The Connection Algorithm Take Risks Defy The Status Quo And Live Your Passions

The Consultative paper issued by the Basel Committee on Banking Supervision (Basel II) cites the failure of bankers to adequately stress test exposures as a major reason for bad loans. Sample quotes from this crucial document: * "Banks should take into consideration potential future changes in economic conditions when assessing individual credits and their credit portfolios, and should assess their credit risk exposures under stressful conditions." * "The recent disturbances in Asia and Russia illustrate how close linkages among emerging markets under stress conditions and previously undetected correlations between market and credit risks, as well as between those risks and liquidity risk, can produce widespread losses." * "Effective stress testing which takes account of business or product cycle effects is one approach to incorporating into credit decisions a fuller understanding of a borrower's credit risk." Written for professionals in financial services with responsibility for IT and risk measurement, management, and modeling, Dimitris Chorafas explains in clear language the testing methodology necessary for risk control to meet Basel II requirements. Stress testing is the core focus of the book, covering stress analysis and the use of scenarios, models, drills, benchmarking, backtesting, and post-mortems, creditworthiness, wrong way risk and statistical inference, probability of default, loss given default and exposure at default, stress testing expected losses, correlation coefficients, and unexpected losses, stress testing related to market discipline and control action, and pillars 2 and 3 of

Basel II. * Written in clear, straightforward style with numerous practical examples * Based on five years of development and research * Focuses on stress probability of default, stress loss given default, stsress exposure at default l This book evolved from the ARCADE evaluation exercise that started in 1995. The project's goal is to evaluate alignment systems for parallel texts, i. e. , texts accompanied by their translation. Thirteen teams from various places around the world have participated so far and for the first time, some ten to fifteen years after the first alignment techniques were designed, the community has been able to get a clear picture of the behaviour of alignment systems. Several chapters in this book describe the details of competing systems, and the last chapter is devoted to the description of the evaluation protocol and results. The remaining chapters were especially commissioned from researchers who have been major figures in the field in recent years, in an attempt to address a wide range of topics that describe the state of the art in parallel text processing and use. As I recalled in the introduction, the Rosetta stone won eternal fame as the prototype of parallel texts, but such texts are probably almost as old as the invention of writing. Nowadays, parallel texts are electronic, and they are be coming an increasingly important resource for building the natural language processing tools needed in the "multilingual information society" that is cur rently emerging at an incredible speed. Applications are numerous, and they are expanding every day: multilingual lexicography and terminology, machine and human translation, cross-language information retrieval, language learning, etc.

Patterns can be any number of items that occur repeatedly, whether in the behaviour of animals, humans, traffic, or even in the appearance of a design. As technologies continue to advance, recognizing, mimicking, and responding to all types

of patterns becomes more precise. Pattern Recognition and Classification in Time Series Data focuses on intelligent methods and techniques for recognizing and storing dynamic patterns. Emphasizing topics related to artificial intelligence, pattern management, and algorithm development, in addition to practical examples and applications, this publication is an essential reference source for graduate students, researchers, and professionals in a variety of computer-related disciplines.

This book constitutes the refereed proceedings of the 34th International Conference on Conceptual Modeling, ER 2015, held in Stockholm, Sweden, in October 2015. The 26 full and 19 short papers presented were carefully reviewed and selected from 131 submissions. The papers are organized in topical sections on business process and goal models, ontology-based models and ontology patterns, constraints, normalization, interoperability and integration, collaborative modeling, variability and uncertainty modeling, modeling and visualization of user generated content, schema discovery and evolution, process and text mining, domain-based modeling, data models and semantics, and applications of conceptual modeling.

"This book brings together scholars with significantly different backgrounds who share interests in the interplay between trust and technology, presenting novel theoretical perspectives on the topics of trust and technology, as well as some empirical investigations into the trust-building, trust-repairing, and trust-destroying practices in the context of technology"--Provided by publisher.

The fourth edition of Principles of Information Security explores the field of information security and assurance with updated content including new innovations in technology and methodologies. Students will revel in the comprehensive coverage that includes a historical overview of information

security, discussions on risk management and security technology, current certification information, and more. The text builds on internationally-recognized standards and bodies of knowledge to provide the knowledge and skills students need for their future roles as business decision-makers. Information security in the modern organization is a management issue which technology alone cannot answer; it is a problem that has important economic consequences for which management will be held accountable. Students can feel confident that they are using a standards-based, content-driven resource to prepare for their work in the field. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

This book introduces the Special Issue entitled "Applications of Internet of Things", of ISPRS International Journal of Geo-Information. Topics covered in this issue include three main parts: (I) intelligent transportation systems (ITSs), (II) location-based services (LBSs), and (III) sensing techniques and applications. Three papers on ITSs are as follows: (1) "Vehicle positioning and speed estimation based on cellular network signals for urban roads," by Lai and Kuo; (2) "A method for traffic congestion clustering judgment based on grey relational analysis," by Zhang et al.; and (3) "Smartphone-based pedestrian's avoidance behavior recognition towards opportunistic road anomaly detection," by Ishikawa and Fujinami. Three papers on LBSs are as follows: (1) "A high-efficiency method of mobile positioning based on commercial vehicle operation data," by Chen et al.; (2) "Efficient location privacy-preserving k-anonymity method based on the credible chain," by Wang et al.; and (3) "Proximity-based asynchronous messaging platform for location-based Internet of things service," by Gon Jo et al. Two papers on sensing techniques and applications are as

follows: (1) "Detection of electronic anklet wearers' groupings throughout telematics monitoring," by Machado et al.; and (2) "Camera coverage estimation based on multistage grid subdivision," by Wang et al.

This book constitutes the refereed post-proceedings of the Third European Workshop on Software Architecture, EWSA 2006, held in France in September 2006. The 13 revised full research papers and five revised position papers presented together with one invited talk were carefully reviewed and selected. All current aspects of software architectures are addressed ranging from foundational and methodological issues to application issues of practical relevance.

Revised and updated with the latest data in the field, Fundamentals of Information Systems Security, Third Edition provides a comprehensive overview of the essential concepts readers must know as they pursue careers in information systems security. The text opens with a discussion of the new risks, threats, and vulnerabilities associated with the transition to a digital world. Part 2 presents a high level overview of the Security+ Exam and provides students with information as they move toward this certification.

GUIDE TO NETWORK DEFENSE AND COUNTERMEASURES provides a thorough guide to perimeter defense fundamentals, including intrusion detection and firewalls. This trusted text

also covers more advanced topics such as security policies, network address translation (NAT), packet filtering and analysis, proxy servers, virtual private networks (VPN), and network traffic signatures. Thoroughly updated, the new third edition reflects the latest technology, trends, and techniques including virtualization, VMware, IPv6, and ICMPv6 structure, making it easier for current and aspiring professionals to stay on the cutting edge and one step ahead of potential security threats. A clear writing style and numerous screenshots and illustrations make even complex technical material easier to understand, while tips, activities, and projects throughout the text allow you to hone your skills by applying what you learn. Perfect for students and professionals alike in this high-demand, fast-growing field, GUIDE TO NETWORK DEFENSE AND COUNTERMEASURES, Third Edition, is a must-have resource for success as a network security professional. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

This glossary provides a central resource of definitions most commonly used in Nat. Institute of Standards and Technology (NIST) information security publications and in the Committee for National Security Systems (CNSS) information assurance publications. Each entry in the glossary

points to one or more source NIST publications, and/or CNSSI-4009, and/or supplemental sources where appropriate. This is a print on demand edition of an important, hard-to-find publication. ASP.NET 4 is the principal standard for creating dynamic web pages on the Windows platform. Pro ASP.NET 4 in C# 2010 raises the bar for high-quality, practical advice on learning and deploying Microsoft's dynamic web solution. This edition is updated with everything you need to master up to version 4 of ASP.NET, including coverage of ASP.NET MVC, ASP.NET AJAX 4, ASP.NET Dynamic Data, and Silverlight 3. Seasoned .NET professionals Matthew MacDonald and Mario Szpuszta explain how you can get the most from these groundbreaking technologies. They cover ASP.NET 4 as a whole, illustrating both the newer features and the functionality carried over from previous versions of ASP. This book will give you the knowledge you need to code real ASP.NET 4 applications in the best possible style. This book constitutes the refereed proceedings of the 10th IFIP WG 5.11 International Symposium on Environmental Software Systems, ISESS 2013, held in Neusiedl am See, Austria, in June 2013. The 65 revised full papers presented were carefully reviewed and selected from numerous submissions. The papers are organized in the following topical sections: environmental application in the scope of

the future Internet; smart and mobile devices used for environmental applications; information tools for global environmental assessment; environmental applications in risk and crises management; SEIS as a part of the 7th environment action programme of EU; human interaction and human factors driving future EIS/EDSS developments; environmental management/-accounting and -statistics; and information systems and applications. Developing techniques for assessing various risks and calculating probabilities of ruin and survival are exciting topics for mathematically-inclined academics. For practicing actuaries and financial engineers, the resulting insights have provided enormous opportunities but also created serious challenges to overcome, thus facilitating closer cooperation between industries and academic institutions. In this book, several renown researchers with extensive interdisciplinary research experiences share their thoughts that, in one way or another, contribute to the betterment of practice and theory of decision making under uncertainty. Behavioral, cultural, mathematical, and statistical aspects of risk assessment and modelling have been explored, and have been often illustrated using real and simulated data. Topics range from financial and insurance risks to security-type risks, from one-dimensional to multi- and even infinite-dimensional risks. The articles in the book were written with a broad audience in mind

and should provide enjoyable reading for those with university level degrees and/or those who have studied for accreditation by various actuarial and financial societies.

This book constitutes the joint refereed proceedings of the 12 International Conference on Next Generation Teletraffic and Wired/Wireless Advanced Networking, NEW2AN, and the 5th Conference on Internet of Things and Smart Spaces, ruSMART 2012, held in St. Petersburg, Russia, in August 2012. The total of 42 papers was carefully reviewed and selected for inclusion in this book. The 14 papers selected from ruSMART are organized in topical sections named: defining an internet-of-things ecosystem; future services; and smart space governing through service mashups. The 28 papers from NEW2AN deal with the following topics: wireless cellular networks; ad-hoc, mesh, and delay-tolerant networks; scalability, cognition, and self-organization; traffic and internet applications; and wireless sensor networks. They also contain 4 selected papers from the NEW2AN 2012 winter session.

Considered the gold-standard reference on information security, the Information Security Management Handbook provides an authoritative compilation of the fundamental knowledge, skills, techniques, and tools required of today's IT security professional. Now in its sixth edition, this 3200 page,

4 volume stand-alone reference is organized under the CISSP Common Body of Knowledge domains and has been updated yearly. Each annual update, the latest is Volume 6, reflects the changes to the CBK in response to new laws and evolving technology.

A bold reassessment of "smart cities" that reveals what is lost when we conceive of our urban spaces as computers Computational models of urbanism—smart cities that use data-driven planning and algorithmic administration—promise to deliver new urban efficiencies and conveniences. Yet these models limit our understanding of what we can know about a city. A City Is Not a Computer reveals how cities encompass myriad forms of local and indigenous intelligences and knowledge institutions, arguing that these resources are a vital supplement and corrective to increasingly prevalent algorithmic models. Shannon Mattern begins by examining the ethical and ontological implications of urban technologies and computational models, discussing how they shape and in many cases profoundly limit our engagement with cities. She looks at the methods and underlying assumptions of data-driven urbanism, and demonstrates how the "city-as-computer" metaphor, which undergirds much of today's urban policy and design, reduces place-based knowledge to information processing. Mattern then imagines how we might sustain institutions and

infrastructures that constitute more diverse, open, inclusive urban forms. She shows how the public library functions as a steward of urban intelligence, and describes the scales of upkeep needed to sustain a city's many moving parts, from spinning hard drives to bridge repairs. Incorporating insights from urban studies, data science, and media and information studies, A City Is Not a Computer offers a visionary new approach to urban planning and design.

This volume of Advances in Intelligent Systems and Computing highlights key scientific achievements and innovations in all areas of automation, informatization, computer science, and artificial intelligence. It gathers papers presented at the IITI 2017, the Second International Conference on Intelligent Information Technologies for Industry, which was held in Varna, Bulgaria on September 14–16, 2017. The conference was jointly co-organized by Technical University of Varna (Bulgaria), Technical University of Sofia (Bulgaria), VSB Technical University of Ostrava (Czech Republic) and Rostov State Transport University (Russia). The IITI 2017 brought together international researchers and industrial practitioners interested in the development and implementation of modern technologies for automation, informatization, computer science, artificial intelligence, transport and power electrical engineering. In addition to

advancing both fundamental research and innovative applications, the conference is intended to establish a new dissemination platform and an international network of researchers in these fields.

Most applications these days are at least somewhat network aware, but how do you protect those applications against common network security threats? Many developers are turning to OpenSSL, an open source version of SSL/TLS, which is the most widely used protocol for secure network communications.The OpenSSL library is seeing widespread adoption for web sites that require cryptographic functions to protect a broad range of sensitive information, such as credit card numbers and other financial transactions. The library is the only free, full-featured SSL implementation for C and C++, and it can be used programmatically or from the command line to secure most TCP-based network protocols.Network Security with OpenSSL enables developers to use this protocol much more effectively. Traditionally, getting something simple done in OpenSSL could easily take weeks. This concise book gives you the guidance you need to avoid pitfalls, while allowing you to take advantage of the library?s advanced features. And, instead of bogging you down in the technical details of how SSL works under the hood, this book provides only the information that is necessary to use OpenSSL safely and effectively. In step-by-step fashion, the

book details the challenges in securing network communications, and shows you how to use OpenSSL tools to best meet those challenges.As a system or network administrator, you will benefit from the thorough treatment of the OpenSSL command-line interface, as well as from step-by-step directions for obtaining certificates and setting up your own certification authority. As a developer, you will further benefit from the in-depth discussions and examples of how to use OpenSSL in your own programs. Although OpenSSL is written in C, information on how to use OpenSSL with Perl, Python and PHP is also included.OpenSSL may well answer your need to protect sensitive data. If that?s the case, Network Security with OpenSSL is the only guide available on the subject.

Collaboration in business allows for equitable opportunities and inclusive growth as the economy rises while also permitting partnering organizations to adopt and utilize the latest successful practices and management. However, a market in stasis may require a displacement in order to allow businesses to grow and create new alliances and partnerships toward a shared economy. There is a need for studies that seek to understand the necessity of market disruption and the best supervisory methods for remaining relevant and profitable in a time of change. The Handbook of Research on Managerial Practices and Disruptive Innovation in Asia is an

essential reference source that explores successful executive behavior and business operations striving toward a more inclusive economy. Featuring research on topics such as employee welfare, brand orientation, and entrepreneurship, this publication is ideally designed for human resources developers, policymakers, IT specialists, economists, executives, managers, corporate directors, information technologists, and academicians seeking current research focusing on innovative business factors and sustainable economies in Asia.

The Linux Programming Interface (TLPI) is the definitive guide to the Linux and UNIX programming interface—the interface employed by nearly every application that runs on a Linux or UNIX system. In this authoritative work, Linux programming expert Michael Kerrisk provides detailed descriptions of the system calls and library functions that you need in order to master the craft of system programming, and accompanies his explanations with clear, complete example programs. You'll find descriptions of over 500 system calls and library functions, and more than 200 example programs, 88 tables, and 115 diagrams. You'll learn how to: –Read and write files efficiently –Use signals, clocks, and timers –Create processes and execute programs –Write secure programs –Write multithreaded programs using POSIX threads –Build and use shared libraries –Perform interprocess communication using pipes,

message queues, shared memory, and semaphores –Write network applications with the sockets API While The Linux Programming Interface covers a wealth of Linux-specific features, including epoll, inotify, and the /proc file system, its emphasis on UNIX standards (POSIX.1-2001/SUSv3 and POSIX.1-2008/SUSv4) makes it equally valuable to programmers working on other UNIX platforms. The Linux Programming Interface is the most comprehensive single-volume work on the Linux and UNIX programming interface, and a book that's destined to become a new classic.

This book comprises high-quality refereed research papers presented at the Fourth International Conference on Computer Science, Engineering and Education Applications (ICCSEEA2021), held in Kyiv, Ukraine, on January 2324, 2021, organized jointly by the National Technical University of Ukraine Igor Sikorsky Kyiv Polytechnic Institute, National Aviation University, and the International Research Association of Modern Education and Computer Science. The topics discussed in the book include state-of-the-art papers in computer science, artificial intelligence, engineering techniques, genetic coding systems, deep learning with its medical applications, and knowledge representation with its applications in education. It is an excellent source of references for researchers, graduate students, engineers, management practitioners, and undergraduate students interested in computer science and their applications in engineering and education.

This book constitutes the thoroughly refereed conference proceedings of the First International Workshop on Risk Assessment and Risk-driven Testing, RISK 2013, held in conjunction with 25th IFIP International Conference on Testing Software and Systems, ICTSS 2013, in Istanbul, Turkey, in November 2013. The revised full papers were carefully reviewed and selected from 13 submissions. The papers are organized in topical sections on risk analysis, risk modeling and risk-based testing. The Connection AlgorithmTake Risks, Defy the Status Quo, and Live Your PassionsA Joosr Guide to ... The Connection Algorithm by Jesse TevelowTake Risks, Defy the Status Quo, and Live Your PassionsRisks and Security of Internet and Systems13th International Conference, CRiSIS 2018, Arcachon, France, October 16–18, 2018, Revised Selected PapersSpringer The era of quantum computing is about to begin, with profound implications for the global economy and the financial system. Rapid development of quantum computing brings both benefits and risks. Quantum computers can revolutionize industries and fields that require significant computing power, including modeling financial markets, designing new effective medicines and vaccines, and empowering artificial intelligence, as well as creating a new and secure way of communication (quantum Internet). But they would also crack many of the current encryption algorithms and threaten financial stability by compromising the security of mobile banking, e-commerce, fintech, digital currencies, and Internet information exchange. While the work on quantum-safe encryption is still in progress, financial institutions should

take steps now to prepare for the cryptographic transition, by assessing future and retroactive risks from quantum computers, taking an inventory of their cryptographic algorithms (especially public keys), and building cryptographic agility to improve the overall cybersecurity resilience.

In recent years, ELM has emerged as a revolutionary technique of computational intelligence, and has attracted considerable attentions. An extreme learning machine (ELM) is a single layer feed-forward neural network alike learning system, whose connections from the input layer to the hidden layer are randomly generated, while the connections from the hidden layer to the output layer are learned through linear learning methods. The outstanding merits of extreme learning machine (ELM) are its fast learning speed, trivial human intervene and high scalability. This book contains some selected papers from the International Conference on Extreme Learning Machine 2013, which was held in Beijing China, October 15-17, 2013. This conference aims to bring together the researchers and practitioners of extreme learning machine from a variety of fields including artificial intelligence, biomedical engineering and bioinformatics, system modelling and control, and signal and image processing, to promote research and discussions of "learning without iterative tuning". This book covers algorithms and applications of ELM. It gives readers a glance of the newest developments of ELM. Robo-Advisory is a field that has gained momentum over recent years, propelled by the increasing digitalization and automation of global financial markets. More and

more money has been flowing into automated advisory, raising essential questions regarding the foundations, mechanics, and performance of such solutions. However, a comprehensive summary taking stock of this new solution at the intersection of finance and technology with consideration for both aspects of theory and implementation has so far been wanting. This book offers such a summary, providing unique insights into the state of Robo-Advisory. Drawing on a pool of expert authors from within the field, this edited collection aims at being the vital go-to resource for academics, students, policy-makers, and practitioners alike wishing to engage with the topic. Split into four parts, the book begins with a survey of academic literature and its key insights paired with an analysis of market developments in Robo-Advisory thus far. The second part tackles specific questions of implementation, which are complemented by practical case studies in Part III. Finally, the fourth part looks ahead to the future, addressing questions of key importance such as artificial intelligence, big data, and social networks. Thereby, this timely book conveys both a comprehensive grasp of the status-quo as well as a guiding outlook onto future trends and developments within the field.

Firewalls are among the best-known network security tools in use today, and their critical role in information security continues to grow. However, firewalls are most effective when backed by thoughtful security planning, well-designed security policies, and integrated support from anti-virus software, intrusion detection systems, and related tools. GUIDE TO FIREWALLS AND VPNs,

THIRD EDITION explores firewalls in the context of these critical elements, providing an in-depth guide that focuses on both managerial and technical aspects of security. Coverage includes packet filtering, authentication, proxy servers, encryption, bastion hosts, virtual private networks (VPNs), log file maintenance, and intrusion detection systems. The text also features an abundant selection of realistic projects and cases incorporating cutting-edge technology and current trends, giving students the opportunity to hone and apply the knowledge and skills they will need as working professionals. GUIDE TO FIREWALLS AND VPNs includes new and updated cases and projects, enhanced coverage of network security and VPNs, and information on relevant National Institute of Standards and Technology guidelines used by businesses and information technology professionals. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

This book documents the state of the art in the field of ambient assisted living (AAL), highlighting the impressive potential of novel methodologies and technologies to enhance well-being and promote active ageing. The coverage is wide ranging, with sections on assistive devices, elderly people monitoring, home rehabilitation, ICT solutions for AAL, living with chronic conditions, robotic assistance for the elderly, sensing technologies for AAL, and smart housing. The book comprises a selection of the best papers presented at the Fifth Italian Forum on Ambient Assisted Living, which was held in Catania, Italy, in September 2014 and brought together end users, technology teams, and policy makers to

develop a consensus on how to improve provision for elderly and impaired people. Readers will find that the expert contributions offer clear insights into the ways in which the most recent exciting advances may be expected to assist in addressing the needs of the elderly and those with chronic conditions.

This book presents the proceedings of The 2020 International Conference on Machine Learning and Big Data Analytics for IoT Security and Privacy (SPIoT-2020), held in Shanghai, China, on November 6, 2020. Due to the COVID-19 outbreak problem, SPIoT-2020 conference was held online by Tencent Meeting. It provides comprehensive coverage of the latest advances and trends in information technology, science and engineering, addressing a number of broad themes, including novel machine learning and big data analytics methods for IoT security, data mining and statistical modelling for the secure IoT and machine learning-based security detecting protocols, which inspire the development of IoT security and privacy technologies. The contributions cover a wide range of topics: analytics and machine learning applications to IoT security; data-based metrics and risk assessment approaches for IoT; data confidentiality and privacy in IoT; and authentication and access control for data usage in IoT. Outlining promising future research directions, the book is a valuable resource for students, researchers and professionals and provides a useful reference guide for newcomers to the IoT security and privacy field

This book constitutes the revised selected papers from the 13th International Conference on Risks and Security of Internet and Systems, CRiSIS 2018, held in Arcachon, France, in October 2018. The 12 full papers and 6 short papers presented in this volume were carefully reviewed and selected from 34 submissions. They cover diverse research themes that range from classic topics, such as vulnerability

analysis and classification; apps security; access control and filtering; cloud security; cyber-insurance and cyber threat intelligence; human-centric security and trust; and risk analysis.

The refereed post-proceedings of the First International Symposium on Combinatorics, Algorithms, Probabilistic and Experimental Methodologies are presented in this volume. The symposium provided an interdisciplinary forum for researchers to share their discoveries and approaches. The 46 full papers address large data processing problems using different methodologies from major disciplines such as computer science, combinatorics, and statistics.

Cybersecurity for medical devices is no longer optional. We must not allow sensationalism or headlines to drive the discussion… Nevertheless, we must proceed with urgency. In the end, this is about preventing patient harm and preserving patient trust. A comprehensive guide to medical device secure lifecycle management, this is a book for engineers, managers, and regulatory specialists. Readers gain insight into the security aspects of every phase of the product lifecycle, including concept, design, implementation, supply chain, manufacturing, postmarket surveillance, maintenance, updates, and end of life. Learn how to mitigate or completely avoid common cybersecurity vulnerabilities introduced during development and production. Grow your awareness of cybersecurity development topics ranging from high-level concepts to practical solutions and tools. Get insight into emerging regulatory and customer expectations. Uncover how to minimize schedule impacts and accelerate time-to-market while still accomplishing the main goal: reducing patient and business exposure to cybersecurity risks. Medical Device Cybersecurity for Engineers and Manufacturers is designed to help all stakeholders lead the charge to a better medical device security posture and improve the resilience of

our medical device ecosystem.

Contains references to documents in the NASA Scientific and Technical (STI) Database.

Copyright: 46989a0fcbe4702b7bc711ec6dadf1fb