

Contents

Contents	i
List of Figures	ii
List of Symbols	iv
Acknowledgements	1
Abstract	1
1 Introduction	3
1.1 A new Level of Trust in CC Environments	4
1.2 Motivation	5
1.3 Contribution	8
1.4 Notation	10
1.5 Related Work	11
1.6 Thesis Organization	14
2 Background	16
2.1 Conventional Service Infrastructure Model	16
2.2 Cloud Infrastructure Models	17
2.2.1 IaaS - Infrastructure-as-a-Service	19
2.2.2 PaaS - Platform-as-a-Service	20
2.2.3 SaaS - Software-as-a-Service	20
2.2.3.1 Amazon Simple Storage Service (Amazon S3)	21
2.3 Distributed Sensor Networks	21
2.3.1 A specific DSN Setup	23
2.4 Data Fusion Models	25
2.4.1 The JDL Process Model	26
2.5 Digital Forensics	28
2.6 Bayesian State Estimation	29
2.6.1 Linear vs. Non-linear	31
2.6.2 The Kalman Filter	33
2.6.3 The Extended Kalman Filter	34
2.6.4 Monte Carlo Methods	35

3	Sources of Forensic Data within Cloud Communication	37
3.1	Investigating Virtual Cloud Instances	38
3.1.1	Volatile Data	40
3.2	Network Forensic Data in Cloud Environments	40
3.3	Browser Forensic Data	42
4	A Simplified Cloud Scenario Environment	44
4.1	Scenario: Suspicious Interaction within a Storage Provider	47
4.1.1	An Abstract DSN Model	48
4.1.2	Protocol Modeling with the Help of Finite State Machines	50
4.1.2.1	Communicating FSMs with DNS and NTP	51
4.1.3	A Discrete System representing a CC Environment	55
5	Pattern Based Identification and Validation of Computational Structures	59
5.1	A Formal Definition for Computational Structures	60
5.2	Uncertainty caused by Observation Probability	62
5.3	Identification of Computational Structures: A Pattern based Approach	67
5.3.1	The Failure of Exact Pattern Approaches	68
5.3.1.1	Pattern Recognition Approaches	68
5.3.1.2	Exact Pattern Matching Approaches	69
5.3.2	Probabilistic Pattern Matching Proposals for Identification of Computational Structures	70
5.4	A Pattern Matching Scenario based on the Levenshtein Distance	73
5.4.1	Issues with the Usage of the Levenshtein Distance	75
6	Fusing and Estimating Uncertain Data for Identification and Validation of Computational Structures	77
6.1	Generic State Space Models	80
6.1.1	State Space Parameter Estimation under Missing Observations	82
6.2	Sequential Monte Carlo Methods	83
6.2.1	Random Number Generation	86
6.2.1.1	Perfect Sampling	87
6.2.1.2	Importance Sampling (IS)	88
6.2.1.3	Sampling Importance Resampling (SIR)	90
6.3	A Generic Particle Filter Approach for Identification and Validation of Computational Structures	91
7	Discussion	94
8	Conclusion	98
	Bibliography	99