International Journal of Engineering Sciences & Research Technology

(A Peer Reviewed Online Journal)
Impact Factor: 5.164

IJESRT

RESEARCHERID
THOMSON REUTERS

[Ansari, *et al.*, 8(12): December, 2019]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

COMPARATIVE LITERATURE ANALYSIS ON SECURITY REQUIREMENTS ENGINEERING

Md Tarique Jamal Ansari[*1], Dhirendra Pandey[2] & Naseem Ahmad Khan[3]
[*1, 2, 3]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow India

DOI: 10.5281/zenodo.3596327

ABSTRACT

Security Requirements Engineering is one of the most important parts of the software development lifecycle that assist the software developer in developing a quality cost effective software application. Security requirements are the non-functional requirements which must be considered early in the software development lifecycle with functional requirements. However, elicitation of effective and efficient security requirements is not an easy task. There are several security requirements engineering techniques. This paper presents a comparative literature analysis of several existing security requirements engineering approaches for the development of secure software application. We discuss each existing security requirements engineering approach. We also comparatively analyze existing security requirements engineering approaches according to different criteria, such as the general approach and scope of the method, its validation, and quality assurance capabilities.

KEYWORDS: Software Security, Threat Modeling, Security Requirements Engineering, Non-Functional Requirements.

1. INTRODUCTION

The network of information technology and IT based application is increasing at a rapid speed. It also increases the complication of technological applications and its services. This involvement and dependency indicate that there is a respectively bigger chance of suffering software security attacks. Nowadays poorly build software systems are becoming very easy to attack by threats and attacker always tries to attack poorly build software systems. Furthermore, due to the heavy dependency of business organizations and many other governments sectors on different automatic software and IT based application systems, the consequences of a security attack in these software applications may range from broad economic losses to dangers to human life. This technological dependency demands a proper security requirements elicitation before the software development which results into a quality software product. Software security has consequently turned out to be an important issue and a reasonable amount of extra security proficiency is compulsory to meet non-functional requirements specifically the security requirements.

Security requirements elicitation at the requirements engineering phase is a vital concern for the development of quality software product. The security requirement engineer tries to elicit all the relevant security requirements in the early phase of software development lifecycle so that he can assist the developer in developing the secure software product and the developed software product continues to work properly under malicious attack. Stakeholders assist the security requirement engineer in identifying the asset, potential vulnerabilities, and threats [32]. The security requirements engineering process must be involved different apprehension of all stakeholders who have concern with security in software development process before the software can be built. Consideration for security at requirements engineering time is the new attention of the current world in recent days. Security Requirements Engineering is an emerging field of research in software engineering, with the realization that security must be analyzed early. Security is the major issue for assuring the quality full software so it must be achieved systematically through the various stages of the requirements engineering process. Since security is non-functional requirement many times it is ignored in the requirements phase of Software Development Life Cycle. But, it is easy to reduce software development cost and time to identify user security requirement at the very first stage of the software development process. The main deal is to present the user security requirements combining with user functional requirements which are collected from requirement phase

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

in Software Development Life Cycle (SDLC). The secure software develop will be ensured from the very beginning, if we can identify user security requirements and present these security requirements in requirements phase of software development.

The organization of this paper is as follows. Section 2 ''Review Method'' discusses the review method, which is based on some procedures. Section 3 ''Accepted Literatures for Review'' presents the selected literature for comparative literature review. Section 4 "Results and Discussion" presents the outcome of comparative literature review. Section 5 ''Conclusion'' summarizes our work.

2. REVIEW METHODS

In this paper, the literature review method for security requirements engineering is based on the sequential strategy. This section discusses the strategy for search, the sources, the study selection and the selection execution. The systematic review was used of the security requirements engineering literature, using a structure strategy in English language from 1996 to 2019. Search strategies were performed the following databases: Scopus, Web of Science, DOAJ, EBSCO, OCLC, Google Scholar, Yahoo, Eric, Google books, Proquest, JSTOR. ACM digital library, IEEE digital library, Science Direct, SREIS symposium, ESORICS symposium, REFSQ conference, DEXA conference, WOSIS workshop, ICCSA conference, Requirements Engineering Journal, IEEE International Requirements Engineering Conference, ICSE conference, COMPSAC conference. Major search keywords consist of: Nonfunctional requirements, Security requirements, Security requirements engineering, requirements engineering, security engineering, secure development, secure IS development, secure software development. Research publications selected based on the inclusion /exclusion criteria. Inclusion criteria include criteria pertaining to publication characteristics, such as full text published, peer reviewed publication, English language publication. Exclusion criteria include duplicate publications, asymmetric information and research with a focus on information and communication technology removed.

The database search for the literature of security requirements engineering produced 5266 papers. However, after analyzing the literature search result on the basis of paper title, 3035 duplicated studies excluded. After removing duplicate papers, 1685 papers are screened by title/abstract and 546 papers are screened on the basis of full text. Again, after reviewing abstract and full text literatures, 1670 papers are excluded by title/abstract and 533 papers are excluded on the basis of full text. At last, in the literature inclusion/exclusion process, total 29 research papers met the inclusion criteria. The accepted literature data for comparative analysis is presented in Table 1.

Table 1 Selected security requirements engineering literature for comparative review

S. No.	Author(s)	Title	Type	Year	Citation
1	AI Anton	Goal-based requirements analysis	Conference	1996	754
2	McDermott & Fox	Using abuse case models for security requirements analysis	Conference	1999	527
3	Yu & Liu	Modelling trust for system design using the i* strategic actors framework	Conference	2001	157
4	Lodderstedt, Basin, &Doser	SecureUML: A UML-based modeling language for model-driven security	Conference	2002	912
5	Jürjens	UMLsec: Extending UML for secure systems development	Conference	2002	809
6	Toval, Nicolás, Moros&García	Requirements reuse for improving information systems security: a practitioner's approach	Journal	2002	144
7	den Braber, Dimitrakos,	The CORAS methodology: model-based risk assessment	Book Chapter	2003	55

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

	Gran, Lund, Stolen &Aagedal	using UML and UP			
8	Firesmith	Security use cases	Journal	2003	263
9	Lin, Nuseibeh, Ince, & Jackson	Using abuse frames to bound the scope of security problems	Conference	2004	88
10	Zuccato	Holistic security requirement engineering for electronic commerce	Journal	2004	50
11	Mead and Stehney	Security quality requirements engineering (SQUARE) methodology	Technical Report	2005	354
12	Sindre and Opdahl	Eliciting security requirements with misuse cases	Journal	2005	1172
13	Mayer, Rifaut& Dubois	Towards a risk-based security requirements engineering framework	Workshop	2005	70
14	Myagmar, Lee &Yurcik	Threat modeling as a basis for security requirements	Symposium	2005	272
15	Peeters	Agile security requirements engineering	Symposium	2005	54
16	Viega	Building security requirements with CLASP	Notes	2005	59
17	Asnar&Giorgini	Modelling risk and identifying countermeasure in organizations	Workshop	2006	89
18	Mellado, Fernández-Medina &Piattini	Applying a security requirements engineering process	Symposium	2006	64
19	Tsoumas and Gritzalis	Towards an ontology-based security management	Conference	2006	142
20	Gürses& Santen	Contextualizing Security Goals: A Method for Multilateral Security Requirements Elicitation	Journal	2006	19
21	Mouratidis&Giorgini	Secure tropos: a security-oriented extension of the tropos methodology	Journal	2007	348
22	Lamsweerde	Engineering requirements for system reliability and security	Book Chapter	2007	44
23	Hatebur, Heisel& Schmidt	A security engineering process based on patterns	Workshop	2007	41
24	Hussein and Zulkernine	Intrusion detection aware component-based systems: A specification-based framework	Journal	2007	34
25	Haley, Laney, Moffett &Nuseibeh	Security requirements engineering: A framework for representation and analysis	Journal	2008	421
26	Salini&Kanmani	Model oriented security	Conference	2013	14

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

		requirements engineering (MOSRE) framework for web applications			
27	Paja, Dalpiaz&Giorgini	Modelling and reasoning about security requirements in socio-technical systems	Journal	2015	30
28	Riaz, Stallings, Singh, Slankas& Williams	DIGS – A Framework for Discovering Goals for Security Requirements Engineering	Symposium	2016	14
29	Ansari, M. T. J., Pandey, D., &Alenezi, M	STORE: Security Threat Oriented Requirements Engineering Methodology	Journal	2019	05

3. ACCEPTED LITERATURE FOR REVIEW

After applying inclusion/exclusion criteria on available literature on security requirement engineering approaches, 29 research papers are accepted for comparative analysis. Information extracted from these research papers must contain the proposed approach, procedures, methods, steps, strategies or any kind of creativity to elicit security requirements in an effective and efficient way during the early phases of software development. The information forms defined for this systematic review will contain the study identification, the study methodology, the study results, the study problems and our general impressions and abstractions. Regarding the study methodology, we shall focus on the modeling of the security requirements, on the modelling / development standard and on the security standards, along with the technical criteria defined within the analytical framework explained in the following section. The following sub-section provides a brief outline of each of the selected studies/initiatives shown in the previous section, according to the extracted information obtained through the information forms.

a. Goal-based requirements analysis

Annie I. Anton proposed goal based requirements analysis. She has discussed goal from the viewpoint of goal analysis and goal evolution. She developed and reviewed his experiences in applying our method to a relatively large example. She also validated some of the problems that experts face when using a goal-based approach to identify the requirements for a system [1].

b. Using abuse case models for security requirements analysis

McDermott and Fox proposed a new technique of capturing and analyzing of security requirements in an easy way with the help of object oriented modeling technique. They used use cases to model abuse cases. An abuse case model is easily understood by the users, customers and developers who understand either use case models or UML [19].

c. Modelling trust for system design using the i* strategic actors framework

Yu and Liu have developed the i*framework to support requirement analysis and high-level design in an agent-oriented system development paradigm. This framework models intentional dependency relationships between different strategic actors and their rationales. These actors depend on each other for goals to be accomplished, tasks to be achieved, and resources to be well-appointed [28].

d. Secure UML: A UML-based modeling language for model-driven security

Lodderstedtet. al. presented a modeling language for the model-driven development of secure and distributed software system founded on the Unified Modeling Language (UML). This method is constructed on role-based access control with additional support for specifying authorization constraints. They presented how UML can be used to identify information related to access control in the overall design of an application and how this information can be used to automatically generate complete access control infrastructures. This approach can be used to improve efficiency during the development of secure distributed systems and the quality of the resulting systems [11].

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

e. UML sec: Extending UML for secure systems development

Jürjens intended to aid the problematic task of developing security-critical systems in an approach based on the notation of the Unified Modeling Language (UML). They presented the extension of UML know as UMLsec defined in form of a UML profile using the standard UML extension mechanisms. The UMLsec permits fast security relevant information inside the diagrams in a system specification. The related constraints give standards to assess the security aspects of a system design, by mentioning to a formal semantics of a basic fragment of UML [15].

f. Requirements reuse for improving information systems security: a practitioner's approach

Tovalet. al. presented an applied technique to elicit and specify the system and software requirements with a source comprising reusable requirements, a spiral process model and a set of requirements templates. This technique is absorbed on the security of information systems and, thus, the reusable requirements repository contains all the requirements taken from MAGERIT, the Spanish public administration risk analysis and management method, which conforms to ISO 15408, Common Criteria Framework. Any information system together with these security requirements must consequently pass a risk analysis and management study performed with MAGERIT [23].

g. The CORAS methodology: model-based risk assessment using UML and UP

Den Braber el. al. introduced the CORAS methodology. This methodology combined Unified Modeling Language (UML) and Unified Process (UP) together to assist the model-based risk assessment on security-critical systems. In the CORAS methodology, an outdated risk management process is combined with UP, which is a well-accepted system development process. The CORAS methodology attempts to express how UML can contribute to better understanding, documentation, and communicating during the different phases of the risk management process. The CORAS methodology addresses both systems under development and systems already in use [2].

h. Security use cases

Use cases are mostly used modeling method for engineering functional requirements but they are often misrepresented when engineering non-functional requirements like security requirements because requirements engineers unreasonably specify security architectural mechanisms instead of security requirements. Misuse cases are extremely effective technique of investigating security threats but are unsuitable for the analysis and specification of security requirements. Fire smith presented Security use cases which used to specify requirements that the application shall successfully protect itself from its relevant security threats. He offers some steps which allow security requirements to be defined from reusable templates [12].

i. Using abuse frames to bound the scope of security problems

Lin et. al. have revised a proven object-oriented modeling technique, use cases, to identify and analyze security requirements in an easy way. They call this revision an abuse case model. From a user viewpoint the relationship of abuse cases to other security engineering work products is relatively easy [7].

j. Holistic security requirement engineering for electronic commerce

Zuccato has proposed an approach named ''holistic security requirement engineering''. This approach is intended to identify security requirements according to system- theoretic considerations. This shows that security requirements can be defined with the help of investigations in the business environment, workshops with stakeholders and risk analysis. This multidimensional approach leads to a holistic understanding of the requirements that fit into the system development life cycles [18].

k. Security quality requirements engineering (SQUARE) methodology

Mead and Stehney have presented the Security Quality Requirements Engineering (SQUARE) Methodology for identifying and prioritizing security requirements for software development projects. The SQUARE methodology developed under NSS program, is a nine steps process, The NSS Program continues to develop SQUARE, which has proven effective in helping organizations understand their security posture and produce products with supportable security requirements [26].

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

l. Eliciting security requirements with misuse cases

Sindre and Opdahl presented a systematic method to identifying security requirements based on use cases, with importance on description and method procedures. This method extends traditional use cases to also cover misuse, and is potentially beneficial for numerous other types of additional-functional requirements beyond security [27].

m. Towards a risk-based security requirements engineering framework

Mayer et. al. presented, that using and adapting an appropriate set of existing tools and techniques of risk analysis methods, improves the effectiveness of an iterative security engineering method starting at the earliest stage of IS development [6].

n. Threat modeling as a basis for security requirements

Myagmaret. al. investigated how threat modeling can be used as foundations for the specification of security requirements. They observed the variances between modeling software products and complex systems, and outline their approach for identifying threats of networked systems. They also presented three case studies of threat modeling: Software-Defined Radio, a network traffic monitoring tool, and a cluster security monitoring tool [14].

o. Agile security requirements engineering

Agile procedures have been believed inappropriate for security sensitive software development as the inflexibilities of assurance are realized to conflict with the lightweight and informal nature of agile processes. Though, such deceptively conflicting demands may be acquiescent by presenting the new conception of abuser stories in the requirements domain. Peeters has extended the agile practices to deal with security in an informal, communicative and assurance driven spirit. These extend the well-established idea of user stories to accomplish security requirements traceability and thus open the door to effective security assurance, exactly because of their informal and lightweight nature [17].

p. Building security requirements with CLASP

Viega presented how to develop security requirements in a structured manner that is encouraging to iterative modification and, if followed properly, metrics for evaluation. He has provided a framework that is an understandable development over traditional methods that do not consider security at all. He also delivered an example using a simple three-tiered architecture. The methodology he documented is a subset of CLASP, a set of process pieces for application security [24].

q. Modeling risk and identifying countermeasure in organizations

The Tropos framework has been proved effective in modeling strategic interests of the stakeholders at organizational level. Asnar & Giorgini have introduced the extended Tropos goal model to analyses risk at organization level and they also demonstrated a number of different techniques to help the analyst in identifying and enumerating relevant countermeasures for risk mitigation [4].

r. Applying a security requirements engineering process

Melladoet. al. presented SREP (Security Requirements Engineering Process), which is a standard-centred process and a reuse-based approach which deals with the security requirements at the earlier stages of software development in a systematic and intuitive way by providing a security resources repository and by integrating the Common Criteria into the software development lifecycle [10].

s. Towards an ontology-based security management

Tsoumas and Gritzalis have presented a security management framework of an arbitrary information system (IS) which builds upon knowledge-based resources, such as security ontology (SO) providing reusable security knowledge interoperability, aggregation and reasoning exploiting security knowledge from diverse sources; in addition, the separation of security requirements from their technical implementations facilitates the security management. They also provided a feasible framework, which links the high-level policy statements and deployable security controls and facilitates the security expert's work [16].

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

t. Contextualizing Security Goals: A Method for Multilateral Security Requirements Elicitation

Gürses and Santen have introduced a method that integrates the process of identifying security requirements of the end-users into the requirements elicitation process of a multilaterally secure system. Throughout the method emphasis is put on contextualizing security goals by analyzing the different viewpoints like whose security goal is it? against whom? for which functionality? which other users have a mutual interest in or conflict with the given security goal?[21].

u. Secure tropos: a security-oriented extension of the tropos methodology

Mouratidis & Giorgini have introduced extensions to the Tropos methodology to enable it to model security concerns throughout the whole development process. A description of the new concepts and modelling activities is given along with a discussion on how these concepts and modelling activities are integrated to the current stages of Tropos. They used a real life case study from the health and social care sector is used to demonstrate the approach [25].

v. Engineering requirements for system reliability and security

Van Lamsweerde overviews a systematic, goal-oriented approach to requirements engineering for high-assurance systems. The target of this approach is a complete, consistent, adequate, and structured set of software requirements and environment assumptions. The approach is model-based and partly relies on the use of formal methods when and where needed for RE-specific tasks, notably, goal refinement and operationalization, analysis of hazards and threats, conflict management, and synthesis of behavior models. The method, known as Keep All Objectives Satisfied (KAOS), has been developed and refined for more than fifteen years of research, tool development, and experience in multiple industrial projects [29].

w. A security engineering process based on patterns

Hateburet. al. have presented a security engineering process based on security problem frames and concretized security problem frames. Both kinds of frames constitute patterns for analyzing security problems and associated solution approaches. They are arranged in a pattern system that makes dependencies between them explicit. They also described step-by-step how the pattern system can be used to analyze a given security problem and how solution approaches can be found [8].

x. Intrusion detection aware component-based systems: A specification-based framework

Hussein & Zulkernine present a framework for developing components with intrusion detection capabilities. This framework uses UML intr, a UML profile for intrusion specifications. The profile allows developers to specify intrusion scenarios using UML diagrams. Specifying intrusion scenarios using the same language that is used for specifying software behavior eliminates the need for separate languages for describing intrusions. Other software specification languages can be easily adopted into this framework. The outcome of this framework is components equipped with intrusion detectors [13].

y. Security requirements engineering: A framework for representation and analysis

Haley et. al. presents a framework for security requirements elicitation and analysis. This framework is based on constructing a context for the system, representing security requirements as constraints, and developing satisfaction arguments for the security requirements. The system context is described using a problem-oriented notation, then is validated against the security requirements through construction of a satisfaction argument. The satisfaction argument consists of two parts: a formal argument that the system can meet its security requirements and a structured informal argument supporting the assumptions expressed in the formal argument. The construction of the satisfaction argument may fail, revealing either that the security requirement cannot be satisfied in the context or that the context does not contain sufficient information to develop the argument [9].

z. Model oriented security requirements engineering (MOSRE) framework for web applications

Salini & Kanmani have proposed a Model oriented framework to Security Requirement Engineering (MOSRE) for Web Applications and applied MOSRE framework for E-Voting system. By applying Modeling technologies to Requirement phases, the Security requirements and domain knowledge can be captured in a well-defined model and it is better than traditional process [20].

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

aa. Modelling and reasoning about security requirements in socio-technical systems

Pajaet. al propose the STS approach for modelling and reasoning about security requirements. In STS, security requirements are specified, via the STS-ml requirements modelling language, as contracts that constrain the interactions among the actors in the socio-technical system. The requirements models of STS-ml have a formal semantics which enables automated reasoning for detecting possible conflicts among security requirements as well as conflicts between security requirements and actors' business policies. They also applied STS to a case study about e-Government, and report on promising scalability results of our implementation [22].

bb. DIGS – A Framework for Discovering Goals for Security Requirements Engineering

Riazet. al. developed Discovering Goals for Security (DIGS) framework, which models the key entities in information security, including assets and security goals. They systematically developed a set of security goal patterns that capture multiple dimensions of security for assets. DIGS explicitly captures the relations and assumptions that underlie security goals to elicit implied goals. They map the goal patterns to NIST controls to help in operationalizing the goals. They also evaluated DIGS via a controlled experiment where 28 participants analyzed systems from mobile banking and human resource management domains [30].

cc. STORE: Security Threat Oriented Requirements Engineering Methodology

Ansari et. al. presented the STORE Methodology which is a ten-step sequential security requirements engineering methodology. This methodology is based on security threats analysis, which includes the identification of four points: PoA, PoB, PoC and PoD for effective security attack analysis. The STORE methodology identifies and priorities all such stakeholders based on their importance. The STORE methodology considers security threats for identifying security requirements with the help of potential stakeholders [32].

4. RESULTS AND DISCUSSION

The following Table 2, shows the comparative analysis of different security requirements approaches. After our analysis we have reached on the result that each of the selected initiatives provides us with highly important aspects that have to do with security requirements engineering. This is the summary that can be used as the basis for new methodologies / approaches / frameworks / techniques or as extensions to those approaches that already exist.

Table 2 Comparative analysis of different security requirements engineering approaches

SRE approaches	Initiative	Year	Standard	Based on	Contribution
GBRAM [1]	AI Anton	1996	-	Goal based	Formulate privacy and security policies using heuristic activities
Abuse Cases [19]	McDermott	1999	-	Abuse Cases	Develop abuse cases with the help of use cases to capture and analyze security requirements in a simple way.
Secure i* [28]	Yu	2001	-	Business process modeling, Software process modelling	i* framework for modelling and reasoning about organizational environments and their information systems
SecureUML [11]	Lodderstedt et. al.	2002	-	Model Driven Architecture	Secure UML (security modelling language for formalizing access control requirements based on UML)
UML Sec [15]	Jürjens	2002	ISO/IEC 15408,	Unified Process	UML Sec (UML extension for secure systems

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

			ISO/IEC 27001, ISO/IEC 17799, ISO/IEC 13335, IEEE 830-1998		development)
SIREN [23]	Toval et. al.	2002	IEEE 830-1998, IEEE-1233, IEEE-1207.1 and partially ISO/IEC 15408	Spiral process	Present a practical method to elicit and specify the system and software requirements
CORAS [2]	F den Braber et. Al.	2003	ISO 31000	Model based Sequential Process	Combined UML and Unified Process (UP) together to assist the model-based risk assessment
Security use cases [12]	Firesmith	2003	ISO/IEC 9126-1 and 9126-2	Conducted by assets and risk	Security use cases (UML extension for modelling security requirements in use case diagrams)
Abuse frames[7]	Lin et. al.	2004	ISO 13335	Object oriented	Object-oriented modeling technique, use cases, to identify and analyze security requirements
Holistic SRE [18]	Zuccato	2004	ISO/IEC 15408, ISO/IEC 17799, ISO 9000:2000, ISO/IEC 13335	Unified Process	Elicit security requirements according to system-theoretic considerations
SQUARE [26]	Mead and Stehney	2005	-	Sequential Process	SQUARE: 9-step process for eliciting, categorizing, and prioritizing security requirements
Misuse cases [27]	Sindre and Opdahl	2005	-	Threats and risks	Extends traditional use cases to cover misuse actions.
ISSRM [6]	Mayer et. al.	2005	ISO 27001	Sequential Process	Improves the effectiveness of an iterative security engineering method
Threat Based SRE [14]	Myagmar et al.	2005	-	Threat modeling based	Threat modeling based approach for SRE
Abuser stories [17]	Peeters	2005	-	Agile requirements engineering	Extended the agile practices to deal with security in an informal

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

CLASP [24]	Viega	2005	-	Resource-centric	CLASP: handles security requirements through a structured walkthrough of resources
Tropos Goal-Risk [4]	Asnar & Giorgini	2006	-		Extended Tropos goal model to analyses risk.
SREP [10]	Mellado el al.	2006	CC	Asset based and Risk driven	Standard-centred process and a reuse-based approach which deals with the security requirements.
Security ontology [16]	Tsoumas and Gritzalis	2006	CRAMM, COBIT	ontologies	A security ontology which extends the DMTF Common Information Model (CIM)
MSRA [21]	Gürses	2006	-	Multilateral security requirements	Integrates the process of identifying security requirements of the end-users into the requirements elicitation process
Secure Tropos [25]	Mouratidis & Giorgini	2007	ISO/IEC 17799	Agent oriented software development	Methodology Tropos Framework for modelling and analyzing security and trust requirements
KAOS [29]	Lamsweerde	2007			Use of antimodels to elaborate security requirements
SEPP [8]	Hatebur el. al.	2007	CC		SRE based on security problem frames and concretized security problem frames.
UMLintr [13]	Hussein and Zulkernine	2007	-	Component-Based Software Engineering	UMLintr (UML profile for intrusion identifications)
SREF [9]	Haley et. al.	2008	-		framework for security requirements elicitation and analysis
MOSRE [20]	Salini & Kanmani	2013	-	Model based	Model oriented framework for SRE
STS [22]	Paja et. al.	2015	-		Approach for modelling and reasoning about security requirements
DIGS [30]	Riaz et. al.	2016	-	Security Goal based	Framework, which models the key entities in information security, including assets and security goals.
STORE [32]	Ansari et. al.	2019	-	Security Threat	A ten step SRE approach based on security threats for complete and well-organized security requirements elicitation.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

This literature review provides us with reliable outcomes about security requirements engineering approaches which cannot be disproved, since it has been conducted in a pre-defined review method. Finally, regardless of requiring more effort than traditional reviews, this pre-defined review method based delivers us with more effective results without any issue. Therefore, we have presented a reasonable assessment of security requirements engineering by using a pre-defined review method.

5. CONCLUSION

In this paper, we have reviewed all the most applicable existing security requirements engineering approaches developed by several authors. This paper provides a summary of all existing information about security requirements engineering in a systematic and balanced manner. The main contribution of this work in comparison to former traditional reviews is that it includes approximately all security requirements engineering approaches till now therefore the precision and reliability of the information and the results obtained shows in a systematic manner. Furthermore, we should understand that the most important lesson from this literature review that if security requirements are elicited in the early stages and as functional requirements following any of the Security Requirements Engineering methods, we can achieve a software system with threat free and reduced vulnerabilities. In software organizations, with these approaches, the security requirements can be identified for software applications and the level of security reached by adopting Security Requirements Engineering.

REFERENCES

[1] Anton, A. I. (1996, April). Goal-based requirements analysis. In *Requirements Engineering, 1996., Proceedings of the Second International Conference on* (pp. 136-144). IEEE.
[2] Den Braber, F., Dimitrakos, T., Gran, B. A., Lund, M. S., Stolen, K., & Aagedal, J. O. (2003). The CORAS methodology: model-based risk assessment using UML and UP. In *UML and the Unified Process* (pp. 332-357). IGI Global.
[3] Den Braber, F., Hogganvik, I., Lund, M. S., Stølen, K., & Vraalsen, F. (2007). Model-based security analysis in seven steps—a guided tour to the CORAS method. *BT Technology Journal*, *25*(1), 101-117.
[4] Asnar, Y., &Giorgini, P. (2006, August). Modelling risk and identifying countermeasure in organizations. In *International Workshop on Critical Information Infrastructures Security* (pp. 55-66). Springer, Berlin, Heidelberg.
[5] Asnar, Y., Giorgini, P., Massacci, F., & Zannone, N. (2007, April). From trust to dependability through risk analysis. In *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on* (pp. 19-26). IEEE.
[6] Mayer, N., Rifaut, A., & Dubois, E. (2005, June). Towards a risk-based security requirements engineering framework. In *Workshop on Requirements Engineering for Software Quality. In Proc. of REFSQ* (Vol. 5).
[7] Lin, L., Nuseibeh, B., Ince, D., & Jackson, M. (2004, September). Using abuse frames to bound the scope of security problems. In *Requirements Engineering Conference, 2004. Proceedings. 12th IEEE International* (pp. 354-355). IEEE.
[8] Hatebur, D., Heisel, M., & Schmidt, H. (2007, September). A security engineering process based on patterns. In *Database and Expert Systems Applications, 2007. DEXA'07. 18th International Workshop on* (pp. 734-738). IEEE.
[9] Haley, C., Laney, R., Moffett, J., & Nuseibeh, B. (2008). Security requirements engineering: A framework for representation and analysis. *IEEE Transactions on Software Engineering*, *34*(1), 133-153.
[10] Mellado, D., Fernández-Medina, E., & Piattini, M. (2006, September). Applying a security requirements engineering process. In *European Symposium on Research in Computer Security* (pp. 192-206). Springer, Berlin, Heidelberg.
[11] Lodderstedt, T., Basin, D., &Doser, J. (2002, September). Secure UML: A UML-based modeling language for model-driven security. In *International Conference on the Unified Modeling Language* (pp. 426-441). Springer, Berlin, Heidelberg.
[12] Firesmith, D. G. (2003). Security use cases. *Journal of object technology*, *2*(3).
[13] Hussein, M., & Zulkernine, M. (2007). Intrusion detection aware component-based systems: A specification-based framework. *Journal of Systems and Software*, *80*(5), 700-710.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

[14] Myagmar, S., Lee, A. J., & Yurcik, W. (2005, August). Threat modeling as a basis for security requirements. In *Symposium on requirements engineering for information security (SREIS)*(Vol. 2005, pp. 1-8).
[15] Jürjens, J. (2002, September). UMLsec: Extending UML for secure systems development. In *International Conference on The Unified Modeling Language* (pp. 412-425). Springer, Berlin, Heidelberg.
[16] Tsoumas, B., & Gritzalis, D. (2006, April). Towards an ontology-based security management. In *Advanced Information Networking and Applications, 2006. AINA 2006. 20th International Conference on* (Vol. 1, pp. 985-992). IEEE.
[17] Peeters, J. (2005, August). Agile security requirements engineering. In *Symposium on Requirements Engineering for Information Security*.
[18] Zuccato, A. (2004). Holistic security requirement engineering for electronic commerce. *Computers & Security*, *23*(1), 63-76.
[19] McDermott, J., & Fox, C. (1999). Using abuse case models for security requirements analysis. In *Computer Security Applications Conference, 1999.(ACSAC'99) Proceedings. 15th Annual* (pp. 55-64). IEEE.
[20] Salini, P., & Kanmani, S. (2013). Model oriented security requirements engineering (MOSRE) framework for web applications. In *Advances in Computing and Information Technology* (pp. 341-353). Springer, Berlin, Heidelberg.
[21] Gürses, S. F., & Santen, T. (2006). Contextualizing Security Goals: A Method for Multilateral Security Requirements Elicitation. In *Sicherheit* (Vol. 6, pp. 42-53).
[22] Paja, E., Dalpiaz, F., & Giorgini, P. (2015). Modelling and reasoning about security requirements in socio-technical systems. *Data & Knowledge Engineering*, *98*, 123-143.
[23] Toval, A., Nicolás, J., Moros, B., &García, F. (2002). Requirements reuse for improving information systems security: a practitioner's approach. *Requirements Engineering*, *6*(4), 205-219.
[24] Viega, J. (2005, May). Building security requirements with CLASP. In *ACM SIGSOFT Software Engineering Notes* (Vol. 30, No. 4, pp. 1-7). ACM.
[25] Mouratidis, H., & Giorgini, P. (2007). Secure tropos: a security-oriented extension of the tropos methodology. *International Journal of Software Engineering and Knowledge Engineering*, *17*(02), 285-309.
[26] Mead, N. R., & Stehney, T. (2005). *Security quality requirements engineering (SQUARE) methodology* (Vol. 30, No. 4, pp. 1-7). ACM.
[27] Sindre, G., & Opdahl, A. L. (2005). Eliciting security requirements with misuse cases. *Requirements engineering*, *10*(1), 34-44.
[28] Yu, E., & Liu, L. (2001). Modelling trust for system design using the i* strategic actors framework. In *Trust in Cyber-societies* (pp. 175-194). Springer, Berlin, Heidelberg.
[29] Van Lamsweerde, A. (2007). Engineering requirements for system reliability and security. *NATO Security Through Science Series D-Information and Communication Security*, *9*, 196.
[30] Riaz, M., Stallings, J., Singh, M. P., Slankas, J., & Williams, L. (2016, September). DIGS: A framework for discovering goals for security requirements engineering. In *Proceedings of the 10th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement* (p. 35). ACM.
[31] Coats, D. R. (2018). *Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community*. Office of the Director of National Intelligence.
[32] Ansari, M. T. J., Pandey, D., & Alenezi, M. (2018). STORE: Security Threat Oriented Requirements Engineering Methodology. *Journal of King Saud University-Computer and Information Sciences*.