modeling-methodologies-overview-for-your-business/ (accessed on 4 January 2022).
57. Octave Method of Security Assessment. Available online: https://technology.ku.edu/octave-method-security-assessment (accessed on 4 January 2022).
58. Threat Modeling: 12 Available Methods. Available online: https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/ (accessed on 4 January 2022).
59. Sion, L.; Wuyts, K.; Yskout, K.; van Landuyt, D.; Joosen, W. Interaction-based Privacy Threat Elicitation. In Proceedings of the 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, UK, 23–27 April 2018; pp. 1–8.
60. Ingalsbe, J.A.; Shoemaker, D.; Mead, N.R. Threat Modeling the Cloud Computing, Mobile Device Toting, Consumerized Enterprise—An overview of considerations. *AMCIS Proc.* **2011**, *359*. Available online: https://aisel.aisnet.org/amcis2011_submissions/359/ (accessed on 4 January 2022).
61. Khamparia, A.; Pandey, B. Threat driven modeling framework using petri nets for e-learning system. *SpringerPlus* **2016**, *5*, 446. [CrossRef] [PubMed]
62. Torkura, K.; Sukmana, M.; Meinig, M.; Kayem, A.; Cheng, F.; Graupner, H.; Meinel, C. Securing Cloud Storage Brokerage Systems Through Threat Models. In Proceedings of the IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), Krakow, Poland, 16–18 May 2018.
63. Wolf, A.; Simopoulos, D.; D'Avino, L.; Schwaiger, P. The PASTA threat model implementation in the IoT development life cycle. *INFORMATIK* **2020**, *2021*, 1195–1204.
64. Seifert, D.; Reza, H. A Security Analysis of Cyber-Physical Systems Architecture for Healthcare. *Computers* **2016**, *5*, 27. [CrossRef]
65. Zhi-Wei, T. OCTAVE-Based Risk Evaluation for E-Government Information Systems. *J. Univ. Electron. Sci. Technol. China* **2009**, *38*, 130–133.
66. Affia, A.O.; Matulevicius, R.; Tonisson, R. Security Risk Estimation and Management in Autonomous Driving Vehicles. In *International Conference on Advanced Information Systems Engineering*; Springer: Cham, Switzerland, 2021; pp. 11–19.
67. Robles-Gonzalez, A.; Parra-Arnau, J.; Forne, J. A LINDDUN-Based Framework for Privacy Threat Analysis on Identification and Authentication Processes. *Comput. Secur.* **2020**, *94*, 101755. [CrossRef]
68. Riva, G.M.; Vasenev, A.; Zannone, N. SoK: Engineering privacy-aware high-tech systems. In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES 2020), Dublin, Ireland, 25–28 August 2020; Volume 19, pp. 1–10.
69. Yin, X.C.; Liu, Z.G.; Nkenyereye, L.; Ndibanje, B. Toward an Applied Cyber Security Solution in IoT-Based Smart Grids: An Intrusion Detection System Approach. *Sensors* **2019**, *19*, 4952. [CrossRef]

70. Basin David, A.; Jurgen, D.; Torsten, L. Model driven security for process-oriented systems. In Proceedings of the SACMAT '03: Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies, Villa Gallia, Como, Italy, 2–3 June 2003; Association for Computing Machinery: New York, NY, USA, 2003; pp. 100–109.
71. Ahmed, U.; Raza, I.; Hussain, S.A.; Ali, A.; Iqbal, M.; Wang, X. *Modelling Cyber Security for Software-Defined Networks Those Grow Strong When Exposed to Threats*; Springer International Publishing: Cham, Switzerland, 2015; Volume 1, pp. 123–146.
72. Aissa, A.B.; Mohamed, I.A.; Hussein, L.F.; Elhadad, A. A Novel Stochastic Model for Cybersecurity Metric Inspired by Markov Chain Model and Attack Graphs. *Int. J. Sci. Technol. Res.* **2020**, *9*, 6329–6335.
73. Jiang, H.; Nagra, J.; Ahammad, P. Sok: Applying Machine Learning in Security. Available online: https://www.researchgate.net/publication/309854646_SoK_Applying_Machine_Learning_in_Security_-_A_Survey (accessed on 17 November 2021).
74. Apruzzese, G.; Colajanni, M.; Ferretti, L.; Guido, A.; Marchetti, M. On the effectiveness of machine and deep learning for cyber security. In Proceedings of the International Conference on Cyber Conflict (ICCC), 10th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 30 May–1 June 2018; pp. 1–16.
75. Ucci, D.; Aniello, L.; Baldoni, R. Survey of machine learning techniques for malware analysis. *Comput. Secur.* **2019**, *81*, 123–147. [CrossRef]
76. Bhuyan, S.S.; Kabir, U.Y.; Escareno, J.M.; Ector, K.; Palakodeti, S.; Wyant, D.; Kumar, S.; Levy, M.; Kedia, S.; Dasgupta, D.; et al. Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. *J. Med. Syst.* **2018**, *44*, 98. [CrossRef]
77. Ford, V.; Siraj, A. Applications of machine learning in cyber security. In Proceedings of the 27th International Conference on Computer Applications in Industry and Engineering 2014, Kota Kinabalu, Malaysia, 13 October 2014; pp. 1–6.
78. Ding, Q.; Zhu, R.; Liu, H.; Ma, M. An Overview of Machine Learning-Based Energy-Efficient Routing Algorithms in Wireless Sensor Networks. *Electronics* **2021**, *1539*, 1539. [CrossRef]
79. Cardenas, A.A.; Roosta, T.; Sastry, S. Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems. *Ad Hoc Netw.* **2009**, *7*, 1434–1447. [CrossRef]
80. Yan, S.; Malaney, R.; Nevat, I.; Peters, G.W. Optimal Information-Theoretic Wireless Location Verification. *IEEE Trans. Veh. Technol.* **2014**, *63*, 3410–3422. [CrossRef]
81. Churcher, A.; Ullah, R.; Ahmad, J.; Rehman, S.U.; Masood, F.; Gogate, M.; Alqahtani, F.; Nour, B.; Buchanan, W.J. An Experimental Analysis of Attack Classification Using Machine Learning in IoT Networks. *Sensors* **2021**, *21*, 446. [CrossRef] [PubMed]
82. Chmiel, M.; Korona, M.; Kozioł, F.; Szczypiorski, K.; Rawski, M. Discussion on IoT Security Recommendations against the State-of-the-Art Solutions. *Electronics* **2021**, *10*, 1814. [CrossRef]
83. Arseni, S.; Chifor, B.; Coca, M.; Medvei, M.; Bica, I.; Matei, I. RESFIT: A Reputation and Security Monitoring Platform for IoT Applications. *Electronics* **2021**, *10*, 1840. [CrossRef]
84. Apostol, I.; Preda, M.; Nila, C.; Bica, I. IoT Botnet Anomaly Detection Using Unsupervised Deep Learning. *Electronics* **2021**, *10*, 1876. [CrossRef]
85. Thaseen, I.S.; Mohanraj, V.; Ramachandran, S.; Sanapala, K.; Yeo, S. A Hadoop Based Framework Integrating Machine Learning Classifiers for Anomaly Detection in the Internet of Things. *Electronics* **2021**, *10*, 1955. [CrossRef]
86. Lagerstrom, R.; Baldwin, C.; MacCormack, A.; Dreyfus, D. Visualizing and Measuring Enterprise Architecture: An Exploratory BioPharma Case. In *IFIP Working Conference on The Practice of Enterprise Modeling*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 9–23.
87. Latif, R.; Abbas, H.; Assar, S.; Ali, Q. Cloud Computing Risk Assessment: A Systematic Literature Review. *Lect. Notes Electr. Eng.* **2014**, *276*, 285–295.
88. Razaque, A.; Frej, M.B.H.; Alotaibi, B.; Alotaibi, M. Privacy Preservation Models for Third-Party Auditor over Cloud Computing: A Survey. *Electronics* **2021**, *10*, 2721. [CrossRef]
89. Belapurkar, A.; Chakrabarti, A.; Ponnapalli, H.; Varadarajan, N.; Padmanabhuni, S.; Sundarrajan, S. *Distributed Systems Security: Issues, Processes and Solutions*; John Wiley & Sons: Hoboken, NJ, USA, 2009; p. 334.
90. Uzunov, A.V.; Fernandez, E.B.; Falkner, K. Engineering security into distributed systems: A survey of methodologies. *J. Univers. Comput. Sci.* **2012**, *18*, 2920–3006.
91. Uzunov, A.V.; Falkner, K.; Fernandez, E.B. A Comprehensive Pattern-Oriented Approach to Engineering Security Methodologies. *Inf. Softw. Technol.* **2015**, *57*, 217–247. [CrossRef]
92. Khan, R.; McLaughlin, K.; Laverty, D.; Sezer, S. STRIDE-based Threat Modeling for Cyber-Physical Systems. In Proceedings of the IEEE PES Innovative Smart Grid Technologies Conference Europe, Turin, Italy, 26–29 September 2017.
93. Scandariato, R.; Wuyts, K.; Joosen, W. A descriptive study of Microsoft's threat modeling technique. *Requir. Eng.* **2015**, *20*, 163–180. [CrossRef]
94. Sion, L.; Yskout, K.; van Landuyt, D.; Joosen, W. Solution-aware data flow diagrams for security threat modeling. In Proceedings of the 33rd Annual ACM Symposium on Applied Computing, Pau, France, 9–13 April 2018; pp. 1425–1432.
95. Honkaranta, A.; Leppanen, T.; Costin, A. Towards Practical Cybersecurity Mapping of STRIDE and CWE—A Multi-Perspective Approach. In Proceedings of the 29th Conference of Open Innovations Association (FRUCT), Tampere, Finland, 12–14 May 2021.
96. Karahasanovic, A.; Kleberger, P.; Almgren, M. Adapting Threat Modeling Methods for the Automotive Industry. In Proceedings of the 15th ESCAR Conference, Berlin, Germany, 7–8 November 2017.

97. Pell, R.; Moschoyiannis, S.; Panaousis, E. Multi-Stage Threat Modelling and Security Monitoring in 5GCN. In *Cybersecurity Issues in Emerging Technologies*; CRC Press: Boca Raton, FL, USA, 2021; pp. 59–76.
98. Lee, C.C.; Tan, T.G.; Sharma, V.; Zhou, J. Quantum Computing Threat Modelling on a Generic CPS Setup. In *International Conference on Applied Cryptography and Network Security*; Springer: Cham, Switzerland, 2021; pp. 171–190.
99. van Landuyt, D.; Joosen, W. A descriptive study of assumptions made in LINDDUN privacy threat elicitation. In Proceedings of the 35th Annual ACM Symposium on Applied Computing, Brno, Czech Republic, 30 March–3 April 2020; pp. 1–8.
100. Deng, M.; Wuyts, K.; Scandariato, R.; Preneel, B.; Joosen, W. A Privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements. *Requir. Eng.* **2011**, *16*, 3–32. [CrossRef]
101. Li, E.; Kang, C.; Huang, D.; Hu, M.; Chang, F.; He, L.; Li, X. Quantitative Model of Attacks on Distribution Automation Systems Based on CVSS and Attack Trees. *Information* **2019**, *10*, 251. [CrossRef]
102. Johnson, P.; Lagerstrom, R.; Ekstedt, M.; Franke, U. Can the Common Vulnerability Scoring System Be Trusted? A Bayesian Analysis. *IEEE Trans. Dependable Secur. Comput.* **2016**, *15*, 1002–1015. [CrossRef]
103. Mantha, B.; Jung, Y.; Garcia, B. Implementation of the Common Vulnerability Scoring System to Assess the Cyber Vulnerability in Construction Projects. In Proceedings of the Creative Construction Conference, Opatija, Croatia, 28 June–1 July 2020; pp. 117–124.
104. Czekster, R.M.; Morisset, C. BDMPathfinder: A tool for exploring attack paths in models defined by Boolean Logic Driven Markov Processes. In Proceedings of the European Dependable Computing Conference, Munich, Germany, 13–16 September 2021; pp. 83–86.
105. Falco, G.; Viswanathan, A.; Santangelo, A. CubeSat Security Attack Tree Analysis. In Proceedings of the 8th IEEE International Conference on Space Mission Challenges for Information Technology, Pasadena, CA, USA, 26–30 July 2021; pp. 1–9.
106. Mead, N.; Shull, F.; Spears, J.; Heibl, S.; Weber, S.; Cleland-Huang, J. Crowd Sourcing the Creation of Personae Non Gratae for Requirements-Phase Threat Modeling. In Proceedings of the IEEE 25th International Requirements Engineering Conference, Lisbon, Portugal, 4–8 September 2017; pp. 404–409.
107. Omotunde, H.; Ibrahim, R. A Hybrid Threat Model for Software Security Requirement Specification. In Proceedings of the International Conference on Information Science and Security, Pattaya, Thailand, 19–22 December 2016; pp. 1–4.
108. Luna, J.; Suri, N.; Krontiris, I. Privacy-by-design based on quantitative threat modeling. In Proceedings of the Risk and Security of Internet and Systems, Cork, Ireland, 10–12 October 2012; pp. 1–8.
109. Alberts, C.; Dorofee, A.; Stevens, J.; Woody, C. Introduction to the OCTAVE Approach. In *Introduction to the OCTAVE Approach*; Software Engineering Institute, Carnegie Mellon University: Pittsburgh, PA, USA, 2003.
110. Saitta, P.; Larcom, B.; Eddington, M. *Trike v.1 Methodology Document*. 2005. Available online: https://www.octotrike.org/papers/Trike_v1_Methodology_Document-draft.pdf (accessed on 4 January 2022).
111. Nhlabatsi, A.; Hussein, A.; Fetais, N.; Khan, K.M. Design and Implementation of a Threat-Specific Security Risk Assessment Tool. In Proceedings of the IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, 2–5 February 2020.
112. Falah, B.; Akour, M.; Oukemeni, S. An Alternative Threat Model-based Approach for Security Testing. *Int. J. Secur. Softw. Eng.* **2015**, *6*, 50–64. [CrossRef]
113. Aydin, M.M. *Engineering Threat Modelling Tools for Cloud Computing*; University of York, Computer Science: York, UK, 2016; p. 138.
114. Lenzini, G.; Mauw, S.; Ouchani, S. Security Analysis of Socio-Technical Physical Systems. In Proceedings of the STM 2016: Security and Trust Management, Heraklion, Crete, Greece, 26–27 September 2016; pp. 170–178.
115. Huang, Y.; Cardenas, A.A.; Aminb, S.; Linc, Z.; Tsai, H.; Sastry, S. Understanding the physical and economic consequences of attacks on control systems. *Int. J. Crit. Infrastruct. Prot.* **2009**, *2*, 73–83. [CrossRef]
116. Burmester, M.; Magkos, E.; Chrissikopoulos, V. Modeling Security in Cyber-Physical Systems. *Int. J. Crit. Infrastruct. Prot.* **2012**, *5*, 118–126. [CrossRef]
117. Baquero, A.O.; Kornecki, A.J.; Zalewski, J. Threat Modeling for Aviation Computer Security. In Proceedings of the 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, Austria, 31 August–2 September 2016.
118. Pan, J.; Zhuang, Y. PMCAP: A Threat Model of Process Memory Data on the Windows Operating System. *Secur. Commun. Netw.* **2017**, *2017*, 1–16. [CrossRef]
119. Abrams, M.D. *NIMS Information Security Threat Methodology*; MITRE Corporation: Bedford, MA, USA, 1998; pp. 1–35.
120. Novokhrestov, A.; Konev, A. Mathematical Model of Threats to Information Systems. In *AIP Conference Proceedings*; AIP Publishing LLC: Melville, NY, USA, 2016; pp. 1–4.
121. Alvaro, A.C.; Amin, S.; Sinopoli, B.; Perrig, A.; Sastry, S. Challenges for securing cyber physical systems. *Electr. Eng. Comput. Sci.* **2009**, *5*, 1–4.
122. Gaddam, N.; Kumar, G.S.A.; Somani, A.K. Securing Physical Processes against Cyber Attacks in Cyber-Physical Systems. In Proceedings of the National Workshop for Research on High-Confidence Transportation Cyber-Physical Systems: Automotive, Aviation & Rail, Tyson's Corner, VA, USA, 18–20 November 2008; pp. 1–3.
123. Myagmar, S.; Lee, A.J.; Yurcik, W. Threat modeling as a basis for security requirements. *Symposium on Requirements Engineering for Information Security (SREIS)*. 2005, pp. 1–8. Available online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.703.8462&rep=rep1&type=pdf (accessed on 4 January 2022).
124. Igure, V.M.; Laughter, S.A.; Williams, R.D. Security issues in SCADA networks. *Comput. Secur.* **2006**, *25*, 498–506. [CrossRef]
125. Shostack, A. *Threat Modeling*; John Wiley & Sons, Inc.: Indianapolis, Indiana; Toronto, ON, Canada, 2014; p. 626.

126. Novokhrestov, A.; Konev, A.; Shelupanov, A.; Buymov, A. Computer network threat modelling. *J. Phys. Conf. Ser.* **2020**, *1488*, 1–6. [CrossRef]
127. Barrere, M.; Hankin, C.; Nicolaou, N.; Eliades, D.G.; Parisini, T. Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies. *J. Inf. Secur. Appl.* **2020**, *52*, 102471. [CrossRef]
128. Novokhrestov, A.; Konev, A.; Shelupanov, A. Model of Threats to Computer Network Software. *Symmetry* **2019**, *11*, 1506. [CrossRef]
129. Egoshin, N.S.; Konev, A.A.; Shelupanov, A.A. A Model of Threats to the Confidentiality of Information Processed in Cyberspace Based on the Information Flows Model. *Symmetry* **2020**, *12*, 1840.
130. Pendergrass, J.C.; Heart, K.; Ranganathan, C.; Venkatakrishnan, V.N. *A Threat Table Based Approach to Telemedicine Security*; Western Michigan University: Kalamazoo, MI, USA, 2013; Volume 2, pp. 104–111.
131. Jiang, R.; Lu, R.; Wang, Y.; Luo, J.; Shen, C.; Shen, X. Energy-Theft Detection Issues for Advanced Metering Infrastructure in Smart Grid. *Tsinghua Sci. Technol.* **2014**, *19*, 105–120. [CrossRef]
132. IEEE Std 1471-2000. IEEE Recommended Practice for Architecture Description of Software-Intensive Systems. Available online: https://ieeexplore.ieee.org/document/875998 (accessed on 4 January 2022).
133. *ISO/IEC/IEEE 15288:2015*; Systems and Software Engineering–System Life Cycle Processes. International Organisation for Standardisation/International Electrotechnical Commissions/Institute of Electrical and Electronics Engineers: Geneva, Switzerland, 2015.