1. **Record Nr.** UNICASVEA0080038

Autore Congresso geografico italiano : <15. : ; 1950

Titolo 1

Pubbl/distr/stampa Torino, : ITER, stampa 1952

Descrizione fisica 554 p., [6] c. di tav. (4 ripieg.) : ill. ; 25 cm.

Lingua di pubblicazione Italiano

Formato Materiale a stampa

Livello bibliografico Monografia

2. **Record Nr.** UNINA9910830412903321

Autore Campbell Roy

Titolo Assured cloud computing / / edited by Roy H. Campbell, Charles A. Kamhoua, Kevin A. Kwiat

Pubbl/distr/stampa Hoboken, New Jersey : , : IEEE Computer Society, Inc./Wiley, , 2018

[Piscataqay, New Jersey] : , : IEEE Xplore, , [2018]

ISBN 1-119-42850-5

1-119-42848-3

1-119-42849-1

Edizione [1st edition]

Descrizione fisica 1 online resource (363 pages)

Disciplina 004.67/82

Soggetti Cloud computing

Lingua di pubblicazione Inglese

Formato Materiale a stampa

Livello bibliografico Monografia

Nota di bibliografia Includes bibliographical references and index.

Nota di contenuto Preface xiii -- Editors’ Biographies xvii -- List of Contributors xix -- 1 Introduction 1 /Roy H. Campbell -- 1.1 Introduction 1 -- 1.1.1 Mission-Critical Cloud Solutions for the Military 2 -- 1.2 Overview of the Book 3 -- 2 Survivability: Design, Formal Modeling, and Validation of Cloud Storage Systems Using Maude 10 /Rakesh Bobba, Jon Grov, Indranil Gupta, Si Liu, José Meseguer,Peter Csaba Ö

lveczky, and Stephen Skeirik -- 2.1 Introduction 10 -- 2.1.1 State of the Art 11 -- 2.1.2 Vision: Formal Methods for Cloud Storage Systems 12 -- 2.1.3 The Rewriting Logic Framework 13 -- 2.1.4 Summary: Using Formal Methods on Cloud Storage Systems 15 -- 2.2 Apache Cassandra 17 -- 2.3 Formalizing, Analyzing, and Extending Google’s Megastore 23 -- 2.3.1 Specifying Megastore 23 -- 2.3.2 Analyzing Megastore 25 -- 2.3.2.1 Megastore-CGC 29 -- 2.4 RAMP Transaction Systems 30 -- 2.5 Group Key Management via ZooKeeper 31 -- 2.5.1 ZooKeeper Background 32 -- 2.5.2 System Design 33 -- 2.5.3 Maude Model 34 -- 2.5.4 Analysis and Discussion 35 -- 2.6 How Amazon Web Services Uses Formal Methods 37 -- 2.6.1 Use of Formal Methods 37 -- 2.6.2 Outcomes and Experiences 38 -- 2.6.3 Limitations 39 -- 2.7 Related Work 40 -- 2.8 Concluding Remarks 42 -- 2.8.1 The Future 43 -- 3 Risks and Benefits: Game-Theoretical Analysis and Algorithm for Virtual Machine Security Management in the Cloud 49 /Luke Kwiat, Charles A. Kamhoua, Kevin A. Kwiat, and Jian Tang -- 3.1 Introduction 49 -- 3.2 Vision: Using Cloud Technology in Missions 51 -- 3.3 State of the Art 54 -- 3.4 System Model 57 -- 3.5 Game Model 59 -- 3.6 Game Analysis 61 -- 3.7 Model Extension and Discussion 67 -- 3.8 Numerical Results and Analysis 71 -- 3.8.1 Changes in User 2’s Payoff with Respect to L2 71 -- 3.8.2 Changes in User 2’s Payoff with Respect to e 72 -- 3.8.3 Changes in User 2’s Payoff with Respect to π 73 -- 3.8.4 Changes in User 2’s Payoff with Respect to qI 74 -- 3.8.5 Model Extension to n = 10 Users 75.
3.9 The Future 78 -- 4 Detection and Security: Achieving Resiliency by Dynamic and Passive System Monitoring and Smart Access Control 81 /Zbigniew Kalbarczyk -- 4.1 Introduction 82 -- 4.2 Vision: Using Cloud Technology in Missions 83 -- 4.3 State of the Art 84 -- 4.4 Dynamic VM Monitoring Using Hypervisor Probes 85 -- 4.4.1 Design 86 -- 4.4.2 Prototype Implementation 88 -- 4.4.3 Example Detectors 90 -- 4.4.3.1 Emergency Exploit Detector 90 -- 4.4.3.2 Application Heartbeat Detector 91 -- 4.4.4 Performance 93 -- 4.4.4.1 Microbenchmarks 93 -- 4.4.4.2 Detector Performance 94 -- 4.4.5 Summary 95 -- 4.5 Hypervisor Introspection: A Technique for Evading Passive Virtual Machine Monitoring 96 -- 4.5.1 Hypervisor Introspection 97 -- 4.5.1.1 VMI Monitor 97 -- 4.5.1.2 VM Suspend Side-Channel 97 -- 4.5.1.3 Limitations of Hypervisor Introspection 98 -- 4.5.2 Evading VMI with Hypervisor Introspection 98 -- 4.5.2.1 Insider Attack Model and Assumptions 98 -- 4.5.2.2 Large File Transfer 99 -- 4.5.3 Defenses against Hypervisor Introspection 101 -- 4.5.3.1 Introducing Noise to VM Clocks 101 -- 4.5.3.2 Scheduler-Based Defenses 101 -- 4.5.3.3 Randomized Monitoring Interval 102 -- 4.5.4 Summary 103 -- 4.6 Identifying Compromised Users in Shared Computing Infrastructures 103 -- 4.6.1 Target System and Security Data 104 -- 4.6.1.1 Data and Alerts 105 -- 4.6.1.2 Automating the Analysis of Alerts 106 -- 4.6.2 Overview of the Data 107 -- 4.6.3 Approach 109 -- 4.6.3.1 The Model: Bayesian Network 109 -- 4.6.3.2 Training of the Bayesian Network 110 -- 4.6.4 Analysis of the Incidents 112 -- 4.6.4.1 Sample Incident 112 -- 4.6.4.2 Discussion 113 -- 4.6.5 Supporting Decisions with the Bayesian Network Approach 114 -- 4.6.5.1 Analysis of the Incidents 114 -- 4.6.5.2 Analysis of the Borderline Cases 116 -- 4.6.6 Conclusion 118 -- 4.7 Integrating Attribute-Based Policies into Role-Based Access Control 118 -- 4.7.1 Framework Description 119 -- 4.7.2 Aboveground Level: Tables 119 -- 4.7.2.1 Environment 120.
4.7.2.2 User-Role Assignments 120 -- 4.7.2.3 Role-Permission Assignments 121 -- 4.7.3 Underground Level: Policies 121 -- 4.7.3.1 Role-Permission Assignment Policy 122 -- 4.7.3.2 User-Role

Assignment Policy 123 -- 4.7.4 Case Study: Large-Scale ICS 123 -- 4.7.4.1 RBAC Model-Building Process 124 -- 4.7.4.2 Discussion of Case Study 127 -- 4.7.5 Concluding Remarks 128 -- 4.8 The Future 128 -- 5 Scalability, Workloads, and Performance: Replication, Popularity, Modeling, and Geo-Distributed File Stores 133 /Roy H. Campbell, Shadi A. Noghabi, and Cristina L. Abad -- 5.1 Introduction 133 -- 5.2 Vision: Using Cloud Technology in Missions 134 -- 5.3 State of the Art 136 -- 5.4 Data Replication in a Cloud File System 137 -- 5.4.1 MapReduce Clusters 138 -- 5.4.1.1 File Popularity, Temporal Locality, and Arrival Patterns 142 -- 5.4.1.2 Synthetic Workloads for Big Data 144 -- 5.4.2 Related Work 147 -- 5.4.3 Contribution from Our Approach to Generating Big Data Request Streams Using Clustered Renewal Processes 149 -- 5.4.3.1 Scalable Geo-Distributed Storage 149 -- 5.4.4 Related Work 151 -- 5.4.5 Summary of Ambry 152 -- 5.5 Summary 153 -- 5.6 The Future 153 -- 6 Resource Management: Performance Assuredness in Distributed Cloud Computing via Online Reconfigurations 160 /Mainak Ghosh, Le Xu, and Indranil Gupta -- 6.1 Introduction 161 -- 6.2 Vision: Using Cloud Technology in Missions 163 -- 6.3 State of the Art 164 -- 6.3.1 State of the Art: Reconfigurations in Sharded Databases/Storage 164 -- 6.3.1.1 Database Reconfigurations 164 -- 6.3.1.2 Live Migration 164 -- 6.3.1.3 Network Flow Scheduling 164 -- 6.3.2 State of the Art: Scale-Out/Scale-In in Distributed Stream Processing Systems 165 -- 6.3.2.1 Real-Time Reconfigurations 165 -- 6.3.2.2 Live Migration 165 -- 6.3.2.3 Real-Time Elasticity 165 -- 6.3.3 State of the Art: Scale-Out/Scale-In in Distributed Graph Processing Systems 166 -- 6.3.3.1 Data Centers 166 -- 6.3.3.2 Cloud and Storage Systems 166 -- 6.3.3.3 Data Processing Frameworks 166.

6.3.3.4 Partitioning in Graph Processing 166 -- 6.3.3.5 Dynamic Repartitioning in Graph Processing 167 -- 6.3.4 State of the Art: Priorities and Deadlines in Batch Processing Systems 167 -- 6.3.4.1 OS Mechanisms 167 -- 6.3.4.2 Preemption 167 -- 6.3.4.3 Real-Time Scheduling 168 -- 6.3.4.4 Fairness 168 -- 6.3.4.5 Cluster Management with SLOs 168 -- 6.4 Reconfigurations in NoSQL and Key-Value Storage/Databases 169 -- 6.4.1 Motivation 169 -- 6.4.2 Morphus: Reconfigurations in Sharded Databases/Storage 170 -- 6.4.2.1 Assumptions 170 -- 6.4.2.2 MongoDB System Model 170 -- 6.4.2.3 Reconfiguration Phases in Morphus 171 -- 6.4.2.4 Algorithms for Efficient Shard Key Reconfigurations 172 -- 6.4.2.5 Network Awareness 175 -- 6.4.2.6 Evaluation 175 -- 6.4.3 Parqua: Reconfigurations in Distributed Key-Value Stores 179 -- 6.4.3.1 System Model 180 -- 6.4.3.2 System Design and Implementation 181 -- 6.4.3.3 Experimental Evaluation 183 -- 6.5 Scale-Out and Scale-In Operations 185 -- 6.5.1 Stela: Scale-Out/Scale-In in Distributed Stream Processing Systems 186 -- 6.5.1.1 Motivation 186 -- 6.5.1.2 Data Stream Processing Model and Assumptions 187 -- 6.5.1.3 Stela: Scale-Out Overview 187 -- 6.5.1.4 Effective Throughput Percentage (ETP) 188 -- 6.5.1.5 Iterative Assignment and Intuition 190 -- 6.5.1.6 Stela: Scale-In 191 -- 6.5.1.7 Core Architecture 191 -- 6.5.1.8 Evaluation 193 -- 6.5.1.9 Experimental Setup 193 -- 6.5.1.10 Yahoo! Storm Topologies and Network Monitoring Topology 193 -- 6.5.1.11 Convergence Time 195 -- 6.5.1.12 Scale-In Experiments 196 -- 6.5.2 Scale-Out/Scale-In in Distributed Graph Processing Systems 197 -- 6.5.2.1 Motivation 197 -- 6.5.2.2 What to Migrate, and How? 199 -- 6.5.2.3 When to Migrate? 201 -- 6.5.2.4 Evaluation 203 -- 6.6 Priorities and Deadlines in Batch Processing Systems 204 -- 6.6.1 Natjam: Supporting Priorities and Deadlines in Hadoop 204 -- 6.6.1.1 Motivation 204 -- 6.6.1.2 Eviction Policies for a Dual-Priority Setting 206 -- 6.6.1.3 Natjam Architecture

209.
6.6.1.4 Natjam-R: Deadline-Based Eviction 215 -- 6.6.1.5 Microbenchmarks 216 -- 6.6.1.6 Natjam-R Evaluation 221 -- 6.7 Summary 223 -- 6.8 The Future 224 -- 7 Theoretical Considerations: Inferring and Enforcing Use Patterns for Mobile Cloud Assurance 237 /Gul Agha, Minas Charalambides, Kirill Mechitov, Karl Palmskog,Atul Sandur, and Reza Shiftehfar -- 7.1 Introduction 237 -- 7.2 Vision 239 -- 7.3 State of the Art 240 -- 7.3.1 Code Offloading 241 -- 7.3.2 Coordination Constraints 241 -- 7.3.3 Session Types 242 -- 7.4 Code Offloading and the IMCM Framework 243 -- 7.4.1 IMCM Framework: Overview 244 -- 7.4.2 Cloud Application and Infrastructure Models 244 -- 7.4.3 Cloud Application Model 245 -- 7.4.4 Defining Privacy for Mobile Hybrid Cloud Applications 247 -- 7.4.5 A Face Recognition Application 247 -- 7.4.6 The Design of an Authorization System 249 -- 7.4.7 Mobile Hybrid Cloud Authorization Language 250 -- 7.4.7.1 Grouping, Selection, and Binding 252 -- 7.4.7.2 Policy Description 252 -- 7.4.7.3 Policy Evaluation 253 -- 7.4.8 Performance- and Energy-Usage-Based Code Offloading 254 -- 7.4.8.1 Offloading for Sequential Execution on a Single Server 254 -- 7.4.8.2 Offloading for Parallel Execution on Hybrid Clouds 255 -- 7.4.8.3 Maximizing Performance 255 -- 7.4.8.4 Minimizing Energy Consumption 256 -- 7.4.8.5 Energy Monitoring 257 -- 7.4.8.6 Security Policies and Energy Monitoring 258 -- 7.5 Coordinating Actors 259 -- 7.5.1 Expressing Coordination 259 -- 7.5.1.1 Synchronizers 260 -- 7.5.1.2 Security Issues in Synchronizers 260 -- 7.6 Session Types 264 -- 7.6.1 Session Types for Actors 265 -- 7.6.1.1 Example: Sliding Window Protocol 265 -- 7.6.2 Global Types 266 -- 7.6.3 Programming Language 268 -- 7.6.4 Local Types and Type Checking 269 -- 7.6.5 Realization of Global Types 270 -- 7.7 The Future 271 -- Acknowledgments 272 -- 8 Certifications Past and Future: A Future Model for Assigning Certifications that Incorporate Lessons Learned from Past Practices 277 /Masooda Bashir, Carlo Di Giulio, and Charles A. Kamhoua.
8.1 Introduction 277 -- 8.1.1 What Is a Standard? 279 -- 8.1.2 Standards and Cloud Computing 281 -- 8.2 Vision: Using Cloud Technology in Missions 283 -- 8.3 State of the Art 284 -- 8.3.1 The Federal Risk Authorization Management Program 286 -- 8.3.2 SOC Reports and TSPC 288 -- 8.3.3 ISO/IEC 27001 291 -- 8.3.4 Main Differences among the Standards 292 -- 8.3.5 Other Existing Frameworks 293 -- 8.3.5.1 PCI-DSS 293 -- 8.3.5.2 C5 294 -- 8.3.5.3 STAR 294 -- 8.3.6 What Protections Do Standards Offer against Vulnerabilities in the Cloud? 294 -- 8.4 Comparison among Standards 296 -- 8.4.1 Strategy for Comparing Standards 298 -- 8.4.2 Patterns, Anomalies, and Discoveries 299 -- 8.5 The Future 302 -- 8.5.1 Current Challenges 304 -- 8.5.2 Opportunities 305 -- 9 Summary and Future Work 312 /Roy H. Campbell -- 9.1 Survivability 312 -- 9.2 Risks and Benefits 313 -- 9.3 Detection and Security 314 -- 9.4 Scalability, Workloads, and Performance 316 -- 9.5 Resource Management 319 -- 9.6 Theoretical Considerations: Inferring and Enforcing Use Patterns for Mobile Cloud Assurance 321 -- 9.7 Certifications 322 -- Index 327.

Sommario/riassunto

Explores themes that drive individual contributions, including design correctness, support for big data and analytics, monitoring and detection, network considerations, and performance - Synthesizes highly cited earlier work (on topics including DARE, trust mechanisms, and elastic graphs) as well as newer research findings on topics including R-Storm, and RAMP transactions - Addresses assured cloud computing concerns such as game theory, stream processing, storage, algorithms, workflow, scheduling, access control, formal analysis of safety, and streaming Marketing Description: IEEE Computer Society,

the IEEE Reliability Society, and the IEEE Systems, Man, and Cybernetics Society--