Ieee Base Paper About Phishing File Type

The mission of the FedCSIS Conference Series is to provide a presentation, discussion and a reputable publication forum in computer science and information systems The forum invites researchers and practitioners from around the world to contribute their research results focused on their scientific and professional interests in a chosen conference track The FedCSIS conference consists of Tracks divided into Technical Sessions Sessions are preannounced in a Call for Papers and refer to a significant number of recurring events Each year, new events are solicited in Calls for Technical Sessions Technical sessions can accentuate special formats of events (symposia, workshops, seminars, focused conferences, etc) reflecting the common interests of research or professional communities proposing the sessions

The preservation of private data is a main concern of governments, organizations, and individuals alike. For individuals, a breach in personal information can mean dire consequences for an individual's finances,

medical information, and personal property. Identity Theft: Breakthroughs in Research and Practice highlights emerging perspectives and critical insights into the preservation of personal data and the complications that can arise when one's identity is compromised. This critical volume features key research on methods and technologies for protection, the problems associated with identity theft, and outlooks for the future. This publication is an essential resource for information security professionals, researchers, and graduate-level students in the fields of criminal science, business, and computer science. This book constitutes the refereed proceedings of the 12th International Conference on Information Systems Security, ICISS 2016, held in Jaipur, India, in December 2016. The 24 revised full papers and 8 short papers presented together with 4 invited papers were carefully reviewed and selected from 196 submissions. The papers address the following topics: attacks and mitigation; authentication; authorization and information flow control; crypto systems and protocols; network security and intrusion detection; privacy; software security; and wireless, mobile and IoT security. The concept of smart cities has spurred

research and development in the domain of smart innovation i e sensor technology, data analytics, energy efficient planning and development, and decision making Sensor technology is applicable in several domains of engineering, such as Civil Engineering, Electrical Engineering, Mechanical Engineering, where the development of sensors is pioneered by the Electronics Engineering Such sensors are applicable in and for environmental audit and pollution monitoring, understanding of structural health e g bridges, dams and tectonic movements, efficient planning and monitoring of sensor networks through data analytics in the spatial and temporal domains and monitoring of engines related to performance, temperature and wear and tear The aim of the conference is to bring together the experts on separate disciplines and encourage multi disciplinary research, and work on techniques and algorithms for the development of regions with special requirements

Advanced Computer and Communication Engineering Technology

Attacks, Applications, Authentication, and Fundamentals

11th International Conference, ICA3PP 2011, Workshops, Melbourne, Australia, October

24-26, 2011, Proceedings
2021 12th International Conference on
Information and Communication Systems
(ICICS)
4th VLDB Workshop, SDM 2007, Vienna,
Austria, September 23-24, 2007, Proceedings
12th International Conference, ICISS 2016,
Jaipur, India, December 16-20, 2016,
Proceedings
Understanding the Increasing Problem of
Electronic Identity Theft
**Data Science and Big Data, Evolutionary
Computation, Big Data Analytics, Data
Engineering Intelligent Systems, NLP,
Computer Security, IoT
This book presents selected papers from the
International Conference on Emerging
Research in Computing, Information,
Communication and Applications, ERCICA
2018. The conference provided an
interdisciplinary forum for researchers,
professional engineers and scientists,
educators, and technologists to discuss,
debate and promote research and technology
in the emerging areas of computing,
information, communication and their
applications. The book discusses these
research areas, providing a valuable resource
for researchers and practicing engineers**

alike.

The 12th International Conference on Information and Communication Systems (ICICS 2021) is a forum for scientists, engineers, and practitioners to present their latest research results, ideas, developments, and applications in all areas of Computer and Information Sciences The topics that will be covered in the ICICS 2021 include, but are not limited to Artificial Intelligence, Mobile Computing, Networking, Information Security and Cryptography, Intrusion Detection and Computer Forensics, Web Content Mining, Bioinformatics and IT Applications, Database Technology, Systems Integration, Information Systems Analysis and Specification, Communications, and Human Computer Interaction

This book covers diverse aspects of advanced computer and communication engineering, focusing specifically on industrial and manufacturing theory and applications of electronics, communications, computing and information technology. Experts in research, industry, and academia present the latest developments in technology, describe applications involving cutting-edge communication and computer systems, and explore likely future trends. In addition, a

wealth of new algorithms that assist in solving computer and communication engineering problems are presented. The book is based on presentations given at ICOCOE 2015, the 2nd International Conference on Communication and Computer Engineering. It will appeal to a wide range of professionals in the field, including telecommunication engineers, computer engineers and scientists, researchers, academics and students. Foundations and Practice of Security Identity Theft: Breakthroughs in Research and Practice 2019 2nd International Conference on New Trends in Computing Sciences (ICTCS) Emerging Organizational, Ethical, and Human Issues Methods and Solutions Phishing and Countermeasures 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)

1 Deep Learning and Recognition Computing 2 Brain like Computing and Brain like Intelligent 3 Network and Graph Analysis 4 Big Data and Information Security 5 Wearable Electronics and Health & Leisure 6 Micro Nano sensor and BioMEMS 7 Multi core Processor and Reconfigurable Computing 8 Cryptographic Algorithm

and Security Management 9 IC Design and System Integration 10 EMC Theory and RFID Techniques This book presents best selected research papers presented at the First International Conference on Integrated Intelligence Enable Networks and Computing (IIENC 2020), held from May 25 to May 27, 2020, at the Institute of Technology, Gopeshwar, India (Government Institute of Uttarakhand Government and affiliated to Uttarakhand Technical University). The book includes papers in the field of intelligent computing. The book covers the areas of machine learning and robotics, signal processing and Internet of things, big data and renewable energy sources.

"This book provides a thorough understanding of issues and concerns in information technology security"--Provided by publisher.

ISDFS provides a platform for researchers and experts in academia, industry and government to exchange ideas and recent developments in digital forensics and security After several successful events, the sixth ISDFS conference will continue to promote and disseminate knowledge concerning several topics and technologies related to Digital Forensics and Security Special sessions, workshops, tutorials, keynotes, panel discussions, poster and oral presentations will be included in the symposium program Topics within the scope of the symposium include, but are not limited to, the following areas Digital Forensics Data Privacy Cryptography Information Security IIENC 2020 Advances in Electronics, Communication and Computing

2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC)

2018 6th International Symposium on Digital Forensic and Security (ISDFS)

2019 International Conference on Intelligent Computing and Its Emerging Applications (ICEA)

Principle, Algorithms, and Practices

2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)

This book constitutes the refereed proceedings of the Fourth VLDB 2007 International Workshop on Secure Data Management, SDM 2007, held in Vienna, Austria, September 23-24, 2007 in conjunction with VLDB 2007. The 11 revised full papers presented were carefully reviewed and selected from 29 submissions. The papers are organized in topical sections on Access Control, Database Security, Privacy Protection and Positon Papers.

This book is a compilation of research work in the interdisciplinary areas of electronics, communication, and computing. This book is specifically targeted at students, research scholars and academicians. The book covers the different approaches and techniques for specific applications, such as particle-swarm optimization, Otsu's function and harmony search optimization algorithm, triple gate silicon on insulator (SOI)MOSFET, micro-Raman and Fourier Transform Infrared Spectroscopy (FTIR) analysis, high-k dielectric gate oxide, spectrum sensing in cognitive radio, microstrip antenna, Ground-penetrating radar (GPR) with

conducting surfaces, and digital image forgery detection. The contents of the book will be useful to academic and professional researchers alike.

Phishing is one of the most widely-perpetrated forms of cyber attack, used to gather sensitive information such as credit card numbers, bank account numbers, and user logins and passwords, as well as other information entered via a web site. The authors of A Machine-Learning Approach to Phishing Detetion and Defense have conducted research to demonstrate how a machine learning algorithm can be used as an effective and efficient tool in detecting phishing websites and designating them as information security threats. This methodology can prove useful to a wide variety of businesses and organizations who are seeking solutions to this long-standing threat. A Machine-Learning Approach to Phishing Detetion and Defense also provides information security researchers with a starting point for leveraging the machine algorithm approach as a solution to other information security threats. Discover novel research into the uses of machine-learning principles and algorithms to detect and prevent phishing attacks Help your business or organization avoid costly damage from phishing sources Gain insight into machine-learning strategies for facing a variety of information security threats

A Beginner's Guide to Internet of Things Security focuses on security issues and developments in the Internet of Things (IoT) environment. The wide-ranging applications of IoT, including home appliances, transportation, logistics, healthcare, and smart cities,

necessitate security applications that can be applied to every domain with minimal cost. IoT contains three layers: application layer, middleware layer, and perception layer. The security problems of each layer are analyzed separately to identify solutions, along with the integration and scalability issues with the cross-layer architecture of IoT. The book discusses the state-of-the-art authentication-based security schemes, which can secure radio frequency identification (RFID) tags, along with some security models that are used to verify whether an authentication scheme is secure against any potential security risks. It also looks at existing authentication schemes and security models with their strengths and weaknesses. The book uses statistical and analytical data and explains its impact on the IoT field, as well as an extensive literature survey focusing on trust and privacy problems. The open challenges and future research direction discussed in this book will help to further academic researchers and industry professionals in the domain of security. Dr. Brij B. Gupta is an assistant professor in the Department of Computer Engineering, National Institute of Technology, Kurukshetra, India. Ms. Aakanksha Tewari is a PhD Scholar in the Department of Computer Engineering, National Institute of Technology, Kurukshetra, India.

17th European Symposium on Research in Computer Security, Pisa, Italy, September 10-12, 2012, Proceedings

Algorithms and Architectures for Parallel Processing, Part II

Handbook of Research on Computational Forensics,

Digital Crime, and Investigation: Methods and Solutions
Distributed Denial of Service (DDoS) Attacks
2021 International Conference on Advance Computing
and Innovative Technologies in Engineering (ICACITE)
4th International Conference, CNSA 2011, Chennai,
India, July 15-17, 2011, Proceedings
2021 International Conference on Communication,
Control and Information Sciences : Proceedings : 16-18
June 2021, Government Engineering College Idukki,
Kerala, India

*This two volume set LNCS 7016 and LNCS 7017
constitutes the refereed proceedings of the 11th
International Conference on Algorithms and Architectures
for Parallel Processing, ICA3PP 2011, held in
Melbourne, Australia, in October 2011. The second
volume includes 37 papers from one symposium and three
workshops held together with ICA3PP 2011 main
conference. These are 16 papers from the 2011
International Symposium on Advances of Distributed
Computing and Networking (ADCN 2011), 10 papers of
the 4th IEEE International Workshop on Internet and
Distributed Computing Systems (IDCS 2011), 7 papers
belonging to the III International Workshop on Multicore
and Multithreaded Architectures and Algorithms (M2A2
2011), as well as 4 papers of the 1st IEEE International
Workshop on Parallel Architectures for Bioinformatics
Systems (HardBio 2011).*
*This conference gives scope to researchers, academicians,
students, industrialist etc This conference focuses on main*

new technologies such as AI, Big data, robotics, energy management, power system, power electronics, renewable energy, wireless communication, control system, robotics, machine learning, deep learning etc This conference will provide an knowledge exposure to the participants by listening to the well renowned speakers at national and international level

The aim of ITNEC 2020 is to provide a platform for researchers, engineers, academicians as well as industrial professionals from all over the world to present their research results and development activities in Information Technology, Networking,Electronic and Automation Control It provides opportunities for the delegates to exchange new ideas and application experiences, to establish business or research relations and to find global partners for future collaboration

This book constitutes the carefully refereed and revised selected papers of the 4th Canada-France MITACS Workshop on Foundations and Practice of Security, FPS 2011, held in Paris, France, in May 2011. The book contains a revised version of 10 full papers, accompanied by 3 keynote addresses, 2 short papers, and 5 ongoing research reports. The papers were carefully reviewed and selected from 30 submissions. The topics covered are pervasive security and threshold cryptography; encryption, cryptanalysis and automatic verification; and formal methods in network security.

Emerging Research in Computing, Information, Communication and Applications

ETAEERE-2016

Proceedings of ICOCOE 2015

Computational Science and Technology

Proceedings of Integrated Intelligence Enable Networks and Computing

A Beginner's Guide to Internet of Things Security

2nd International Conference on Advancements of Computing (ICAC 2020) provides a forum for academics, researchers and practitioners with an interest in advancements of all areas related to computing including Computer Engineering, Computer Science, Information Systems, Information Technology and Software Engineering

While Computer Security is a broader term which incorporates technologies, protocols, standards and policies to ensure the security of the computing systems including the computer hardware, software and the information stored in it, Cyber Security is a specific, growing field to protect computer networks (offline and online) from unauthorized access, botnets, phishing scams, etc. Machine learning is a branch of Computer Science which enables computing machines to adopt new behaviors on the basis of observable and verifiable data and information. It can be applied to ensure the security of the computers and the information by detecting anomalies using data mining and other such techniques. This book will be an invaluable resource to understand the importance of machine learning and data mining in establishing computer and cyber security. It emphasizes important

security aspects associated with computer and cyber security along with the analysis of machine learning and data mining based solutions. The book also highlights the future research domains in which these solutions can be applied. Furthermore, it caters to the needs of IT professionals, researchers, faculty members, scientists, graduate students, research scholars and software developers who seek to carry out research and develop combating solutions in the area of cyber security using machine learning based approaches. It is an extensive source of information for the readers belonging to the field of Computer Science and Engineering, and Cyber Security professionals. Key Features: This book contains examples and illustrations to demonstrate the principles, algorithms, challenges and applications of machine learning and data mining for computer and cyber security. It showcases important security aspects and current trends in the field. It provides an insight of the future research directions in the field. Contents of this book help to prepare the students for exercising better defense in terms of understanding the motivation of the attackers and how to deal with and mitigate the situation using machine learning based approaches in better manner. This book constitutes the refereed proceedings of the 17th European Symposium on Computer Security, ESORICS 2012, held in Pisa, Italy, in September 2012. The 50 papers included in the book were carefully reviewed and selected from 248 papers. The articles are organized in topical sections on security and data protection in real systems; formal models for

cryptography and access control; security and privacy in mobile and wireless networks; counteracting man-in-the-middle attacks; network security; users privacy and anonymity; location privacy; voting protocols and anonymous communication; private computation in cloud systems; formal security models; identity based encryption and group signature; authentication; encryption key and password security; malware and phishing; and software security.

An essential anti-phishing desk reference for anyone with anemail address Phishing Dark Waters addresses the growing and continuingscourge of phishing emails, and provides actionable defensivetechniques and tools to help you steer clear of malicious emails.Phishing is analyzed from the viewpoint of human decision-makingand the impact of deliberate influence and manipulation on therecipient. With expert guidance, this book provides insight intothe financial, corporate espionage, nation state, and identitytheft goals of the attackers, and teaches you how to spot a spoofede-mail or cloned website. Included are detailed examples of highprofile breaches at Target, RSA, Coca Cola, and the AP, as well asan examination of sample scams including the Nigerian 419,financial themes, and post high-profile event attacks. Learn how toprotect yourself and your organization using anti-phishing tools,and how to create your own phish to use as part of a securityawareness program. Phishing is a social engineering technique through email thatdeceives users into taking an action that is not in their bestinterest, but usually with the goal of disclosing

information orinstalling malware on the victim's computer. Phishing DarkWaters explains the phishing process and techniques, and thedefenses available to keep scammers at bay. Learn what a phish is, and the deceptive ways they've beenused Understand decision-making, and the sneaky ways phishers reelyou in Recognize different types of phish, and know what to do whenyou catch one Use phishing as part of your security awareness program forheightened protection Attempts to deal with the growing number of phishing incidentsinclude legislation, user training, public awareness, and technicalsecurity, but phishing still exploits the natural way humansrespond to certain situations. Phishing Dark Waters is anindispensible guide to recognizing and blocking the phish, keepingyou, your organization, and your finances safe.
ERCICA 2018, Volume 1
The Death of the Internet
2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)
Computer Security -- ESORICS 2012
2019 5th International Conference on Advanced Computing and Communication Systems (ICACCS)
Classification, Attacks, Challenges and Countermeasures
Advances in Network Security and Applications
Phishing and Counter-Measures discusses how and why phishing is a threat, and presents effective countermeasures. Showing you how phishing attacks have been mounting over the years, how to detect and prevent current as well as future attacks, this text focuses on corporations who supply the resources used by

attackers. The authors subsequently deliberate on what action the government can take to respond to this situation and compare adequate versus inadequate countermeasures.

The ICEE 2020 aims at promoting research in the field of electrical engineering in its theoretical, experimental and applied aspects The conference will bring together researchers, engineers and scientists in this field of engineering

2020 International Conference on Advanced Computing & Communication Systems (ICACCS) aims at exploring the interface between the industry and real time environment with state of the art techniques ICACCS 2020 publishes original and timely research papers and survey articles in current areas of sustainable computing, energy, smart city, temperature, power and environment related research areas of current importance to readers

2020 3rd International Conference on Advancements in Computational Sciences (ICACS).2019 2nd International Conference on New Trends in Computing Sciences (ICTCS) Towards a Wireless Connected World: Achievements and New Technologies

4th Canada-France MITACS Workshop, FPS 2011, Paris, France, May 12-13, 2011, Revised Selected Papers
2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)
2020 15th Conference on Computer Science and Information Systems (FedCSIS)
Secure Data Management
2019 IEEE 13th International Conference on Anti Counterfeiting, Security, and Identification (ASID)
Techniques and Applications for Advanced Information Privacy and Security: Emerging Organizational, Ethical, and Human

Issues

This book constitutes the proceedings of the 4th International Conference on Network Security and Applications held in Chennai, India, in July 2011. The 63 revised full papers presented were carefully reviewed and selected from numerous submissions. The papers address all technical and practical aspects of security and its applications for wired and wireless networks and are organized in topical sections on network security and applications, ad hoc, sensor and ubiquitous computing, as well as peer-to-peer networks and trust management.

Developing an effective and efficient artificial intelligent method for enhancing the performance of an intelligent system has been a critical issue today Besides developing more useful supervised unsupervised learning algorithms to enhance the performance of an intelligent system, how to adopt cloud computing and GPU technologies to accelerate the performance of such systems has attracted the attention of researchers from different disciplines Several emerging intelligent applications can also be found in data mining, network security, smart city, and many applications in our daily life The ICEA 2019 provides an open platform for researchers from different countries to exchange their research

results, experiences, and opinions in the topics on intelligent computing and other relevant emerging applications This conference features all recent advances in an integral concept that highlights the trends in search algorithms, systems, and applications in intelligent computing

Fraud poses a significant threat to the Internet. 1.5% of all online advertisements attempt to spread malware. This lowers the willingness to view or handle advertisements, which will severely affect the structure of the web and its viability. It may also destabilize online commerce. In addition, the Internet is increasingly becoming a weapon for political targets by malicious organizations and governments. This book will examine these and related topics, such as smart phone based web security. This book describes the basic threats to the Internet (loss of trust, loss of advertising revenue, loss of security) and how they are related. It also discusses the primary countermeasures and how to implement them. This book gathers the proceedings of the Sixth International Conference on Computational Science and Technology 2019 (ICCST2019), held in Kota Kinabalu, Malaysia, on 29–30 August 2019. The respective contributions offer practitioners and researchers a range of new

computational techniques and solutions, identify emerging issues, and outline future research directions, while also showing them how to apply the latest large-scale, high-performance computational methods.

2020 3rd International Conference on Advancements in Computational Sciences (ICACS).

A Machine-Learning Approach to Phishing Detection and Defense

ICCISc 2021

2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)

Information Systems Security

6th ICCST 2019, Kota Kinabalu, Malaysia, 29-30 August 2019

Phishing Dark Waters

The complexity and severity of the Distributed Denial of Service (DDoS) attacks are increasing day-by-day. The Internet has a highly inconsistent structure in terms of resource distribution. Numerous technical solutions are available, but those involving economic aspects have not been given much consideration. The book, DDoS Attacks – Classification, Attacks, Challenges, and Countermeasures, provides an overview of both types of defensive solutions proposed so

far, exploring different dimensions that would mitigate the DDoS effectively and show the implications associated with them. Features: Covers topics that describe taxonomies of the DDoS attacks in detail, recent trends and classification of defensive mechanisms on the basis of deployment location, the types of defensive action, and the solutions offering economic incentives. Introduces chapters discussing the various types of DDoS attack associated with different layers of security, an attacker's motivations, and the importance of incentives and liabilities in any defensive solution. Illustrates the role of fair resource-allocation schemes, separate payment mechanisms for attackers and legitimate users, negotiation models on cost and types of resources, and risk assessments and transfer mechanisms. DDoS Attacks – Classification, Attacks, Challenges, and Countermeasures is designed for the readers who have an interest in the cybersecurity domain, including students and researchers who are exploring different dimensions associated with the DDoS attack, developers and security professionals who are focusing on developing defensive schemes and applications for detecting or mitigating the DDoS attacks, and faculty members across different universities.

IEEE CCWC 2021 which will provide an opportunity for researchers, educators and students to discuss and exchange ideas on issues, trends, and developments in Computing and Communication The conference aims to bring together scholars from different disciplinary backgrounds to emphasize dissemination of ongoing research in the fields of in Computing and Communication Contributed papers are solicited describing original works in the above mentioned fields and related technologies

"This book provides a media for advancing research and the development of theory and practice of digital crime prevention and forensics, embracing a broad range of digital crime and forensics disciplines"--Provided by publisher.

2019 International Conference on Advanced Computing & Communication Systems (ICACCS 2019) aims at exploring the interface between the industry and real time environment with state of the art techniques ICACCS 2019 publishes original and timely research papers and survey articles in current areas of energy, smart city, temperature, power and environment related research areas of current importance to readers

Breakthroughs in Research and Practice
2020 International Conference on Electrical
Engineering (ICEE)
Machine Learning for Computer and Cyber
Security
2020 2nd International Conference on
Advancements in Computing (ICAC)
The Offensive and Defensive Sides of
Malicious Emails
The conference will cover a broad area
of electrical and electronic
engineering, computer science and
engineering, biomedical engineering,
industrial management It is targeted on
results of research carried out by
young researchers (Master and PhD
students, engineers)