

Dear visitor!

The SQLab team have prepared a supplementary material related to the paper entitled: “**A Systematic Mapping Study on Intrusion Alert Analysis in Intrusion Detection Systems**”.

To access the PDF file of the supplementary material ([AC-SupMat.pdf](#)), please contact us with your name, official email, and your specific request.

The [AC-SupMat](#) document has the following contents:

Chapter 1 .....	8
Conducting the Search .....	8
Figure 1-1: The SMS Process .....	9
Table 1-1: The Related Aims and Scopes .....	10
Figure 1-2: The Search Strategy .....	11
Figure 1-3: The Finding Process of the Included Search Spaces Set from Initial Set .....	12
Table 1-2: The Secondary Studies used for Generating Initial Set of our SMS .....	13
Table 1-3: Aims and Scopes of the Journals .....	14
Table 1-4: Candidate Journals .....	31
Table 1-5: Aims and Scopes about Conferences .....	35
Table 1-6: Candidate Conferences .....	71
Table 1-7: Aims and Scopes about the Workshops .....	76
Table 1-8: Candidate Workshops .....	97
Table 1-9: Search Spaces Statistics .....	100
Table 1-10: Journal Papers .....	101
Table 1-11: Conference Papers .....	105
Table 1-12: Workshop Papers .....	110
Table 1-13: Journals Statistics .....	113
Table 1-14: Conferences Statistics .....	116
Table 1-15: Workshops Statistics .....	120
Chapter 2 .....	122
Evaluating the Search .....	122
Table 2-1: Related Ph.D and M.Sc Theses .....	123
Table 2-2: Related Books and Book Chapters .....	126
Table 2-3: Related Patents .....	128
Table 2-4: Intrusion Alerts Analysis Selected Projects .....	135
Table 2-5: List of Pioneer Researchers .....	137
Table 2-6: Data Extracted for the Evaluation Phase .....	139
Table 2-7: Found Search Spaces during Evaluation Phase .....	142
Chapter 3 .....	143
Analysis and Results .....	143
Figure 3-1: Level One Topic Detection Process .....	145
Table 3-1: Top Frequent Keywords of the Included Studies .....	146

Table 3-2: Co-occurrence Matrix for Frequent Keywords .....	147
Table 3-3: Co-occurrence Matrix for Frequent Keywords (Continued) .....	149
Table 3-4: The Main Keywords of Each Level One Topic .....	151
Table 3-5: Detailed Information for Level One Topic Detection .....	155
Table 3-6: Keywords Evolution during the SMS Process .....	157
Table 3-7: Journal Papers _ Information Needed to Answer RQ2-RQ7 .....	158
Table 3-8: Conference Papers _ Information Needed to Answer RQ2-RQ6 .....	168
Table 3-9: Workshop Papers_ Information Needed to Answer RQ2-RQ6 .....	179
Figure 3-2: Research Tree Construction Process .....	183
Figure 3-3: Research Tree .....	184
Figure 3-4: Evolution of Intrusion Alert Analysis Topics Publications over Time .....	185
Figure 3-5: Percentage of Publications per Topic .....	185
Figure 3-6: Main Keywords and Phrases in Intrusion Alert Analysis Field .....	186
Table 3-10: Comparison between our SMS and Secondary Studies .....	187
Table 3-11: Journal Papers _ Information Needed to Answer RQ1 and RQ7-RQ10 .....	188
Table 3-12: Conference Papers_ Information Needed to Answer RQ1 and RQ7-RQ10 .....	200
Table 3-13: Workshop Papers_ Information Needed to Answer RQ1 and RQ7-RQ10 .....	214
Figure 3-7: Journals in Intrusion Alert Analysis Field .....	219
Figure 3-8: Categories and Active Journals Mapping .....	220
Figure 3-9: Conferences in Intrusion Alert Analysis Field .....	221
Figure 3-10: Workshops in Intrusion Alert Analysis Field .....	222
Figure 3-11: Categories and Active Conferences and Workshops Mapping .....	222
Figure 3-12: Frequency of Publications per Year .....	223
Figure 3-13: Geographical Distribution of Publications .....	223
Figure 3-14: Categories and Pioneer Researchers Mapping .....	224
Figure 3-15: Details on Level One Topics .....	225
Figure 3-16: Details on Pioneer Researchers .....	226
Chapter 4 .....	227
Supplement Information .....	227
Useful Information .....	228
Journals Ranking Metrics .....	228
Conferences and Workshop Ranking Metrics .....	228
Chapter 5 .....	229
References .....	229

Our support email address is here to help you with any questions, requests, and feedback you may have:  
[sqlab@um.ac.ir](mailto:sqlab@um.ac.ir)

We will reply you as quickly as possible!

Regards,

SQLab team.