Wireless Personal Communications
https://doi.org/10.1007/s11277-021-08585-y

Analysing the User Actions and Location for Identifying Online Scam in Internet Banking on Cloud

Arokia Jesu Prabhu Lazar[1] · Sudhakar Sengan[2] · Luigi Pio Leonardo Cavaliere[3] · Thillaiarasu Nadesan[4] · Deepesh Sharma[5] · Mukesh Kumar Gupta[6] · Thangam Palaniswamy[7] · Mahendiran Vellingiri[7] · Dilip Kumar Sharma[8] · Thirukumaran Subramani[9]

Accepted: 4 May 2021

Abstract
Although money laundering does seem to be a new problem, the financial crisis generally occurs during an economic recession compared with standard economic development periods. Due to user fraud transactions and tolerance, they encountered numerous issues, particularly with internet banking fraud. Modernization and an enormous impact on online shopping have caused a significant increase in card payments (like credit, debit) worldwide. Increased acceptance and affordability of i-Banking services for online ordering have benefited customers personally, but it has also increased hackers' number. Fraud entails a significant financial level of risk that can adversely affect an economic entity's profit margins and image. In-fractions of a second, the system is capable of Online Transaction Fraud Detection. This method recommends an unchecked method for dynamically profiling a customer's behavioral patterns. This method's importance is that secure authentication credentials are not exposed to banks and cloud authorization servers but enable them to authenticate their remote access. The received transactions are then evaluated by comparing to the customer ID to identify abnormalities, upon which the appropriate warnings are output. This paper aims to provide such a high-level outline of how new technologies can enhance fraud observation within a publicly or privately economic unit.

Keywords User fraud detection · i-Banking · K-mean algorithm · Data security and privacy · Public cloud

1 Introduction

Because of the fast growth in online transactions, and use of internet banking (i-banking) has risen dramatically. As the online i-Banking sector is the most highly regarded mode of online payment and shopping, fraud seems to increase. Phishing, Pharming, Skimming, and Dumpster drive are several ways cash can be derived from the credit/debit card.

✉ Sudhakar Sengan
sudhasengan@gmail.com

Extended author information available on the last page of the article

Published online: 15 May 2021

Soft Computing (2021) 25:12343–12356
https://doi.org/10.1007/s00500-021-05928-6

FOCUS

Securing data in transit using data-in-transit defender architecture for cloud communication

Keerthana Nandakumar[1] · Viji Vinod[2] · Syed Musthafa Akbar Batcha[3] · Dilip Kumar Sharma[4] · Mohanraj Elangovan[5] · Anjana Poonia[6] · Suresh Mudlappa Basavaraju[7] · Sanwta Ram Dogiwal[8] · Pankaj Dadheech[9] · Sudhakar Sengan[10]

Accepted: 31 May 2021 / Published online: 10 June 2021

Abstract
The advent of cloud infrastructure in which third-party cloud services may retain sensitive consumer and company data in storage environments underlines the need to advocate for encryption and multi-tenant shared processing as a primary security mechanism. Digital information movement, storage, and processing are widely defined in terms of "Data in Motion," "Data at Rest," and "Data in Usage," respectively. The implementation of security methods for each of these states can be viewed similarly. Transit data applies to data when being moved from one source of data to another. Transit data contains data sent across the network from back-end clients, programs, and repositories. There could be two data centers inside the same organizational network in the cloud, as a member of completely separate networks. This paper presents a novel architecture data-in-transit defender (DiTD), to protect data in transit; DiTD provides a novel security framework based on high-performance cloud computing. This protocol enables more efficient use of the key strength and time of symmetric block encrypted data, public-key cryptography (PUKC), cryptographic hash, and brief key exchange function.

Keywords Data in transit · Cloud security · Encryption · Ciphertext · Cloud service

1 Introduction

Over the past decades, the world's Web has undergone an unprecedented increase in hackers, malware, ransom wares, and other harmful bugs or groups who are actively attempting to find a way to access user data. This state goes without saying that security has become one of the most critical activities that can be addressed, irrespective of the position we usually perform (Adrian et al. 2015). The general necessity to avoid unauthorized access to confidential, private/otherwise vital details is something every end-users, database operators, system managers, and so on can acknowledge: The disagreements are primarily linked to what we ought to secure and how we can do it.

The process of deciding the best route to secure our data always includes a well-conducted risk analysis supported by a cost–benefit analysis, which is an effective model for the order to assist us in identifying the appropriate technological and operational measures to be followed in our given scenario (Aviram et al. 2016). The control system or processor must use adequate processes and technologies to maintain a minimum level of security to minimize the costs, taking into account communications systems, the cost of implementation and design, the scope, description, and objective, the threat of varying probability and the impact on human freedoms and privileges.

As the name suggests, in-transit data can be treated just like a medium of transmission: A perfect illustration of in-transit data is a standard Web page that we receive from the internet while we browse the internet. In a nutshell, this is what happens under the hood (Flavel et al. 2015):

1. We submit a request for HTTP (or HTTPS) to the server, which runs the Web site we use.
2. The Web server acknowledges our request, processes it by identifying the (static/dynamic) information that we have requested, and then sends it to us as an HTTP (or HTTPS) address over a specific TCP port (usually 80 for HTTP and 443 for HTTPS).

Communicated by Vicente Garcia Diaz.

Extended author information available on the last page of the article

Arabian Journal for Science and Engineering
https://doi.org/10.1007/s13369-021-05936-6

RESEARCH ARTICLE - SPECIAL ISSUE - FRONTIERS IN PARALLEL PROGRAMMING MODELS FOR FOG AND EDGE COMPUTING INFRASTRUCTURES

Utilizing Index-Based Periodic High Utility Mining to Study Frequent Itemsets

Roy Setiawan[1] · Dac-Nhuong Le[2] · Regin Rajan[3] · Thirukumaran Subramani[4] · Dilip Kumar Sharma[5] · Vidya Sagar Ponnam[6] · Kailash Kumar[7] · Syed Musthafa Akbar Batcha[8] · Pankaj Dadheech[9] · Sudhakar Sengan[10]

Received: 8 May 2021 / Accepted: 28 June 2021

Abstract
The potential employability in different applications has garnered more significance for Periodic High-Utility Itemset Mining (PHUIM). It is to be noted that the conventional utility mining algorithms focus on an itemset's utility value rather than that of its periodicity in the transaction. A MEAN periodicity measure is added to the minimum (MIN) and maximum (MAX) periodicity to incorporate the periodicity feature into PHUIM in this proposed work. The MEAN-periodicity measure brings a new dimension to the periodicity factor and is arrived at by dividing itemset's period value by the total number of transactions in that dataset. Further, an algorithm to mine Index-Based Periodic High Utility Itemset Mining (IBPHUIM) from the database using an indexing approach is also proposed in this paper. The proposed IBPHUIM algorithm employs a projection-based technique and indexing procedure to increase memory and execution speed efficiency. The proposed model avoids redundant database scans by generating sub-databases using an indexing data structure. The proposed IBPHUIM model has experimented with test datasets, and the results drawn show that the proposed IBPHUIM model performs considerably better.

Keywords IBPHUIM · Periodic pattern · Frequent periodic pattern

✉ Sudhakar Sengan
sudhasengan@gmail.com

Roy Setiawan
roy@petra.ac.id

Dac-Nhuong Le
ledacnhuong@duytan.edu.vn

Regin Rajan
regin12006@yahoo.co.in

Thirukumaran Subramani
thirukumaran75@kluniversity.in

Dilip Kumar Sharma
dilipsharmajiet@gmail.com

Vidya Sagar Ponnam
pvsagar20@gmail.com

Kailash Kumar
k.kumar@seu.edu.sa

Syed Musthafa Akbar Batcha
syedmusthafait@gmail.com

Pankaj Dadheech
pankajdadheech777@gmail.com

1 Department Management, Universitas Kristen Petra, Jawa Timur, Indonesia

2 School of Computer Science/Institute of Research and Development, Duy Tan University, Danang 550000, Vietnam

3 Department of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, Tamil Nadu 635109, India

4 Department of Computer Science and Engineering, KL University, Vijayawada, Andhra Pradesh 522502, India

5 Jaypee University of Engineering and Technology, Guna, Madhya Pradesh 473226, India

6 Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh 522502, India

7 College of Computing and Informatics, Saudi Electronic University, Riyadh 11673, Kingdom of Saudi Arabia

8 Department of Information Technology, M. Kumarasamy College of Engineering, Karur, Tamil Nadu 639113, India

9 Department of Computer Science and Engineering, Swami Keshvanand Institute of Technology, Management and Gramothan (SKIT), Jaipur, Rajasthan 302017, India

10 Department of Computer Science and Engineering, PSN College of Engineering and Technology, Tirunelveli, Tamil Nadu 627152, India

Published online: 14 July 2021

Arabian Journal for Science and Engineering
https://doi.org/10.1007/s13369-021-05620-9

RESEARCH ARTICLE - SPECIAL ISSUE - FRONTIERS IN PARALLEL PROGRAMMING MODELS FOR FOG AND EDGE COMPUTING INFRASTRUCTURES

A Multi-Stakeholder Involved Effective E-Waste Management in Manufacturing Recycled Electronic Products Using Game Theory

Sudhakar Sengan[1] · Kanmani Palaniappan[2] · Nirmala Devi Kathamuthu[3] · Rashid Amin[4] · Rajesh Babu Mariappan[5] · Nik Alif Amri Nik Hashim[6] · Eni Noreni Mohamad Zain[7] · Pankaj Dadheech[8]

Received: 21 September 2020 / Accepted: 24 March 2021

Abstract
Globally, electronic waste (E-Waste) has grown as a severe concern owing to the increasing quantity of waste and the toxic it. E-Waste includes plastics and metals, which are highly recyclable but which, if not adequately managed, are concerned about the health and the environment by plastic waste and heavy metal traces of additives and chemicals. This article investigates the modeling of game theory for E-Waste. It presents a framework to analyze various stakeholders' behavior in the manufacture of electronic products using recycled (ERM) and non-recycled (ENRM) materials, understanding the importance of the actual cost variation. This study suggested a framework to decide which Game Plan is best-suited to gain each stakeholder's leading company's profit allocation. Data demonstrate that ERM can be the best choice for manufacturers and customers and recommend applying return schemes to consumers with specific incentives and penalties to those who do not comply with the agreed E-Waste management process could be of great help to discourage computer waste disposal on land.

Keywords E-Waste management · Game theory · Multi-stakeholder · Recycle · Nash equilibrium game plan

✉ Sudhakar Sengan
sudhasengan@gmail.com

✉ Kanmani Palaniappan
pkanmaniit@gmail.com

Nirmala Devi Kathamuthu
k_nirmal.cse@kongu.edu

Rashid Amin
rashid4nw@gmail.com

Rajesh Babu Mariappan
drmrajeshbabu@gmail.com

Nik Alif Amri Nik Hashim
nikalifamri@gmail.com

Eni Noreni Mohamad Zain
noreni@umk.edu.my

Pankaj Dadheech
pankajdadheech777@gmail.com

1 Department of Computer Science and Engineering, PSN College of Engineering and Technology, Tirunelveli, Tamil Nadu 627152, India

2 Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Tamil Nadu 603203, India

3 Department of Computer Science and Engineering, Kongu Engineering College, Perundurai, Tamil Nadu 638060, India

4 Department of Computer Science, University of Engineering and Technology, Taxila, Pakistan

5 Department of Computer Science and Engineering, RVS College of Engineering and Technology, Coimbatore, Tamil Nadu 641402, India

6 Faculty of Hospitality, Tourism and Wellness, Universiti Malaysia Kelantan, Kelantan, Malaysia

7 Faculty of Entrepreneurship and Business, Universiti Malaysia Kelantan, Kelantan, Malaysia

8 Department of Computer Science and Engineering, Swami Keshvanand Institute of Technology, Management and Gramothan (SKIT), Jaipur, Rajasthan 302017, India

Published online: 12 April 2021

Office of the Controller General of Patents, Designs & Trade Marks
Department of Industrial Policy & Promotion,
Ministry of Commerce & Industry,
Government of India

(http://ipindia.nic.in/index.htm)

INTELLECTUAL PROPERTY INDIA
PATENTS | DESIGNS | TRADE MARKS | GEOGRAPHICAL INDICATIONS
(http://ipindia.nic.in/index.htm)

Application Details

APPLICATION NUMBER	202141006550
APPLICATION TYPE	ORDINARY APPLICATION
DATE OF FILING	17/02/2021
APPLICANT NAME	**1 . Dr.L.K.Rex** **2 . Dr.V.S.Sethuraman** **3 . Mr.Akash Johari** **4 . Mr.Pankaj Gupta** **5 . Mr.Akshay.K.Uday** **6 . Dr.D.S.Vijayan** **7 . Mr.D.Antony Prabu** **8 . Dr.G.Vijayakumar** **9 . Dr.V.Manikandan** **10 . Dr.S.Sudhakar**
TITLE OF INVENTION	UTILIZATION OF BURR WASTES AS MICRO-REINFORCEMENTS IN CONCRETE TO OVERCOME DISPOSAL OF HAZARDOUS MATERIALS IN GLOBAL ENVIRONMENT
FIELD OF INVENTION	CHEMICAL
E-MAIL (As Per Record)	lkrphd1@gmail.com
ADDITIONAL-EMAIL (As Per Record)	
E-MAIL (UPDATED Online)	
PRIORITY DATE	
REQUEST FOR EXAMINATION DATE	--
PUBLICATION DATE (U/S 11A)	26/02/2021

Application Status

APPLICATION STATUS	**Awaiting Request for Examination**

View Documents

➡ Filed ➡ Published ➡ RQ Filed ➡ Under Examination ➡ Disposed

(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :17/02/2021

(21) Application No.202141006550 A
(43) Publication Date : 26/02/2021

(54) Title of the invention : UTILIZATION OF BURR WASTES AS MICRO-REINFORCEMENTS IN CONCRETE TO OVERCOME DISPOSAL OF HAZARDOUS MATERIALS IN GLOBAL ENVIRONMENT

(51) International classification	:C04B0014020000, C04B0018140000, C08L0023020000, B28B0023020000, D07B0005000000
(31) Priority Document No	:NA
(32) Priority Date	:NA
(33) Name of priority country	:NA
(86) International Application No	:NA
Filing Date	:NA
(87) International Publication No	: NA
(61) Patent of Addition to Application Number	:NA
Filing Date	:NA
(62) Divisional to Application Number	:NA
Filing Date	:NA

(71)**Name of Applicant :**
1)Dr.L.K.Rex
Address of Applicant :30/34, Annai Theresa Street, Kamaraj Nagar Extn, Gorimedu Puducherry-605006, India Tamil Nadu India
2)Dr.V.S.Sethuraman
3)Mr.Akash Johari
4)Mr.Pankaj Gupta
5)Mr.Akshay.K.Uday
6)Dr.D.S.Vijayan
7)Mr.D.Antony Prabu
8)Dr.G.Vijayakumar
9)Dr.V.Manikandan
10)Dr.S.Sudhakar
(72)**Name of Inventor :**
1)Dr.L.K.Rex
2)Dr.V.S.Sethuraman
3)Mr.Akash Johari
4)Mr.Pankaj Gupta
5)Mr.Akshay.K.Uday
6)Dr.D.S.Vijayan
7)Mr.D.Antony Prabu
8)Dr.G.Vijayakumar
9)Dr.V.Manikandan
10)Dr.S.Sudhakar

(57) Abstract :
Concrete is the basic engineering material used in most civil constructions. It is extremely used because of the ability to possess high compressive strength and be molded into any desired shape. In order to overcome the poor tensile strength of concrete, fibers are introduced in the matrix. In this idea, burr wastes obtained from the CNC turning process in the lathe industry were disposed of as wastes in open lands in the industries' proximity, causing a hazard to the environment. Hence, these wastes were tested as fiber material in the form of micro-reinforcements in the concrete. Burr wastes were added to the concrete in volume fractions Vf=0%, 0.5%, 1.0%, 1.5% and 2.0% and tested for its compressive, split tensile and flexural strength. The experimental test results revealed that the compressive and flexural strength of burr waste concrete increased from 16.16% to 23.36% and 117% to 124%, respectively, for Vf = 0.5% to 2.0% at 28 days strength in comparison with concrete made without burr waste. The tensile strength of burr waste concrete increased up to 6.06% for Vf = 0.5% at 28 days strength when compared to conventional concrete. The experimental investigation observed that the addition of burr wastes as micro reinforcements in the concrete had significant improvement in concrete strength.

No. of Pages : 16 No. of Claims : 5