PRIVACY-PRESERVED SECURITY-CONSCIOUS FRAMEWORK TO
ENHANCE WEB SERVICE COMPOSITION

HOMA MOVAHEDNEJAD

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Computer Science)

Faculty of Computing
Universiti Teknologi Malaysia

JULY 2016
To my GOD, ALLAH, who is always with me in every moment

To our prophet, Mohammad, the messenger of truth, fraternization and kindness

To Mahdi the promised saviour, looking forward to his arrival

To my dear and beloved husband who encouraged and supported me

To my dears mother, father, sisters, and brothers

To my dears mother-, father-, and sister-in-law

And to all who supported me in my study, especially my supervisor
ACKNOWLEDGEMENT

In the name of Allah, Most Gracious, Most Merciful. I thank Allah S.W.T for granting me perseverance and strength I needed to complete this thesis.

In preparing this thesis, I was in contact with many people, researchers, academicians, and practitioners. They have contributed towards my understanding and thoughts. First and foremost, I wish to express my sincere appreciation to my thesis supervisor, Prof. Dr. Suhaimi Ibrahim, for encouragement, guidance, and critics. He has built and directed an environment that granted me an opportunity to learn and practice research skills, meet and collaborate with brilliant researchers, and transfer the long journey of PhD to a great and lovely experience. I would like to thank Assoc. Prof. Dr. Harihodin Selamat, my project leader for his support during my study. I am also indebted to Universiti Teknologi Malaysia (UTM) and the Ministry of Education (MOE), Malaysia for funding my PhD study.

In particular, I would like to express my gratitude towards Dr. Mohammad Mahdi Taheri from University of Illinois at Chicago, Dr. Sayed Gholam Hassan Tabatabei from Isfahan University of Technology, Dr. Arash Habibi Lashkari from University of New Brunswick, and Dr. Mahmoud Danaee from University of Malaya who closely collaborated with me. Moreover, I am very thankful to Dr. Ali Keyvanfar, and Dr. Arezou Shafagh from Universiti Teknologi Malaysia for their supports and friendships.

I would particularly like to thank my parents and my husband’s parents, who deserve my gratitude for their inseparable prayer, encouragement and endless patience. Words fail me in expressing my deepest appreciation to my husband, Mahdi, whose encouragement and love gave me confidence. My thesis would not have been possible without his support. Thank you.
ABSTRACT

The emergence of loosely coupled and platform-independent Service-Oriented Computing (SOC) has encouraged the development of large computing infrastructures like the Internet, thus enabling organizations to share information and offer value-added services tailored to a wide range of user needs. Web Service Composition (WSC) has a pivotal role in realizing the vision of implementing just about any complex business processes. Although service composition assures cost-effective means of integrating applications over the Internet, it remains a significant challenge from various perspectives. Security and privacy are among the barriers preventing a more extensive application of WSC. First, users possess limited prior knowledge of security concepts. Second, WSC is hindered by having to identify the security required to protect critical user information. Therefore, the security available to users is usually not in accordance with their requirements. Moreover, the correlation between user input and orchestration architecture model is neglected in WSC with respect to selecting a high performance composition execution process. The proposed framework provides not only the opportunity to securely select services for use in the composition process but also handles service users’ privacy requirements. All possible user input states are modelled with respect to the extracted user privacy preferences and security requirements. The proposed approach supports the mathematical modelling of centralized and decentralized orchestration regarding service provider privacy and security policies. The output is then utilized to compare and screen the candidate composition routes and to select the most secure composition route based on user requests. The D-optimal design is employed to select the best subset of all possible experiments and optimize the security conscious of privacy-preserving service composition. A Choreography Index Table (CIT) is constructed for selecting a suitable orchestration model for each user input and to recommend the selected model to the choreographed level. Results are promising that indicate the proposed framework can enhance the choreographed level of the Web service composition process in making adequate decisions to respond to user requests in terms of higher security and privacy. Moreover, the results reflect a significant value compared to conventional WSC, and WSC optimality was increased by an average of 50% using the proposed CIT.
ABSTRAK

Kemunculan ikatan pasangan yang longgar dan platform bebas Pengkomputeran Berorientasikan Perkhidmatan (SOC) telah menggalakkan pembangunan infrastuktur komputeran yang besar seperti Internet, oleh itu ia membolehkan organisasi untuk berkongsi maklumat dan menawarkan perkhidmatan nilai tambah sesuai dengan keperluan pengguna yang luas. Komposisi Khidmat Laman Sesawang (WSC) memainkan peranan utama dalam merealisasikan wawasan untuk melaksanakan hampir semua proses perniagaan yang kompleks. Walaupun komposisi perkhidmatan menjamin cara yang kos efektif untuk mengintegrasikan aplikasi terhadap Internet, ia kekal sebagai satu cabaran penting dari pelbagai perspektif. Keselamatan dan rahsia adalah antara masalah yang menghalang lebih banyak aplikasi WSC. Pertama, pengguna memiliki pengetahuan awal yang terbatas mengenai konsep keselamatan. Kedua, penggunaan WSC tergendala disebabkan terpaksa mengenal pasti keselamatan yang diperlukan untuk mengawal maklumat pengguna yang kritikal. Oleh itu, keselamatan yang sedia ada pada pengguna biasanya tidak selari dengan keperluan mereka. Malah, hubung kait antara input pengguna dan model senibina orkestra diabaikan dalam penggunaan WSC bagi memilih proses pelaksanaan komposisi yang berprestasi tinggi. Rangka kerja yang dicadangkan bukan sahaja memberi peluang untuk memilih perkhidmatan yang selamat dalam proses komposisi tetapi juga mengendalikan keperluan kerahsiaan khidmat pengguna. Segala kemungkinan keadaan input pengguna dimodelkan dari segi keutamaan kerahsiaan pengguna dan keperluan keselamatan. Pendekatan yang dicadangkan menyokong pemodelan matematik terhadap orkestra berpusat dan tidak berpusat yang berkaitan dengan kerahsiaan khidmat pengguna dan polisi keselamatan. Hasil kerja kemudian digunakan untuk membanding dan menapis laluan komposisi calon dan memilih laluan komposisi yang terselamat berdasarkan permintaan pengguna. Reka bentuk optimum-D digunakan untuk memilih subset yang terbaik terhadap semua kemungkinan eksperimen dan meningkatkan kesedaran keselamatan terhadap komposisi perkhidmatan kekal rahsia. Jadual Indek Koreografi (CIT) dirangka bagi memilih model koreografi yang sesuai untuk setiap input pengguna dan mencadangkan model yang dipilih kepada aras koreografi. Hasilnya menunjukkan rangka kerja yang dicadangkan boleh meningkatkan aras koreografi terhadap proses komposisi khidmat sesawang dalam membuat keputusan yang sesuai dengan permintaan pengguna dari segi keselamatan dan rahsia yang mantap. Juga, keputusan menggambarkan nilai yang signifikan apabila dibandingkan dengan WSC konvensional, dan keoptimuman WSC didapati bertambah sebanyak 50% dengan menggunakan CIT yang dicadangkan.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DECLARATION</td>
<td>ii</td>
</tr>
<tr>
<td></td>
<td>DEDICATION</td>
<td>iii</td>
</tr>
<tr>
<td></td>
<td>ACKNOWLEDGEMENT</td>
<td>iv</td>
</tr>
<tr>
<td></td>
<td>ABSTRACT</td>
<td>v</td>
</tr>
<tr>
<td></td>
<td>ABSTRAK</td>
<td>vi</td>
</tr>
<tr>
<td></td>
<td>TABLE OF CONTENTS</td>
<td>vii</td>
</tr>
<tr>
<td></td>
<td>LIST OF TABLES</td>
<td>xiii</td>
</tr>
<tr>
<td></td>
<td>LIST OF FIGURES</td>
<td>xv</td>
</tr>
<tr>
<td></td>
<td>LIST OF SYMBOLS</td>
<td>xix</td>
</tr>
<tr>
<td></td>
<td>LIST OF ABBREVIATIONS</td>
<td>xxi</td>
</tr>
<tr>
<td></td>
<td>LIST OF APPENDICES</td>
<td>xxiv</td>
</tr>
</tbody>
</table>

1 INTRODUCTION

1.1 Overview  1
1.2 Background of the Problem  3
1.3 Statement of the Problem  6
1.4 Purpose of the Research  8
1.5 Objectives of the Research  9
1.6 Scope of the Research  10
1.7 Significance of the Research  11
1.8 Thesis Organization  11

2 LITERATURE REVIEW

2.1 Introduction  13
2.2  Web Service Concept 14
2.3  Web Service Reference Model 15
2.4  Web Service Reference Standardization 17
   2.4.1  Simple Object Access Protocol (SOAP) 17
   2.4.2  Web Service Description Language (WSDL) 18
   2.4.3  Universal Description, Discovery, and Integration (UDDI) 19
2.5  Web Service Stack and Key Dimensions 19
2.6  Web Service Classification 23
2.7  Web Service Composition (WSC) 24
   2.7.1  Business Process Modeling 25
      2.7.1.1  Web Service Orchestration 25
      2.7.1.2  Web Service Choreography 26
   2.7.2  Web Service Composition Lifecycle 27
   2.7.3  Web Service Composition Modeling 29
      2.7.3.1  Syntactic-based 30
      2.7.3.2  Semantic-based 31
      2.7.3.3  Goal-Oriented 32
   2.7.4  Challenges in Web Service Composition 34
      2.7.4.1  Secure Service Composition 35
      2.7.4.2  Pervasive Service Composition 36
      2.7.4.3  Dependable Service Composition 36
      2.7.4.4  Adaptable and Autonomous Service Composition 37
      2.7.4.5  Support of RESTful Services 38
2.8  Quality of Service (QoS) 38
   2.8.1  Security 41
      2.8.1.1  Data Security 41
      2.8.1.2  Access Control 46
   2.8.2  Privacy 52
      2.8.2.1  Data Privacy Model 52
      2.8.2.2  Service Privacy Model 54
      2.8.2.3  User Privacy Model 54
| 3.4 | Experimental Setup of the Research | 100 |
| 3.5 | Design of Experiment | 101 |
| 3.6 | Result Validation | 103 |
| 3.7 | Operational Framework | 103 |
| 3.8 | Summary | 105 |

4 SECURITY-CONSCIOUS PRIVACY-ENABLED MODELING 106

4.1 Introduction 106

4.2 Concept of the Web Service Composition Process 106

4.2.1 Component Web Service 107

4.2.1.1 Goal 108

4.2.1.2 Required Data Items 108

4.2.1.3 Security 108

4.2.2 Provider 109

4.2.3 Orchestration 109

4.2.3.1 Centralized Orchestration 110

4.2.3.2 Decentralized Orchestration 110

4.2.4 Choreograpged Composite Service 111

4.2.5 Provider Privacy Policy and User Privacy Preference 111

4.2.5.1 Provider Privacy Policy 112

4.2.5.2 User Privacy Preference 112

4.3 Assumptions 114

4.4 Framework of the Proposed Approach 116

4.5 Mathematical Modeling of the Web Service Composition Process 118

4.5.1 Mathematical Modeling of Provider Privacy Policy 119

4.5.2 Mathematical Modeling for User Privacy Preference 119

4.5.3 Mathematical Modeling for Orchestration 123

4.5.4 Comparison 125

4.5.5 Screening Process 126
4.6 Empirical Analysis 130
4.7 Algorithms 131
4.8 Choreography Index Table (CIT) 148
4.9 Summary 149

5 EVALUATION AND DISCUSSION 150
5.1 Introduction 150
5.2 Applicability and Feasibility of the Proposed Approach 150
  5.2.1 User Input 151
  5.2.2 Centralized Orchestration 152
  5.2.3 Decentralized Orchestration 157
5.3 Experiments 161
  5.3.1 Experimental Design 161
  5.3.2 Centralized Empirical Model 163
    5.3.2.1 ANOVA Analysis for ARN 165
    5.3.2.2 ANOVA Table for ARN 170
    5.3.2.3 ANOVA Analysis for ARQ 177
    5.3.2.4 ANOVA Table for ARQ 182
  5.3.3 Decentralized Empirical Model 188
    5.3.3.1 ANOVA Analysis for ARN 188
    5.3.3.2 ANOVA Table for ARN 194
    5.3.3.3 ANOVA Analysis for ARQ 202
    5.3.3.4 ANOVA Table for ARQ 207
  5.3.4 Validation Results 213
  5.3.5 Optimization 217
5.4 Discussion 220
5.5 Summary 226

6 CONCLUSION 228
6.1 Introduction 228
6.2 Objectives Revisited 229
6.3 Contributions of the Research 232
6.4 Limitation of the Research 233
6.5 Recommendations for Future Work 234
6.6 Closing Remarks 235

REFERENCES 238
Appendices A-B 259-277
## LIST OF TABLES

<table>
<thead>
<tr>
<th>TABLE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Encryption Algorithm Security Strength for Applying Confidentiality</td>
<td>44</td>
</tr>
<tr>
<td>2.2</td>
<td>Security Strengths of Digital Signature Algorithms for Applying Integrity and Non-Repudiation</td>
<td>45</td>
</tr>
<tr>
<td>2.3</td>
<td>QoS-based Web Service Selection Approaches – Part 1</td>
<td>62</td>
</tr>
<tr>
<td>2.4</td>
<td>QoS-based Web Service Selection Approaches – Part 2</td>
<td>63</td>
</tr>
<tr>
<td>2.5</td>
<td>Summary of Existing Works Supporting Security and Privacy Aware WSC</td>
<td>83</td>
</tr>
<tr>
<td>3.1</td>
<td>Variable Parameters Levels</td>
<td>103</td>
</tr>
<tr>
<td>3.2</td>
<td>Operational Framework</td>
<td>104</td>
</tr>
<tr>
<td>4.1</td>
<td>Specified Weights for Each Data Item</td>
<td>115</td>
</tr>
<tr>
<td>4.2</td>
<td>Specified Weights for Each Data Item Considering the Modify Action</td>
<td>115</td>
</tr>
<tr>
<td>4.3</td>
<td>Descriptions of Symbols of All Elements Used in Web Service Composition Modeling</td>
<td>118</td>
</tr>
<tr>
<td>4.4</td>
<td>Data Item Weights with Respect to Item Significance</td>
<td>121</td>
</tr>
<tr>
<td>4.5</td>
<td>Weights of ‘Read-only’ and ‘Modify’ Actions for each Data Item</td>
<td>122</td>
</tr>
<tr>
<td>4.6</td>
<td>User Input and Provided Service Routes</td>
<td>126</td>
</tr>
<tr>
<td>4.7</td>
<td>Screening Process</td>
<td>127</td>
</tr>
<tr>
<td>5.1</td>
<td>Experimental Range and Independent Variable Levels</td>
<td>161</td>
</tr>
<tr>
<td>5.2</td>
<td>ARQ Parameter Descriptions</td>
<td>162</td>
</tr>
<tr>
<td>5.3</td>
<td>Part of D-Optimal Design Consisting of 373 Experiments for the Study of Four Experimental Factors (Centralized Orchestration)</td>
<td>164</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>5.4</td>
<td>ANOVA Table for ARN (Centralized Model)</td>
<td>170</td>
</tr>
<tr>
<td>5.5</td>
<td>Model Coefficient Estimations by Regression for ARN (Centralized Model)</td>
<td>171</td>
</tr>
<tr>
<td>5.6</td>
<td>ANOVA Table for ARQ (Centralized Model)</td>
<td>183</td>
</tr>
<tr>
<td>5.7</td>
<td>Model Coefficient Estimations by Regression for ARQ (Centralized Model)</td>
<td>184</td>
</tr>
<tr>
<td>5.8</td>
<td>Part of D-Optimal Design Consisting of 373 Experiments for the Study of Four Experimental Factors (Decentralized Orchestration)</td>
<td>190</td>
</tr>
<tr>
<td>5.9</td>
<td>ANOVA Table for ARN (Decentralized Model)</td>
<td>195</td>
</tr>
<tr>
<td>5.10</td>
<td>Model Coefficient Estimations by Regression for ARN (Decentralized Model)</td>
<td>196</td>
</tr>
<tr>
<td>5.11</td>
<td>ANOVA Table for ARQ (Decentralized Model)</td>
<td>208</td>
</tr>
<tr>
<td>5.12</td>
<td>Model Coefficient Estimations by Regression for ARQ (Decentralized Model)</td>
<td>209</td>
</tr>
<tr>
<td>5.13</td>
<td>Validation Test for Available Route Number (ARN) – Centralized Orchestration</td>
<td>214</td>
</tr>
<tr>
<td>5.14</td>
<td>Validation Test for Available Route Quality (ARQ) – Centralized Orchestration</td>
<td>215</td>
</tr>
<tr>
<td>5.15</td>
<td>Validation Test for Available Route Number (ARN) – Decentralized Orchestration</td>
<td>216</td>
</tr>
<tr>
<td>5.16</td>
<td>Validation Test for Available Route Quality (ARQ) – Decentralized Orchestration</td>
<td>217</td>
</tr>
<tr>
<td>5.17</td>
<td>Goals for Centralized Orchestration Model Optimization</td>
<td>218</td>
</tr>
<tr>
<td>5.18</td>
<td>Solution for Centralized Orchestration Model Optimization</td>
<td>219</td>
</tr>
<tr>
<td>5.19</td>
<td>Goals for Decentralized Orchestration Model Optimization</td>
<td>219</td>
</tr>
<tr>
<td>5.20</td>
<td>Solution for Decentralized Orchestration Model Optimization</td>
<td>220</td>
</tr>
<tr>
<td>5.21</td>
<td>Part of the Choreography Index Table</td>
<td>223</td>
</tr>
</tbody>
</table>
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>FIGURE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Web Service Architecture</td>
<td>16</td>
</tr>
<tr>
<td>2.2</td>
<td>SOAP Message</td>
<td>18</td>
</tr>
<tr>
<td>2.3</td>
<td>WSDL Example</td>
<td>19</td>
</tr>
<tr>
<td>2.4</td>
<td>Web Service Stack and Key Dimensions</td>
<td>21</td>
</tr>
<tr>
<td>2.5</td>
<td>Web Service Management System (WSMS) Architecture</td>
<td>23</td>
</tr>
<tr>
<td>2.6</td>
<td>Web Service Classification</td>
<td>24</td>
</tr>
<tr>
<td>2.7</td>
<td>Service Orchestration and Service Choreography</td>
<td>26</td>
</tr>
<tr>
<td>2.8</td>
<td>Orchestration and Choreography Interrelation</td>
<td>27</td>
</tr>
<tr>
<td>2.9</td>
<td>Web Service Composition Lifecycle</td>
<td>28</td>
</tr>
<tr>
<td>2.10</td>
<td>Classification of Web Service Composition Modeling</td>
<td>29</td>
</tr>
<tr>
<td>2.11</td>
<td>Web Service Composition Challenges</td>
<td>35</td>
</tr>
<tr>
<td>2.12</td>
<td>Quality of Web Service Taxonomy</td>
<td>40</td>
</tr>
<tr>
<td>2.13</td>
<td>Security and Privacy Taxonomy</td>
<td>42</td>
</tr>
<tr>
<td>2.14</td>
<td>Authentication Strength Evaluation</td>
<td>48</td>
</tr>
<tr>
<td>2.15</td>
<td>Multi-Criteria Decision-Making Approaches</td>
<td>65</td>
</tr>
<tr>
<td>2.16</td>
<td>Discovery Framework</td>
<td>73</td>
</tr>
<tr>
<td>2.17</td>
<td>SWS-Broker Framework</td>
<td>74</td>
</tr>
<tr>
<td>2.18</td>
<td>High-Level Architecture of the SCAIMO Framework</td>
<td>75</td>
</tr>
<tr>
<td>2.19</td>
<td>Privacy-Aware Service Composition and Ranking Framework</td>
<td>77</td>
</tr>
<tr>
<td>2.20</td>
<td>PAIRSE Global Framework</td>
<td>78</td>
</tr>
<tr>
<td>2.21</td>
<td>Privacy-Conscious Service Composition Framework</td>
<td>79</td>
</tr>
<tr>
<td>2.22</td>
<td>Privacy-Aware Selection and Provisioning Framework</td>
<td>79</td>
</tr>
<tr>
<td>2.23</td>
<td>Service Choreography Scenario for Service Selection</td>
<td>80</td>
</tr>
<tr>
<td>2.24</td>
<td>Security Policy Composition Framework</td>
<td>81</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>2.25</td>
<td>Secure Web Service Composition Framework</td>
<td>82</td>
</tr>
<tr>
<td>3.1</td>
<td>Execution Process Modeling</td>
<td>87</td>
</tr>
<tr>
<td>3.2</td>
<td>Research Design</td>
<td>89</td>
</tr>
<tr>
<td>3.3</td>
<td>User Input Modeling Process</td>
<td>91</td>
</tr>
<tr>
<td>3.4</td>
<td>Centralized Orchestration Modeling Process</td>
<td>93</td>
</tr>
<tr>
<td>3.5</td>
<td>Decentralized Orchestration Modeling Process</td>
<td>94</td>
</tr>
<tr>
<td>3.6</td>
<td>Selection and Screening Process for Centralized Orchestration</td>
<td>96</td>
</tr>
<tr>
<td>3.7</td>
<td>Selection and Screening Process for Decentralized Orchestration</td>
<td>97</td>
</tr>
<tr>
<td>3.8</td>
<td>Statistical Modeling Process for Centralized Orchestration</td>
<td>99</td>
</tr>
<tr>
<td>3.9</td>
<td>Statistical Modeling Process for Decentralized Orchestration</td>
<td>100</td>
</tr>
<tr>
<td>4.1</td>
<td>Web Service Composition Process</td>
<td>107</td>
</tr>
<tr>
<td>4.2</td>
<td>Provider Policy Model</td>
<td>109</td>
</tr>
<tr>
<td>4.3</td>
<td>Centralized Orchestration Model</td>
<td>110</td>
</tr>
<tr>
<td>4.4</td>
<td>Decentralized Orchestration Model</td>
<td>111</td>
</tr>
<tr>
<td>4.5</td>
<td>Proposed Framework for Security-Conscious Privacy-Preserving Service Composition</td>
<td>117</td>
</tr>
<tr>
<td>5.1</td>
<td>User Input States</td>
<td>151</td>
</tr>
<tr>
<td>5.2</td>
<td>Fragment of Computed Composition Routes for Centralized Orchestration</td>
<td>153</td>
</tr>
<tr>
<td>5.3</td>
<td>Part of the Composition Routes Selected with Respect to Each User Input State (Centralized Orchestration)</td>
<td>154</td>
</tr>
<tr>
<td>5.4</td>
<td>Screened Composition Routes with Respect to Each User Input State (Centralized Orchestration)</td>
<td>155</td>
</tr>
<tr>
<td>5.5</td>
<td>Example of Composition Route Selection with Respect to User Input</td>
<td>156</td>
</tr>
<tr>
<td>5.6</td>
<td>Part of the Computed Composition Routes for Decentralized Orchestration</td>
<td>158</td>
</tr>
<tr>
<td>5.7</td>
<td>Part of the Composition Routes Selected with Respect to Each User Input State (Decentralized Orchestration)</td>
<td>159</td>
</tr>
<tr>
<td>5.8</td>
<td>Part of the Screened Composition Routes with Respect to Each User Input State (Decentralized Orchestration)</td>
<td>160</td>
</tr>
<tr>
<td>5.9</td>
<td>Normal Probability Plot of Residuals for ARN (Centralized Model)</td>
<td>165</td>
</tr>
</tbody>
</table>
5.10 Plot of Residuals vs. Predicted Response for ARN (Centralized Model) 166
5.11 Main Effect Plot for Purpose (Centralized Model - ARN Response) 166
5.12 Main Effect Plot for Data Items (Centralized Model - ARN Response) 167
5.13 Main Effect Plot for Role of Provider (Centralized Model - ARN Response) 168
5.14 Plot of Interaction between Role of Provider and Purpose (Centralized Model - ARN Response) 169
5.15 Plot of Interaction between Data Items and Role of Provider (Centralized Model - ARN Response) 169
5.16 Normal Probability Plot of Residuals for ARQ (Centralized Model) 177
5.17 Plot of Residuals vs. Predicted Response for ARQ (Centralized Model) 178
5.18 Plot of Interaction between Purpose and Data Items (Centralized Model - ARQ Response) 179
5.19 Main Effect Plot for Data Items (Centralized Model - ARQ Response) 179
5.20 Main Effect Plot for Action Types (Centralized Model - ARQ Response) 180
5.21 Main Effect Plot for Role of Provider (Centralized Model - ARQ Response) 181
5.22 Plot of Interaction between Purpose and Action Type (Centralized Model - ARQ Response) 181
5.23 Plot of Interaction between Data Items and Action Type (Centralized Model - ARQ Response) 182
5.24 Normal Probability Plot of Residuals for ARN (Decentralized Model) 189
5.25 Plot of Residuals vs. Predicted Response for ARN (Decentralized Model) 189
5.26 Main Effect Plot for Purpose (Decentralized Model - ARN Response) 191
5.27 Main Effect Plot for Data Items (Decentralized Model - ARN Response) 192
5.28 Main Effect Plot for Role of Provider (Decentralized Model - ARN Response) 192
5.29 Plot of Interaction between Purpose and Role of Provider (Decentralized Model - ARN Response) 193
5.30 Plot of Interaction between Role of Provider and Data Items (Decentralized Model - ARN Response) 194
5.31 Normal Probability Plot of Residuals for ARQ (Decentralized Model) 202
5.32 Plot of Residuals vs. Predicted Response for ARQ (Decentralized Model) 203
5.33 Plot of Interaction between Purpose and Data Items (Decentralized Model - ARQ Response) 204
5.34 Main Effect Plot for Data Items (Decentralized Model - ARQ Response) 204
5.35 Main Effect Plot for Action Type (Decentralized Model - ARQ Response) 205
5.36 Plot of Interaction between Purpose and Action Type (Decentralized Model - ARQ Response) 206
5.37 Main Effect Plot for Role of Provider (Decentralized Model - ARQ Response) 206
5.38 Plot of Interaction between Data Items and Action Type (Decentralized Model - ARQ Response) 207
5.39 Proposed Mechanism for the Choreography Index Table 221
5.40 User Requests Handled by Centralized and Decentralized Orchestration with Respect to Requested Purpose 224
5.41 User Requests Handled by Centralized and Decentralized Orchestration with Respect to the Number of Data Items 225
5.42 User Requests Handled by Centralized and Decentralized Orchestration with Respect to Action Type 225
5.43 User Requests Handled by Centralized and Decentralized Orchestration with Respect to Service Provider Role 226
LIST OF SYMBOLS

\( g \) - Goal
\( rdi \) - Required data item
\( S \) - Security
\( C \) - Confidentiality
\( I \) - Integrity
\( \mathcal{A} \) - Availability
\( P \) - Provider
\( r \) - Role
\( dl \) - Delegation
\( P_O \) - Orchestrator
\( p \) - Purpose
\( adi \) - Available data items
\( a \) - Action
\( v \) - Visibility
\( se \) - Sensitivity
\( ri \) - Risk
\( \mathcal{U}P \) - User privacy preference
\( se_H \) - Highest value of sensitivity
\( C_L \) - Confidentiality at low level
\( C_M \) - Confidentiality at medium level
\( C_H \) - Confidentiality at high level
\( ri_H \) - Highest value of risk
\( I_L \) - Integrity at low level
$I_M$ - Integrity at medium level

$I_H$ - Integrity at high level

$l$ - Depth level

$M_{Orch-Ce}$ - Centralized orchestration model

$M_{Orch-De}$ - Decentralized orchestration model

$n_{CL}$ - Number of confidentiality at low level

$n_{CM}$ - Number of confidentiality at medium level

$n_{CH}$ - Number of confidentiality at high level

$w_{CL}$ - Weight of confidentiality at low level

$w_{CM}$ - Weight of confidentiality at medium level

$w_{CH}$ - Weight of confidentiality at high level

$n_{IL}$ - Number of integrity at low level

$n_{IM}$ - Number of integrity at medium level

$n_{IH}$ - Number of integrity at high level

$w_{IL}$ - Weight of integrity at low level

$w_{IM}$ - Weight of integrity at medium level

$w_{IH}$ - Weight of integrity at high level

$UI$ - User input

$PP$ - Privacy policy of provider

$ARQ_i$ - Available route quality for composition route $i$

$N_D$ - Number of delegation

$N_{Rp}$ - Number of requested purposes by service user

$N_{Op}$ - Number of offered purposes in composition route

$N_p$ - Number of providers involved in composition route

$C_R$ - Confidentiality level required based on user preferences

$C_p$ - Confidentiality level provided by composition route

$I_R$ - Integrity level required based on user preferences

$I_p$ - Integrity level provided by composition route

$N_R$ - Number of routes

$CS$ - Component web service
LIST OF ABBREVIATIONS

ABAC - Attribute-Based Access Control Model
ACL - Access Control List
AHP - Analytical Hierarchy Process
ANOVA - Analysis of Variance
Anti-DoS - Anti-Denial of Service
BBD - Box-Behnken Designs
BPMN - Business Process Modeling Notation
B2C - Business-to-Consumer
CCD - Central Composite Design
CIA - Confidentiality, Integrity, and Availability
CIT - Choreography Index Table
DaaS - Data-as-a-Service
DAC - Discretionary Access Control Model
DM - Dominance Method
DOE - Design of Experiments
IBAC - Identity Based Access Control Model
IDS - Intrusion Detection System
IPS - Intrusion Prevention System
IoT - Internet of Things
MAC - Mandatory Access Control Model
MADM - Multi Attribute Decision Making
MCDM - Multi Criteria Decision Making
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MODM</td>
<td>Multi Objective Decision Making</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>PBAC</td>
<td>Policy-Based Access Control Model</td>
</tr>
<tr>
<td>PN</td>
<td>Private Negotiator</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RAdAC</td>
<td>Risk Adaptive Access Control Model</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role-based Access Control Model</td>
</tr>
<tr>
<td>RE</td>
<td>Requirement Engineering</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio-Frequency Identification</td>
</tr>
<tr>
<td>RSM</td>
<td>Response Surface Methodology</td>
</tr>
<tr>
<td>RTD</td>
<td>Round Trip Delay</td>
</tr>
<tr>
<td>SAW</td>
<td>Simple Additive weighting</td>
</tr>
<tr>
<td>SI*</td>
<td>Secure i*</td>
</tr>
<tr>
<td>SOA</td>
<td>Service Oriented Architecture</td>
</tr>
<tr>
<td>SOC</td>
<td>Service Oriented Computing</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
</tr>
<tr>
<td>TBAC</td>
<td>Task Based Access Control Model</td>
</tr>
<tr>
<td>UDDI</td>
<td>Universal Description, Discovery, and Integration</td>
</tr>
<tr>
<td>URI</td>
<td>Universal Resource Identifier</td>
</tr>
<tr>
<td>URL</td>
<td>Universal Resource Locator</td>
</tr>
<tr>
<td>OWL-S</td>
<td>Web Ontology Language for Web Services</td>
</tr>
<tr>
<td>WS-BPEL</td>
<td>Web Services Business Process Execution Language</td>
</tr>
<tr>
<td>WSC</td>
<td>Web Service Composition</td>
</tr>
<tr>
<td>WS-CDL</td>
<td>Web Service Choreography Description Language</td>
</tr>
<tr>
<td>WSDL</td>
<td>Web Service Description Language</td>
</tr>
<tr>
<td>WS-Federation</td>
<td>Web Service Federation</td>
</tr>
<tr>
<td>WSML</td>
<td>Web Service Modeling Language</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>WSMO</td>
<td>Web Service Modeling Ontology</td>
</tr>
<tr>
<td>WSMS</td>
<td>Web Service Management System</td>
</tr>
<tr>
<td>WS-Security</td>
<td>Web Service Security</td>
</tr>
<tr>
<td>WS-Trust</td>
<td>Web Service Trust</td>
</tr>
<tr>
<td>XML</td>
<td>eXtensible Markup Language</td>
</tr>
</tbody>
</table>
# LIST OF APPENDICES

<table>
<thead>
<tr>
<th>APPENDIX</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Experimental Plan Recommended by D-Optimal Design for Centralized Empirical Model</td>
<td>259</td>
</tr>
<tr>
<td>B</td>
<td>Experimental Plan Recommended by D-Optimal Design for Decentralized Empirical Model</td>
<td>269</td>
</tr>
</tbody>
</table>
CHAPTER 1

INTRODUCTION

1.1 Overview

Service-Oriented Computing (SOC) has adapted new ways of software application design, delivery, and use over the last decade. SOC relies on services as fundamental elements that promise the development of rapid and low-cost distributed applications in heterogeneous environments (Yu et al., 2008). The goal of SOC is to achieve platform-independent, standard-based and loosely coupled distributed computing. To realize this aim, an architectural model is established with Service-Oriented Architecture (SOA) that organizes software infrastructures and applications into a set of interacting services. These services can be published, discovered, and used by other services. The most promising choice in accomplishing SOA objectives is Web service technology (Papazoglou and van den Heuvel, 2007). Sheng et al. (2014b) defined a Web service as “a semantically well-defined abstraction of a set of computational or physical activities involving a number of resources, intended to fulfil a customer need or a business requirement”. Standard-based languages and Internet-based protocols have been utilized to describe, advertise, and discover Web services.

A sizable body of literature has investigated service composition as a key challenge of SOC and SOA (Bouguettaya et al., 2014g). The basic blocks of service computing are atomic services whose interoperations realize distributed applications. SOC cannot achieve its full potential unless the service composition challenge is appropriately addressed to provide more powerful value-added services and applications. Service composition enables organizations and enterprises to outsource functionalities, form alliances, and deliver professional services to their customers. It
leads to reduce their cost and risk in building new business applications (Sheng et al., 2014b).

Although service composition promises cost-effective means of integrating applications over the Internet, it remains an important challenge from a the non-functional perspective known as Quality of Service (QoS) (Halvard, 2009). Different aspects of non-functional properties of a service are presented in its QoS. The literature features various QoS considerations. According to Liu et al. (2012), ISO 840216 and ITUE.80017 are utilized to model QoS metrics of a service. They may include but are not limited to success rate, response time, availability, reliability, cost, privacy, trustworthiness, and security. Among these QoS metrics, security and privacy are of great importance to adopting service composition considering the fact that SOC environments are becoming more dynamic and open (Bouguettaya et al., 2014a; Noor et al., 2013; Satoh and Tokuda, 2011).

Secure service computing is increasingly gaining momentum in ensuring that users’ private data are securely processed and handled. A Number of Web service standards have been proposed by industry and academia including WS-Security (OASIS, 2006), WS-Federation (OASIS, 2009), and WS-Trust (OASIS, 2007b). Nonetheless, they have not fully paved the way to secure service composition yet, the reason being that they were originally proposed for atomic services and cannot address the challenges related to composite services (Sheng et al., 2014b). A few works have mainly concentrated on secure service composition (Brucker et al., 2013; Dragovic et al., 2014; Karatas et al., 2015). However, privacy concerns are neglected in existing works (Costante et al., 2013c). Therefore, the current research investigates the problem of secure service composition and introduces an integrated approach to address this challenge from two key perspectives: security and privacy. This study not only provides an opportunity to securely select services for use in the composition process but also to handle service users’ privacy requirements.

The remainder of this chapter explains the need for secure and private service composition. The research problem, objectives, and scope are also discussed, respectively. The significance of the research and the thesis organization are presented in the final section of this chapter.
1.2 Background of the Problem

Service-Oriented Computing (SOC) is facing the growth of the everything-as-a-service (or X-as-a-service) phenomenon, resulting in the significant evolution of system integration in Business-to-Consumer (B2C) and Business-to-Business (B2B) applications. Web service coordination and deployment as a process of making a service ready to be used is crucial to fully realizing this promising phenomenon (Dastjerdi, 2013). It comprises several steps including discovery, selection, composition, and execution.

Web service discovery is responsible for publishing service descriptions and details in Universal Description, Discovery, and Integration (UDDI) repositories so those services are discoverable by potential consumers. Service discovery may return several web services that provide the same functionality (da Silva et al., 2011). Therefore, selecting the best candidate services among numerous functionally-equal services discovered is a primary mission of Web service selection. To achieve this goal, service selection involves non-functional properties of Web services known as Quality of Service (QoS) metrics (Moghaddam and Davis, 2014; Raj and Sasipraba, 2010). However, component services cannot generally satisfy user demands. A process is necessary to combine existing services to fulfil the requested goals. Hence, a value-added service, namely composite service, is created in the Web service composition step using selected component services (Carminati et al., 2015). The composite service created is finally implemented to address user requirements in the Web service execution step.

As Web services are progressively adopted for Internet-based applications, QoS-aware service selection and composition has become a well-known research problem in the service computing area (Barakat et al., 2014; Zheng et al., 2011). A wealth of literature has addressed this problem (D'Mello and Ananthanarayana, 2010; Strunk, 2010; Sun et al., 2011). Different aspects of the QoS-aware service selection and composition challenge have been investigated and referred in existing approaches (El Hadad et al., 2010; Ngu et al., 2010; Zheng et al., 2013). However, privacy and security as two imperative aspects of QoS have attracted less attention. Critical private and business data and information are transferred in service workflows either directly
or indirectly. This fact highlights the importance of security in SOC (Karatas et al., 2015). Moreover, sensitive information exchanges between parties involved in the process of service composition raises the issue of service users’ information privacy (Carminati et al., 2015; Sun et al., 2014).

The problem of security and privacy is a well-known research problem in the service computing field (Bouguettaya et al., 2014a; Carminati et al., 2015; Satoh and Tokuda, 2011). A number of research and standardization efforts have been proposed to deal with these matters. WS-Federation (OASIS, 2009), WS-Security(OASIS, 2006), and WS-Trust (OASIS, 2012) are instances of such efforts. However, the applicability and feasibility of these standards have not been fully proven for service composition, as they were originally devised for single component services (Sheng et al., 2014b). In fact, the majority of early works have focused on handling security and privacy issues for single atomic services. With the increasing importance of service composition, a considerable number of research works are investigating the problem of security and privacy for composite services in recent years. Different security matters, including integrity, confidentiality, and accountability i.e., authentication and authorization are highlighted in several research works (Alrifai et al., 2012; Immonen and Pakkala, 2014; Tabatabaei et al., 2010). Trustworthy and privacy-preserving service composition is also investigated in existing research (Costante et al., 2013c; Dalpiaz et al., 2014; Tbahriti et al., 2011; Tbahriti et al., 2013; Zhang et al., 2014).

Although only security or privacy is necessary, but they are insufficient to accomplish secure private service composition. Fulfilling security requirements does not guarantee that all privacy dimensions of user information will be covered and vice versa. Some literature considers privacy as a sub-class of security (W3C, 2003a, 2004c), while a number of studies deem security a sub-class of privacy (Carminati et al., 2015; Squicciarini et al., 2013). Nevertheless, security and privacy are interrelated, as defined by OASIS (2010), and need to be considered together to protect sensitive information. An appropriate mechanism to support security-aware and privacy-enabled service composition should be proposed. Different elements are involved in providing a new value-added composite service for solving the more complex problems with respect to the security and privacy constraints required (Sheng et al., 2014b). All these elements play an important role in accomplishing the task and affect
the composition process in specific ways. To investigate the effect of each element on the service composition process, statistical analysis is normally utilized. It is necessary to propose mathematical modeling of each element to conduct a statistical analysis on the service composition process. Statistical analysis necessitates the proposed mathematical models to examine the effectiveness of each element with respect to the security-aware privacy-enabled service composition. Proposing an appropriate modeling mechanism to handle this matter is considered the first research gap identified in this study.

From a service users’ point of view, protecting their in-transit sensitive data is of paramount importance in unpredictable and open SOC environments. Users often express concerns via declared privacy preferences. At the same time, the privacy policies of service providers must comply with the expressed user privacy preferences. Moreover, service providers’ privacy policies are grounded on security concepts while service users declare their preferences based on the privacy dimensions. As a result, two heterogeneous concepts render the compliance process more complicated. In addition, the intrinsic complexity of security concepts poses many difficulties for service users who have limited knowledge of security requirements. Such complexities necessitate a methodology to bridge security requirements based on the modeled privacy preferences expressed. Thus, bridging the gap can help non-expert users protect critical information while not compelling them to have prior knowledge of security concepts. It can also facilitate the compliance process between required service user preferences and existing service provider policies. It is expected this bridge will eliminate the subject of heterogeneity in the compliance process. Addressing this issue is the second research gap that needs to be filled in this study.

Furthermore, service composition is often modeled in either centralized or decentralized orchestration. Centralized orchestrated service composition is grounded on centralized architecture, whereby the central entity coordinates interactions between the entities involved in accomplishing the required task. On the other hand, decentralized orchestrated service composition is based on the distributed architecture, where the entities involved collaborate toward achieving a predefined goal without the presence of a centralized coordinator. The choreographed composite services may choose either of these composition modeling types with respect to their specific
advantages and privileges. Some research works (Chafle et al., 2004; Ghosal and Mann, 2012) offer the decentralized orchestration model as a model with improved performance in terms of lower response time and higher scalability and throughput. Other researchers (Schonberger and Wirtz, 2012) believe that centralized orchestration guarantees higher levels of security as sensitive information is exposed to fewer entities.

The current literature suffers from overlooking two matters. First, they only investigate whether the proposed composition model fulfils the security requirements with respect to direct user requests. They do not consider selecting a model that provides the higher possible security level(s). Second, making a trade-off between performance and security in choosing a suitable composition execution process is a demanding task that is ignored in existing approaches. Therefore, it is important to select a high performance composition execution process while maintaining the higher possible security level(s). Addressing the abovementioned concerns is considered as filling the third research gap in this study.

1.3 Statement of the Problem

Distributed computing has witnessed a new generation of platforms with the help of SOC concepts in heterogeneous environments, wherein interoperable services facilitate low-cost and rapid development of distributed applications (Moghaddam and Davis, 2014). WSC, as one of the core concepts of SOC, has been widely utilized, enabling existing services to create new value-added services and share autonomously and independently (El Hadad et al., 2010; Wu et al., 2014). Due to the significance of WSC, it has been heavily investigated in both academia and industries. Despite the progressive improvement, a number of issues have not been appropriately addressed (Bouguettaya et al., 2014a; Sheng et al., 2014b).

Security and privacy are among the problematic barriers that prevent the wider application of WSC and still need to be investigated. They have attracted a great deal of interest in the WSC context. A wealth of literature has explored the secure service composition problem (Brucker et al., 2013; Carminati et al., 2014; Karatas et al., 2015;
Several research efforts have also been devoted to addressing privacy in service composition (Carminati et al., 2015; Costante et al., 2013a; Jensen, 2013; Squicciarini et al., 2013; Tbahriti et al., 2014). As discussed in the previous section, security and privacy are interrelated, but no existing research works address the problem of security and privacy-based service composition in an interactive manner, which is the focus of this research. The general research question to be answered through this research is:

“How can a security-conscious privacy-preserving service composition be achieved by linking users’ security requirements with their privacy preferences; integrating modeling of users’ privacy preferences, service providers’ privacy policies, and the composition execution process; and selecting the most secure possible composition route(s)?”

On a journey towards security-conscious privacy-preserving service composition, the following questions arising in each phase need to be addressed:

RQ1: How can user input that preserves privacy preference be appropriately modeled? (User input modeling phase)

The proposed solution should be able to answer the following sub-questions raised regarding user input modeling process:

i. How are security requirements inferred based on the privacy preferences expressed by users without their interventions?

ii. How can all possible user input states be mathematically modeled with respect to the defined privacy dimensions?

RQ2: How can the composition execution process be properly modeled to preserve the privacy policies of service providers? (Web service composition modeling phase)
The proposed solution should be able to answer the following sub-question raised regarding modeling of the Web service composition execution process:

i. How can centralized and decentralized orchestration execution be mathematically modeled with respect to all possible states of service providers’ privacy policies?

RQ3: How can the most secure possible composition route(s) be selected to preserve both privacy preferences and privacy policies of service users and providers, respectively? (Selection and optimization phase)

The proposed solution should be able to answer the following sub-questions raised regarding the service comparison and selection process:

i. How can the modeled user input be matched against the modeled composition execution processes (i.e., centralized and decentralized orchestration) based on the defined security requirements and privacy preferences?

ii. How can a multi-criteria selection mechanism be proposed for the matched candidate services to screen and then select composition route(s) with the highest possible security?

iii. How can the power of the empirical optimization technique be employed in selecting a high-performance composition model (i.e., centralized or decentralized orchestration) based on user requests while maintaining the highest possible security level(s)?

1.4 Purpose of the Research

The purpose of this research is to design a security-conscious and privacy-preserving service composition for use in service deployment and coordination for SOC environments. Mathematical modeling of service user privacy preferences in the
form of user input, mathematical modeling of service providers’ privacy policies in the form of centralized and decentralized orchestration is introduced, and an empirical optimization technique is presented.

1.5 Objectives of the Research

The main objective of this study is to model all states of user input and the Web service composition process and then introduce an approach to identify the desired route(s) in an appropriate execution model (centralized or decentralized orchestration) in terms of security requirements and privacy preferences. Therefore, the sub objectives of this research are outlined as follows:

1. To identify the required security based on user privacy preference.

2. To develop a mathematical model for user input that can fulfil all states of privacy preference.

3. To develop mathematical models for centralized and decentralized orchestrations that include all states of service providers’ privacy policy.

4. To develop a mathematical model to compare the developed user input state with the developed centralized and decentralized orchestration states in terms of the required security and privacy identified.

5. To employ a multi-criteria decision-making method on the outcome of comparison model to find the composition route(s) with the highest possible security.

6. To develop empirical models that represents the relationship between independent variables (including purposes, available data items, action types and roles) and dependent variables (including Available Route
Number (ARN) and Available Route Quality (ARQ)) for centralized and decentralized orchestrations to be used for optimization.

1.6 Scope of the Research

This research was inspired by four research directions, namely service selection and composition, security and privacy, multi-criteria decision-making, and statistical-based optimization. In this research:

1. The Web service composition process is limited to the two, choreographed and execution process levels.
2. The information that users can provide as user input are purpose, available data items, visibility, and actions (read-only, modify).
3. The security of the Web service composition process is limited to the CIA principles i.e., confidentiality, integrity, and availability in the orchestration model.
4. The features designed for providers are based on the user inputs and include the goal, requested data items, role, and defined security.
5. The privacy extracted from user input is restricted to the sensitivity and risk concepts, which are directly related to the availability of data items and their actions.
6. The user input states and modeled composition routes of orchestrations (centralized and decentralized) are compared against user request, extracted privacy and defined security criteria.
7. The empirical models are designed based on the D-Optimal method and are employed to optimize the dependent variables (purposes, available data items, action types and roles) and independent variables (including ARN and ARQ).

The choreographed level in this study is assumed to illustrate the service composition architecture and to demonstrate the empirical model’s outcome to select the best composition execution process. Investigating choreographed level details is beyond the scope of this research.
1.7 Significance of the Research

The emergence of loosely coupled and platform-independent SOC eventuates building large computing infrastructures like the Internet, which enable organizations to share information and offer value-added services tailored to all variant needs of users. Web service composition plays a key role in realizing this vision of implementing almost any complex business process (Carminati et al., 2014; Costante et al., 2013c; Karatas et al., 2015).

A growing number of services provide the same functionalities and variant QoS, resulting in a sizable body of literature on QoS-aware service composition. Despite the massive improvements, service composition suffers from improperly addressed challenges. Privacy and security are the two most important challenges that have attracted less attention owing to their complexity. Therefore, security and privacy-aware service composition is still considered a complicated task.

Moreover, the increase in newly emerging SOC paradigms such as cloud computing, and Internet of Things imposes new, unaddressed privacy and security challenges, requiring revisiting the previously addressed problems to propose new outperforming solutions. This research endeavours to open a new horizon for security-conscious privacy-preserving service composition to more securely and privately serve user requests.

1.8 Thesis Organization

This chapter fully discussed the nature of the research, the research gaps and problems faced, the research purpose and objectives, how these research gaps and problems will be addressed, as well as the research scope and significance. The remainder of this thesis is organized as follows:

The second chapter describes a background on research directions, explains the unaddressed challenges, and presents a literature review of existing works on service selection and composition. The proposed research methodology is discussed in
Chapter 3 by providing an overview of the research phases, operational framework, and explanations on the validation and evaluation of these phases.

The forth chapter presents the research design and implementation by introducing the mathematical modeling of the security-conscious privacy-preserving Web service composition process. The proposed techniques and algorithms are described in detail.

The experimental results and a discussion are provided in Chapter 5 to indicate the applicability and feasibility of the proposed approach and investigate its evaluation and validation. Finally, a summary and conclusions of the thesis are provided in Chapter 6 by discussing the contributions of this research and suggesting for potential future research directions.
REFERENCES


Medjahed, B. (2004). *Semantic Web Enabled Composition of Web Services*. Virginia Polytechnic Institute and State University, Virginia, USA.


