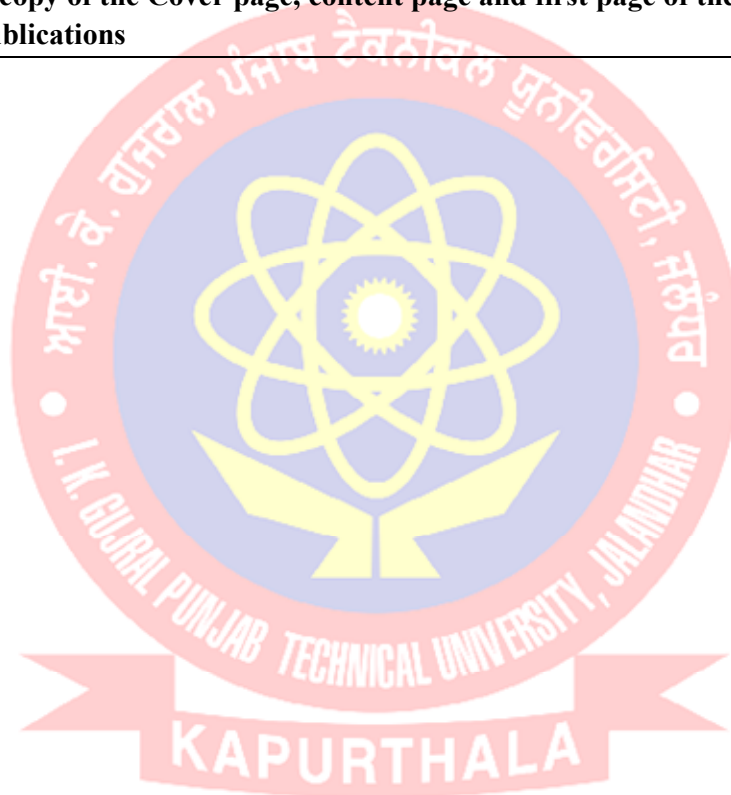


Department: Computer Science & Engineering

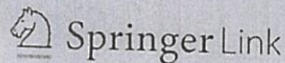
3.4.6

Books and Chapters published in edited volumes

Sl. No.	Documents Attached
1.	E-copy of the Cover page, content page and first page of the publications



E-copy of the Cover page, content page and first page of the publications



Fog Computing in IOT: An Overview of New Opportunities

Proceedings of ICETIT 2019 pp 59-68 | Cite as

- Ketanpreet Kaur (1) Email author (ketanpreet.kaur@gmail.com) View author's OrcID profile (View OrcID profile)
- Monika Sachdeva (2) View author's OrcID profile (View OrcID profile)

1. GNA University, , Phagwara, India
2. I.K. Gujral Punjab Technical University, , Kapurthala, India

Conference paper

First Online: 24 September 2019

- 937 Downloads

Part of the Lecture Notes in Electrical Engineering book series (LNEE, volume 605)

Abstract

With the emergence of the Internet of Things (IoT) millions of devices and sensors are connected to each other producing a huge amount of data. To analyze and compute the data, it is sent to the cloud but because of latency, bandwidth and storage problem we need some computing paradigm near to edge devices. Fog computing is an extended version of cloud computing which extend some of its services to the end user level. The emerging rate of mobile traffic needs mobility and wide geographical distribution which is fulfilled by Fog Computing. In this paper, we will discuss how Fog computing is providing different services to the users which were lacking in cloud paradigm. We will be discussing the main features of Fog computing and how it is solving challenges faced by the IoT paradigm.

Keywords

Fog computing Sensors Internet of Things (IoT) Cloud computing
This is a preview of subscription content, [log in](#) to check access.

References

1. Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. Comput. Netw. 54, 2787–2805 (2010)
[CrossRef](https://doi.org/10.1016/j.comnet.2010.05.010) (https://doi.org/10.1016/j.comnet.2010.05.010)
[Google Scholar](http://scholar.google.com/scholar_lookup?title=The%20internet%20of%20things%3A%20a%20survey&author=L.%20Atzori) (http://scholar.google.com/scholar_lookup?title=The%20internet%20of%20things%3A%20a%20survey&author=L.%20Atzori)

HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

Detection and Prevention of DDoS Attacks in Wireless Sensor Networks

Networking Communication and Data Knowledge Engineering pp 3-13 | Cite as

- Shivam Dhuria (1) Email author (sdlhuria13@gmail.com)
- Monika Sachdeva (2)

1. CSE, SBSSTC, , Ferozepur, India
2. CSE, IKGPTU, , Kapurthala, India

Conference paper

First Online: 14 November 2017

- 638 Downloads

Part of the Lecture Notes on Data Engineering and Communications Technologies book series (LNDECT, volume 3)

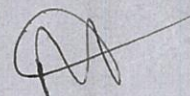
Abstract

Wireless Sensor Networks are emerging at a great pace due to their cost effective solutions for the sensitive and remote applications like military, medical and environmental applications (Chatterjee and Pandey in Int J Sci Eng Res 5, 2014) [1]. But due to limited range, memory, processing and power supply, gathering of important remote data from wireless sensors is really challenging. The use of ad hoc network and radio waves for data transmission has also increased the chance for attackers to attack on such networks. Various schemes have been proposed in the past to fight against the attacks in WSN (Sahu and Pandey in Mod Educ Comput Sci 1:65–71, 2014) [2], (Paul et al. in Wireless Sensor Network Security: A Survey. Auerbach Publications, Florida, 2006) [3]. In this paper two methods have been introduced, one is light weight two way authentication method that will prevent majority of attacks in WSN and other is traffic analysis based data filtering method that will detect and prevent DDoS attacks in WSN. The results have been verified using the Network Simulator 2 (NS2) on several performance metrics i.e. throughput, delay, lost packets, energy consumption and PDR.

Keywords

Data filtration Authentication Network performance Simulator Data rate
Sensor Data packets Data traffic Base station Node
This is a preview of subscription content, [log in](#) to check access.

References



HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

Detection of Selective Forwarding (Gray Hole) Attack on LEACH in Wireless Sensor Networks

Next-Generation Networks pp 389-398 | Cite as

- Priya Chawla (1) Email author (piyachawla12@gmail.com)
- Monika Sachdeva (1)

1. Department of Computer Science and Engineering, Shaheed Bhagat Singh State Technical Campus, , Ferozepur, India

Conference paper

First Online: 21 November 2017

- 819 Downloads

Part of the Advances in Intelligent Systems and Computing book series (AISC, volume 638)

Abstract

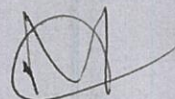
Wireless sensor networks (WSN) are mainly deployed in an unattended and hostile environment. So security is a major concern in these types of networks. Many routing protocols have been designed in WSN, which are responsible for maintaining the routes in the network. We mainly focused on LEACH, the most popular hierarchical routing protocol. But the services of LEACH are threatened by various kinds of attacks such as Black Hole, Selective Forwarding (Gray Hole), Sybil, and HELLO flood attacks. In this paper, firstly we have discussed LEACH and then how it can be compromised by Selective Forwarding Attack. The performance of LEACH without the existence of attack and with the attack has been evaluated in terms of various performance metrics such as packet delivery ratio, packet loss, and remaining energy of the network using Network Simulator (NS-2). We have also emphasized on how to secure the network if they have been threatened to Selective Forwarding Attack. To detect the malicious nodes in the network, we have proposed and implemented a detection strategy.

Keywords

Wireless sensor networks LEACH NS-2

This is a preview of subscription content, [log in](#) to check access.

Notes



HOD

Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

Detection of Hello Flood Attack on LEACH in Wireless Sensor Networks

Next-Generation Networks pp 377-387 | Cite as

- Reenkamal Kaur Gill (1) Email author (reenkamalgill@gmail.com)
- Monika Sachdeva (1)

1. Department of Computer Science and Engineering, Shaheed Bhagat Singh State Technical Campus, , Ferozepur, India

Conference paper

First Online: 21 November 2017

- 870 Downloads

Part of the Advances in Intelligent Systems and Computing book series (AISC, volume 638)

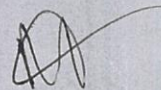
Abstract

Wireless sensor networks are newer technology consisting of sensor nodes deployed in an unattended environment which collect environmental data by sensing and then forward it to the base station. The security of WSN in such an environment is very difficult. There are many routing protocols for WSN, but LEACH is the widely used energy proficient hierarchical routing protocol which saves nodes energy by forming clusters. In LEACH, cluster member forwards its data to the cluster head, which then aggregate and forward the entire data it received from member nodes to the base station. There are various types of attacks which threaten the services of LEACH are Sybil attack, black hole, selective forwarding, and Hello flooding attack. Hello flooding attack is a type of DoS attack which degrades the performance of LEACH by continuously sending large number of cluster head advertisement packets. Inside this text, firstly, we have discussed LEACH routing protocol and how it can be compromised by Hello flooding attackers. Once we threaten the services of LEACH by Hello flood attack, the impact of attacks on the performance metrics of LEACH is evaluated. In this paper, we have also proposed a detection strategy using coordinator nodes which detect the nodes causing Hello flood attack and then prevent it. The performance of algorithm is then tested using the NS-2 simulator.

Keywords

Wireless sensor networks LEACH Hello flood NS-2
This is a preview of subscription content, [log in](#) to check access.

Notes



HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

Energy Conscious Packet Transmission in Wireless Networks Using Trust Based Mechanism: A Cognitive Approach

Anshu Bhasin^(1,*), Sandeep Singh, and Anshul Kalia

IKG Punjab Technical University, Kapurthala, India
Dr. anshubhasin@ptu.ac.in, Sandeep_madda@yahoo.co.in,
Anshul17215@ptuniversity.in

Abstract. The self-motivated nature of wireless ad-hoc networks deters the possibility of a centralized solution. Also, no specific node can act as a centralized point due to energy and processing constraints. Constraint of non-centralization demands efficient and effective transmission of data between nodes by sharing information whenever needed without any disruption. This co-operation is a prodigious challenge due to the presence of covetous and malicious nodes in the network. Hence, an asserted need of some lightweight trust based mechanism in differentiating among reliable and unreliable nodes arises. This mechanism enhances security and improve co-operation in nodes. Energy efficiency remains central to the above segregation. Many trust-based methods are proposed which use packet delivered ratio as the major parameter for direct trust calculation. This work presents investigation of other related parameters like routing overhead, energy level etc. which can increase the effectiveness of trust based mechanisms for early detection of malicious nodes along with packet delivered ratio. Furthermore, an ameliorated energy optimization model is proposed for wireless network.

Keywords: Wireless ad-hoc networks · Routing · Attacks · Energy · MANET

1 Introduction

Wireless systems are extensively in use for communication nowadays. Wireless systems have various characteristics like scalability, dynamic topology, low cost, easy setup, mobility, high user density, multi hop wireless transmission and convenience [1]. In ad hoc setup, nodes can move in or move out from the network at any time, causing the topology to change quickly and unpredictably. Each node in the ad hoc setup has to work as a transmitter and a receiver. All nodes are in authority to create, operate and maintain the ad hoc network. Wireless systems can be categorized into two types - the infrastructure based wireless networks and the infrastructure-less wireless networks (ad hoc networks).

MANET is an interconnected system of wireless networks that can be designed quickly and dynamically without requiring any additional external router or access point [2]. MANET is also sometimes referred as Self-Organizing Networks (SONs) [3].

Anshu Bhasin, Ankita Sharma

Understanding and implementation of machine learning using support vector machine for efficient DDoS attack detection

Abstract: Excessive communication over the Internet in the present era has made our privacy vulnerable. With zoomed technology and engineering, it has in turn given wider opportunity to the attackers to penetrate the network just like that of normal users. When attacker's purpose is to make any specific server or network fail to normal services, it is called network denial-of-service (DoS) attack. Further, distributed DoS (DDoS) attacks are launched through Zombies, which are compromised machines. Recently, for attack detection strategies, most of the researchers and organizations are opting for machine learning (ML) techniques, as these are cost-efficient than humans, when it is about analyzing a huge amount of data. ML in cybersecurity holds the potential to handle areas of prediction, detection, and continuous monitoring. This chapter explores detailed contemporary research and presents meliorated detection mechanism for DDoS attack, based on one-class support vector machine (OC-SVM), an efficient ML technique. More specifically, it focuses on identification of high relevance feature extraction that can exploit the classification capability of OC-SVM for attack detection. The proposed technique includes supervised learning, using NSL-KDD dataset and works adroitly for DDoS attack detection. The empirical results on accuracy and detection rate are compared with other existing methods. False alarm rate and training speed are recorded to project the efficacy of the proposed system.

Keyword: cybersecurity, DDoS attacks, machine learning, one-class support vector machine (OC-SVM)

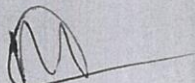
1 Introduction

Computer network technology has new-fangled through Internet in the present era. Organizational and personal daily activities such as e-commerce, email, social networking, online transactions include billions of users per second to depend heavily on computer network. This excessive dependence on the Internet leads to underlying security issues toward our activities and make privacy vulnerable. Centre for Deliberate and

Anshu Bhasin, Department of CSE, Main Campus, IKG Punjab Technical University, Kapurthala, Punjab, India, e-mail: dr.anshubhasin@ptu.ac.in

Ankita Sharma, Department of CSE, Lovely Professional University, Phagwara, Punjab, India, e-mail: ankitabs12sharma@gmail.com

<https://doi.org/10.1515/9783110619751-002>



HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

Handbook of Research on Advanced Concepts in Real-Time Image and Video Processing

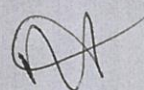
Md. Imtiyaz Anwar
National Institute of Technology, Jalandhar, India

Arun Khosla
National Institute of Technology, Jalandhar, India

Rajiv Kapoor
Delhi Technological University, India

A volume in the Advances in Multimedia and
Interactive Technologies (AMIT) Book Series

IGI Global
DISSEMINATOR OF KNOWLEDGE



HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

Published in the United States of America by
IGI Global
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: <http://www.igi-global.com>

Copyright © 2018 by IGI Global. All rights reserved. No part of this publication may be reproduced, stored or distributed in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher. Product or company names used in this set are for identification purposes only. Inclusion of the names of the products or companies does not indicate a claim of ownership by IGI Global of the trademark or registered trademark.
Library of Congress Cataloging-in-Publication Data

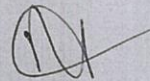
Names: Anwar, Md. Imtiyaz, 1982- editor. | Khosla, Arun, 1967- editor. | Kapoor, Rajiv, editor.
Title: Handbook of research on advanced concepts in real-time image and video processing / Md. Imtiyaz Anwar, Arun Khosla, and Rajiv Kapoor, editors.
Other titles: Advanced concepts in real-time image and video processing
Description: Hershey, PA : Information Science Reference, [2018] | Series: Information science reference
Identifiers: LCCN 2017012029 | ISBN 9781522528487 (hardcover) | ISBN 9781522528494 (ebook)
Subjects: LCSH: Video recording. | Image processing--Digital techniques. | Real-time data processing. | Digital video--Editing.
Classification: LCC TR850 .A26 2018 | DDC 777--dc23 LC record available at <https://lcn.loc.gov/2017012029>

This book is published in the IGI Global book series Advances in Multimedia and Interactive Technologies (AMIT) (ISSN: 2327-929X; eISSN: 2327-9303)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

For electronic access to this publication, please contact: eresources@igi-global.com.



HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

Chapter 14

Radial Moments for Image Retrieval

Pooja Sharma
DAV University, India

ABSTRACT

Images have always been considered an effective medium for presenting visual data in numerous applications ranging from industry to academia. Consequently, managing and indexing of images become essential in order to retrieve relevant images effectively and efficiently. Therefore, the proposed chapter aims to elaborate one of the advanced concepts of image processing, i.e., Content Based Image Retrieval (CBIR) and image feature extraction using advanced methods known as radial moments. In this chapter, various radial moments are discussed with their properties. Besides, performance measures and various similarity measures are elaborated in depth. The performance of radial moments is evaluated through an extensive set of experiments on benchmark databases such as Kimia-99, MPEG-7, COIL-100, etc.

INTRODUCTION

Images have always been considered an effective medium for presenting visual data in numerous applications ranging from industry to academia. With the development in technology, a large amount of images are being generated everyday. Therefore, managing and indexing of images become essential in order to retrieve relevant images effectively and efficiently. Early work on image retrieval can be traced back to 1970s. In 1979, a conference was held regarding database techniques for pictorial applications (Blaser, 1979). Since then, the research pertaining to image database management has influenced several researchers (Chang and Fu, 1979; Chang and Fu, 1980; Chang and Kunii, 1981; Chang et al., 1988). In traditional systems, textual annotations of images were used to describe images. Afterwards, the images were searched using text based approach from traditional database management system such as SQL query. A comprehensive survey of text based retrieval can be found in (Chang and Hsu, 1988; Chang et al. 1988). In text based image retrieval, images are organized by semantic hierarchies to facilitate navigation and browsing using standard keyword queries. However, the textual annotation of images is a cumbersome task, which requires intensive manual labor for large image databases. Apart from that,

DOI: 10.4018/978-1-5225-2848-7.ch014

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.



HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

Handbook of Research on Advanced Concepts in Real-Time Image and Video Processing

Md. Imtiyaz Anwar

National Institute of Technology, Jalandhar, India

Arun Khosla

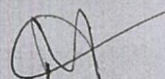
National Institute of Technology, Jalandhar, India

Rajiv Kapoor

Delhi Technological University, India

A volume in the Advances in Multimedia and
Interactive Technologies (AMIT) Book Series

IGI Global
DISSEMINATOR OF KNOWLEDGE



HOD

Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

Published in the United States of America by
IGI Global
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: <http://www.igi-global.com>

Copyright © 2018 by IGI Global. All rights reserved. No part of this publication may be reproduced, stored or distributed in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher. Product or company names used in this set are for identification purposes only. Inclusion of the names of the products or companies does not indicate a claim of ownership by IGI Global of the trademark or registered trademark.
Library of Congress Cataloging-in-Publication Data

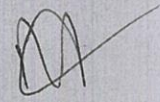
Names: Anwar, Md. Imtiyaz, 1982- editor. | Khosla, Arun, 1967- editor. | Kapoor, Rajiv, editor.
Title: Handbook of research on advanced concepts in real-time image and video processing / Md. Imtiyaz Anwar, Arun Khosla, and Rajiv Kapoor, editors.
Other titles: Advanced concepts in real-time image and video processing
Description: Hershey, PA : Information Science Reference, [2018] | Series: Information science reference
Identifiers: LCCN 2017012029 | ISBN 9781522528487 (hardcover) | ISBN 9781522528494 (ebook)
Subjects: LCSH: Video recording. | Image processing--Digital techniques. | Real-time data processing. | Digital video--Editing.
Classification: LCC TR850 .A26 2018 | DDC 777--dc23 LC record available at <https://lcn.loc.gov/2017012029>

This book is published in the IGI Global book series Advances in Multimedia and Interactive Technologies (AMIT) (ISSN: 2327-929X; eISSN: 2327-9303)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

For electronic access to this publication, please contact: eresources@igi-global.com.


HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

Chapter 17

Recognition of Face Biometrics

Pooja Sharma
DAV University, India

ABSTRACT

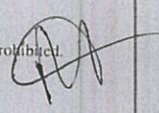
In the proposed chapter, a novel, effective, and efficient approach to face recognition is presented. It is a fusion of both global and local features of images, which significantly achieves higher recognition. Initially, the global features of images are determined using polar cosine transforms (PCTs), which exhibit very less computation complexity as compared to other global feature extractors. For local features, the rotation invariant local ternary patterns are used rather than using the existing ones, which help improving the recognition rate and are in alignment with the rotation invariant property of PCTs. The fusion of both acquired global and local features is performed by mapping their features into a common domain. Finally, the proposed hybrid approach provides a robust feature set for face recognition. The experiments are performed on benchmark face databases, representing various expressions of facial images. The results of extensive set of experiments reveal the supremacy of the proposed method over other approaches in terms of efficiency and recognition results.

INTRODUCTION

Biometric is a recently emerged and vastly increasing technology, which has numerous applications in forensics, surveillance and security. Primarily, biometric system identifies and recognizes human biological features such as fingerprints, iris, hand geometry, and face recognition. The human face considers to be a dynamic object exhibiting high erraticism due to its appearance and expressions. Moreover, face recognition is a challenging area in real time applications. Among other biometrics, face based recognition has advantages in terms of uniqueness. To describe the facial images acquired using camera or other sources various descriptors are available. An image descriptor can be region based/dense or contour based/discrete. A region based descriptor computes features on all the pixels of the image, while contour based descriptor computes on a subset of image pixels. The region based descriptors can be termed as global descriptors because these descriptors extract features by considering the entire image as a whole and represent the global characteristics of the image.

DOI: 10.4018/978-1-5225-2848-7.ch017

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.


HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

Programming in Python

Dr. Pooja Sharma

Assistant Professor
Department of Computer Application
I.K Gujral Punjab Technical University (Main Campus)
Kapurthala, Punjab



BPB PUBLICATIONS

HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

FIRST EDITION 2017

Copyright © BPB Publications, INDIA

ISBN : 978-93-8655-127-6

All Rights Reserved. No part of this publication can be stored in a retrieval system or reproduced in any form or by any means without the prior written permission of the publishers.

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The Author and Publisher of this book have tried their best to ensure that the programmes, procedures and functions described in the book are correct. However, the author and the publishers make no warranty of any kind, expressed or implied, with regard to these programmes or the documentation contained in the book. The author and publisher shall not be liable in any event of any damages, incidental or consequential, in connection with, or arising out of the furnishing, performance or use of these programmes, procedures and functions. Product name mentioned are used for identification purposes only and may be trademarks of their respective companies.

All trademarks referred to in the book are acknowledged as properties of their respective owners.

Distributors:

BPB PUBLICATIONS
20, Ansari Road, Darya
Ganj New Delhi-110002
Ph: 23254990/23254991

BPB BOOK CENTRE
376 Old Lajpat Rai
Market, Delhi-110006
Ph: 23861747

COMPUTER BOOK CENTRE
12, Shrungar Shopping Centre,
M.G.Road, Bengaluru -560001
Ph: 25587923/25584641

DECCAN AGENCIES
4-3-329, Bank Street,
Hyderabad-500195
Ph: 24756967/24756400

MICRO MEDIA
Shop No. 5, Mahendra Chambers, 150
DN Rd. Next to Capital Cinema, V.T.
(C.S.T.) Station, MUMBAI-400 001
Ph: 22078296/22078297

Published by Manish Jain for BPB Publications, 20, Ansari Road, Darya Ganj
New Delhi- 110002 and Printed him at Repro India Pvt. Ltd, Mumbai

HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

Effective image retrieval using polar cosine transform and local binary patterns

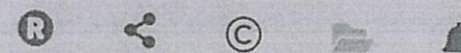
Publisher: IEEE

Cite This

PDF

Pooja All Authors

71
Full
Text Views



Abstract

Document Sections

- I. Introduction
- II. Feature Extraction
- III. Similarity Measure
- IV. Experimental Study and Performance Analysis

Abstract:

In this paper, we present a novel, effective, and efficient approach to image retrieval. Basically, it is a fusion of both global and local features of images, which achieves significantly higher retrieval competency. Initially, the global features of images are determined using polar cosine transforms (PCTs). For local features, we use rotation invariant local binary patterns (RLBP) rather than using the existing ones, which help in improving the retrieval rate and are in alignment with the rotation invariant property of PCTs. The combination of both acquired global and local features is performed by mapping their features into a common domain. Finally, the proposed hybrid approach provides a robust feature set for image retrieval. Detailed experiments are performed on various sorts of image databases. The results of extensive set of experiments reveal the supremacy of the proposed approach over other approaches in terms of efficiency and retrieval results.

HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

Cryptanalysis of Protocol for Enhanced Threshold Proxy Signature Scheme Based on Elliptic Curve Cryptography for Known Signers

Raman Kumar

Abstract The proxy signature is the elucidation to the entrustment of signing capabilities in any secure electronic milieu. Numerous schemes are prophesied, but they are chattels of information security. In this, I anticipate an enhanced secure threshold proxy signature scheme based on elliptic curve cryptography. I compare the performance of scheme(s) with the performance of a scheme has been anticipated by the writer of this article formerly. I investigate enhanced threshold proxy signature scheme for diverse parameters like entropy, floating frequencies/intuitive synthesis, ASCII histogram, autocorrelation, histogram analysis and vitany. Consequently, the enhanced threshold proxy signature scheme based on elliptic curve cryptography is safe and effective against infamous conspiracy attack(s).

Keywords Proxy signature • Unforgeability • Secret sharing • Time constraint Elliptic curve cryptography • Non-repudiation and threshold scheme for known signers

1 Introduction

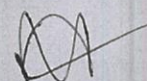
Nowadays Internet is close part of our life. The data going transversely via Internet may be unsafe. There are a lot of examples for its illustrations. When I discuss ATM PIN, SSN, or some other secluded information, it becomes a complete diverse story. So, security engineering plays vital role for this.

Nowadays commercial milieu, creating a framework for the validation between notions and arenas, is quite difficult. Elliptic curve cryptography is one of the most powerful but slightest understood types of cryptography. An increasing number of Web sites evolve extensive usage of elliptic curve cryptography to protect all as of customer's HTTPS acquaintances to know how they pass data among data centers.

R. Kumar (✉)
Department of Computer Science and Engineering, I. K. Gujral
Punjab Technical University, Kapurthala, Punjab, India
e-mail: er.ramankumar@aol.in; dr.ramankumar@ptu.ac.in

© Springer Nature Singapore Pte Ltd. 2018
S. Margret Anouncia and U. K. Wail (eds.), *Knowledge Computing and Its Applications*, https://doi.org/10.1007/978-981-10-6680-1_10

191



HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

Design and Analysis of an Enhanced Multifactor Authentication Through a Covert Approach



Raman Kumar and Uffe Kock Wiil

Abstract Most of the network service providers currently use two-factor authentication for their wireless networks. This exposes the network subscribers to identify theft and user's data to security threats like snooping, sniffing, spoofing and phishing. There is need to control these problems with the use of an enhanced multi factor authentication approach. The objective of this work is to create a multi-factor authentication software for a wireless network. Multi factor authentication involves user's knowledge factor, user's possession factor and user's inherence factor; that is who the user is to be presented before system access can be granted. Multi factor authentication depends mainly on three factors: (1) Something a user knows, such as a password or PIN (2) Something a user has, such as a key, a card, or another kind of token (3) Something a user is, such as a retina scan, or fingerprint. We may enhance the reliability and security of the authentication mechanism by combining multiple authentication factors into a single model. Multi factor authentication is far better if we use this schema both statically and dynamically. The three factors together provide a much higher confidence in the all prerequisite parameters of cryptography.

Keywords Multifactor authentication · One factor · Two factor · Authentication and authorization

R. Kumar (✉)

Department of Computer Science and Engineering, I K Gujral Punjab Technical University,
Kapurthala, Punjab, India
e-mail: er.ramankumar@aol.in; dr.ramankumar@ptu.ac.in

U. K. Wiil

The Maersk Mc-Kinney Moller Institute, University of Southern Denmark, Odense, Denmark
e-mail: ukwiil@mmmi.sdu.dk

© Springer Nature Switzerland AG 2019

R. Kumar and U. K. Wiil (eds.), *Recent Advances in Computational Intelligence*,
Studies in Computational Intelligence 823,
https://doi.org/10.1007/978-3-030-12500-4_3

er.ramankumar@aol.in

HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

Review on Current Trends of Deep Learning



Stuti Mehla, Anjali Chaudhary and Raman Kumar

Abstract Artificial Intelligence is that term which take Science to new horizons. In field of computers, AI is described as where machine acts like human. AI has different fields on the basis of problem i.e. machine learning, natural language processing, computer vision and robotics. To achieve these objectives several approaches are in trend like Symbolic Reasoning, Neural Network, Deep Learning and Evolutionary Algorithms. Out of these, Neural Network and Deep learning are those approaches which attracts the researchers. Both are inspired by biological neural network but Deep learning is more refined neural network in which feature extraction and abstraction is automatic as compared to Neural Network. In this chapter we will emphasise on AI technologies and then focus on recent researches in field of Deep Learning i.e. Sentiment Analysis, WSN etc.

Keywords AI · Symbolic reasoning · RNN · Sentiment analysis · WSN

1 Introduction

According to Smitther Artificial Intelligence is that field of computer science where intelligent behavior is created artificially. AI focuses on to make such machines which act intelligent as human mind do. Basic aim of AI is to make cognitive machines which can find solutions of problem solving tasks, logical reasoning and can do

S. Mehla (✉)

Maharishi Markandeshwar Deemed University, Mullana, Ambala, India
e-mail: stuti21mehla@gmail.com

A. Chaudhary

Panipat Institute of Engineering and Technology, Panipat, Haryana, India
e-mail: anjali.dhankar@gmail.com

R. Kumar

Department of Computer Science and Engineering, I K Gujral Punjab
Technical University, Kapurthala, Punjab, India
e-mail: er.ramankumar@aol.in; dr.ramankumar@ptu.ac.in

© Springer Nature Switzerland AG 2019

R. Kumar and U. K. Wiil (eds.), *Recent Advances in Computational Intelligence*,
Studies in Computational Intelligence 823,
https://doi.org/10.1007/978-3-030-12500-4_4

63

er.ramankumar@aol.in

HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

Hybrid Homomorphic Encryption Scheme for Secure Cloud Data Storage



Bijeta Seth, Surjeet Dalal and Raman Kumar

Abstract Cloud computing is the budding paradigm nowadays in the macrocosm of the information processing system. It offers a variety of services for the users through the Internet and is highly cost-efficient and flexible. Information storage in the cloud is showing great attention. Yet, despite all its advantages, security and privacy has evolved to be of significant apprehension in cloud computing and is discouraging factor for potential adopters. Consumers and businesses prefer online computing only if their data are guaranteed to remain secret and safe. Hence, the focal point is to discover techniques in the direction of offering more confidentiality. Homomorphic encryption is one such technique. This paper targets to study several key concepts of cloud computing, namely characteristics, delivery models, deployment models and cloud computing platforms. The theme includes the security challenges/issues and their associated work in cloud computing. A generic flow of data and the operations to be performed in the proposed scheme for multi-clouds are presented. The report explains the details and effects related to different parameters of Homomorphic properties of some cryptosystems. In this paper, our main work is to ensure the protection of information, thus we offered a method to amend the Paillier Homomorphic algorithm without compromising the protection of existing technique. In our prospect work, we plan to propose an efficient Multicloud architecture so that information is stored, maintained and retrieved efficiently by employing a modified Paillier approach.

Keywords Cloud computing · Security · Issues · Attacks · Homomorphic encryption · RSA · ElGamal · Paillier · Encryption · Decryption · Entropy

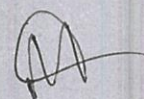
B. Seth (✉) · S. Dalal
SRM University, Sonepat, Haryana, India
e-mail: bijetaoberoi@gmail.com

S. Dalal
e-mail: profsurjeetdalal@gmail.com

R. Kumar
Department of Computer Science and Engineering,
I K Gujral Punjab Technical University, Kapurthala, Punjab, India
e-mail: er.ramankumar@aol.in; dr.ramankumar@ptu.ac.in

© Springer Nature Switzerland AG 2019
R. Kumar and U. K. Wiil (eds.), *Recent Advances in Computational Intelligence*,
Studies in Computational Intelligence 823,
https://doi.org/10.1007/978-3-030-12500-4_5

er.ramankumar@aol.in


HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

A Gamification Framework for Redesigning the Learning Environment



Rishipal, Sweta Saraff and Raman Kumar

Abstract In the modern education system, one of the major concerns today is maintaining students' interest in the school curriculum. With the growing popularity of gamification in various fields, it can serve as a useful pedagogical tool for the educators to make the learning environment more stimulating and immersive. There is a need for a succinct and coherent framework of gamification. Though gamification cannot be a panacea for all maladies, our focus is on crafting a research based and carefully designed model, so that we can utilize it to its maximum potential.

Play is innate to not only humans but also animals. In any "Play", the primary reinforcement is the fun element or enjoyment. There is a freedom of choice, a sense of autonomy as game selection depends on the player's interest, personality and level of difficulty. This empowerment is one of the basic premises on which the concept of "Play" lies on. "Play is not an optional leisure activity, but a biological imperative that supports our cognitive and emotional well-being, occupying an important role in our development as humans" [1]. Often players are so engrossed in games that they enjoy the challenges, simply to achieve the desired targets and collect badges. Sometimes the game is so immersive that they become emotionally charged. The players sometime develop a feeling of affiliation and sentimental attachment to the co-gaming peer group.

A game is more structured than a play with clearly identified rules and goals. Players engage in conflicts or challenges, even in a single user game they try to boost their last scores. Learning is usually not considered fun or entertaining, therefore "It is much more challenging to keep the students motivated to engage in studies," [2]. It is difficult to keep learners motivated in the process of acquiring a new skill or

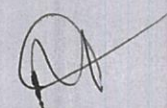
Rishipal (✉) · S. Saraff
AIBAS Amity University, Gurgaon, Haryana, India
e-mail: rishipal_anand@rediffmail.com

R. Kumar
Department of Computer Science and Engineering,
I K Gujral Punjab Technical University, Kapurthala, Punjab, India
e-mail: dr.ramankumar@ptu.ac.in; er.ramankumar@aol.in

© Springer Nature Switzerland AG 2019
R. Kumar and U. K. Wil (eds.), *Recent Advances in Computational Intelligence*,
Studies in Computational Intelligence 823,
https://doi.org/10.1007/978-3-030-12500-4_6

93

er.ramankumar@aol.in


HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

A Variant of Secret Sharing Protected with Poly-1305



Shakti Arora, Surjeet Dalal and Raman Kumar

Abstract We are working in the era of cloud computing, where all of the required resources are available online at pay-par-basis. It made all the IT industry easily accessible to all types of users. It provides the services in software, hardware and in storage terms. We are dealing the model of IAAS which provides on demand secured storage services. A number of researchers has designed and proposed a number of techniques and algorithms for assurance of storage services provided by cloud service providers. Our paper presents a modified approach of integrity verification in multiparty communication in decentralized cloud computing environment. We enhanced the basic model of AES with AES Poly Library 1305 and also redesigned the variant of secret sharing scheme for handling a secured group communication. Our factors for evaluation are the hardness and randomness of key i.e. entropy of the proposed technique and other measurable units which gives the efficiency of communication overhead and security.

Keywords Entropy · CPU cycles · Poly-1305 · Encryption · Decryption

1 Introduction

A new revolution and advancements in field of hardware, software, virtual machines, and middleware or in can say revolutionary advancements in IT technology has led to an emergence of wide global distributed platform. Now a days cloud computing

S. Arora (✉) · S. Dalal
SRM University, Sonepat, Haryana, India
e-mail: shakti.nagpal@gmail.com

S. Dalal
e-mail: profsurjeetdalal@gmail.com

R. Kumar
Department of Computer Science and Engineering, I K Gujral Punjab
Technical University, Kapurthala, Punjab, India
e-mail: er.ramankumar@aol.in; dr.ramankumar@ptu.ac.in

© Springer Nature Switzerland AG 2019
R. Kumar and U. K. Wiil (eds.), *Recent Advances in Computational Intelligence*,
Studies in Computational Intelligence 823,
https://doi.org/10.1007/978-3-030-12500-4_7

107

er.ramankumar@aol.in

HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

Securing Bioinformatics Cloud for Big Data: Budding Buzzword or a Glance of the Future



Bijeta Seth, Surjeet Dalal and Raman Kumar

Abstract Insight to utilize the Big data of Bioinformatics information generated by a paradigm; Cloud Computing is coming up as a guarantee to deal with big information storage and scrutiny challenges in the Bioinformatics field. Cloud computing is viewed to be a cost effectual technique to process and accumulate this immense quantity of data with parallel processing tools and carried as "Services" through the internet. Due to its fast and efficient performance for data processing on cloud clusters and easy to use environments, The Hadoop parallel programming framework is dominantly used. This document will be bearing in the direction of the productive course for economical Bioinformatics clouds for the Big data and also the challenges that would obstruct Bioinformatics Big data to take a stride towards the cloud. In this document, we state an outline of the applications of Bioinformatics clouds, merits, and limitations of the current research activity methods used for storing Big Data in Bioinformatics. The paper mentions how the existing dilemma can be addressed from the perspective of Cloud computing services in addition to Bioinformatics tools. For ensuring trust, a simulation comparing the trust values for different Cloud providers is being illustrated in Fog server. For Future enhancements, efforts are being made to build up an efficient cloud data storage system employing different Bioinformatics tools ensuring security so that various Healthcare organizations are benefited by this approach.

Keywords Big data • Bioinformatics • Cloud computing • Secure cloud • Bioinformatics cloud tools • MapReduce • Fog

B. Seth (✉) • S. Dalal
SRM University, Sonapat, Haryana, India
e-mail: bijetaoberoi@gmail.com

S. Dalal
e-mail: profsurjeetdalal@gmail.com

R. Kumar
Department of Computer Science and Engineering, I K Gujral Punjab Technical University,
Kapurthala, Punjab, India
e-mail: er.ramankumar@aol.in; dr.ramankumar@ptu.ac.in

© Springer Nature Switzerland AG 2019

R. Kumar and U. K. Wiil (eds.), *Recent Advances in Computational Intelligence*,
Studies in Computational Intelligence 823,
https://doi.org/10.1007/978-3-030-12500-4_8

121

er.ramankumar@aol.in

HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

Enhancing Gadgets for Blinds Through Scale Invariant Feature Transform



Raman Kumar and Uffe Kock Wiil

Abstract ICT can help blind people in movement and direction-finding tasks. This paper proposes a new methodology for safe mobility based on scale invariant feature transform (SIFT) that is expected to lead to higher precision and accuracy. Various existing gadgets for visually impaired are examined, and the conclusion is that the proposed methodology can enhance these gadgets.

Keywords Scale invariant feature transform · Visually impaired · Partially-sighted and blind people

1 Introduction

One of the biggest recent advances in technology is closely related to the use of mobile technology. The Internet of Things (IoT) era enables plenty of information to be extracted that can be fundamental in decision and recommendation making, such as anticipating citizen problems and providing them with better services [1, 2]. The technological evolution has led to higher processing speeds, which made new applications emerge at a faster pace. Smartphone features, such as navigation, sensing and location-based information, opens a new world of possibilities. Designing devices to people with some kind of visually disability—visually impaired people, partially-sighted people, blind people—(we will use the term PVD—people with some visual disability) is a big challenge and subject to plenty of current and emerging research [3, 4].

R. Kumar (✉)

Department of Computer Science and Engineering, I K Gujral Punjab Technical University,
Kapurthala, Punjab, India
e-mail: er.ramankumar@aol.in; dr.ramankumar@ptu.ac.in

U. K. Wiil

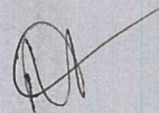
The Maersk Mc-Kinney Moller Institute, University of Southern Denmark, Odense, Denmark
e-mail: ukwiil@mmmi.sdu.dk

© Springer Nature Switzerland AG 2019

R. Kumar and U. K. Wiil (eds.), *Recent Advances in Computational Intelligence*,
Studies in Computational Intelligence 823,
https://doi.org/10.1007/978-3-030-12500-4_9

149

er.ramankumar@aol.in


HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

Design of a Low-Cost Sensor-Based IOT System for Smart Irrigation



Kunal Singh and Raman Kumar

1 Introduction

Water is the most precious resource in agriculture. As agriculture is fundamentally the most important sector of Indian economy, an appropriate measure to control and regulate constant supply of clean water at different intervals of time in a year is our utmost priority. It has been observed [1] through studies that the impact of climate change on the availability of water throughout the year is appreciable and has received much attention from scientific community in recent years. With ever-increasing population of India, the crop requirement would undoubtedly increase every year to feed this growing population, while the resources would remain limited. With the advent of new technologies and emerging sciences combined with recent researches, it is now possible to estimate the optimal resources required for a particular crop production, whether it is moisture, nutrients, or temperature of the field. It may be noted that in this world of competition, emerging technologies in the field of communication, artificial Intelligence, robotics, and actuation have flourished [2] beautifully and proved to be beneficial for the people of India and other developing countries. It is now possible to buy powerful computing devices inexpensively in these countries, and high cost is no longer a factor preventing the implementation of these technologies in smart irrigation systems. It may be noted that some of the Indian scientific communities, under ignorance and lack of

K. Singh (✉)

Mechanical Engineering Department, Maharaja Agrasen University-Baddi, Baddi, Himachal Pradesh, India

R. Kumar

Department of Computer Science and Engineering, I. K. Gujral Punjab Technical University, Kapurthala, Punjab, India

e-mail: er.ramankumar@aol.in; dr.ramankumar@ptu.ac.in

© Springer Nature Switzerland AG 2021

R. Kumar, S. Paiva (eds.), *Applications in Ubiquitous Computing*, EAI/Springer

Innovations in Communication and Computing,

https://doi.org/10.1007/978-3-030-35280-6_4

59

HOD

Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala



PMME 2016

ANALYSIS AND DESIGN OF AN OPTIMIZED SECURE AUDITING PROTOCOL FOR STORING DATA DYNAMICALLY IN CLOUD COMPUTING

Raman Kumar^a and Gurpreet Singh^b

^{a,b}Department of Computer Science and Engineering

^{a,b}D A V Institute of Engineering and Technology, Jalandhar, Punjab

^{a,b}er.ramankumar@aol.in

Abstract

The remote server (Cloud Service Provider (CSP)) store their data on cloud servers and users can access their data from cloud servers while implementing the concept of cloud computing. Because of some security constraints in data outsourcing, the latest concept of data hosting service also arises new security challenges; those challenges can be handled by third party auditing service to check the data integrity in the cloud server. There are few existing remote integrity checking methods those can serve for static stored data but not able to work dynamically. In this paper, we develop three-tier security architecture for storing multimedia files which include role base access control, encryption, and signature verification. Therefore, an enhanced secure dynamic auditing protocol is proposed, which can store data correctly in the cloud. In the proposed scheme, both the combiner and the third party auditor (TPA) can verify the integrity of the information that they are receiving from each other. Therefore, the proposed an optimized secure dynamic auditing protocol is secure and efficient against various conspiracy attacks.

© 2016 Elsevier Ltd. All rights reserved.

Selection and Peer-review under responsibility of International Conference on Processing of Materials, Minerals and Energy (July 29th – 30th) 2016, Ongole, Andhra Pradesh, India.

Keywords: Cloud Computing, Communication overhead, Time cost of individual client, Packet delivery ratio, Energy level, Average delay, Packet delivery time and Throughput

1. Introduction

The cloud computing is a well nourishing paradigm. The NIST definition characterized on important aspects of cloud computing and broad comparisons of cloud computing services and deployment strategies. The service and formation models defined form a simple taxonomy not predetermined to constrain any particular method of implementation, service delivery, or business operation. The hybrid cloud management platform performs some

2214-7853© 2016 Elsevier Ltd. All rights reserved.

Selection and Peer-review under responsibility of International Conference on Processing of Materials, Minerals and Energy (July 29th – 30th) 2016, Ongole, Andhra Pradesh, India.

HOD

Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

Effect of Randomization for Privacy Preservation on Classification Tasks

Reena
Department of CSE
DAVIET, Jalandhar
er_reenatchie@hotmail.com

Raman Kumar
Department of CSE
DAVIET, Jalandhar
er.ramankumar@aol.in

ABSTRACT

Advances in the technology of information processing and storage capacity generated a new term BIG DATA. Due to heterogeneous nature of Big Data there is always a concern with security and privacy. While extracting useful patterns and hidden knowledge from this huge data one question arises when data exposed to several parties how privacy of individual guaranteed and whether application of various privacy preservation techniques produces generate accurate results. Privacy preservation technique prevents a disclosure of sensitive attributes but it may not be at the cost of information loss and quality of data. Different approaches are applied to different type of attributes of data sets for preservation of privacy.

Keywords

Privacy Preserving Techniques, Data mining, Security.

1. INTRODUCTION

The term Data mining simply means extraction of information from the huge volume of data. It follows three main stages: Preprocessing, Data mining algorithms, Evaluate Patterns[19]. Each phase main concern is to protect the sensitive data but not at the cost of utility of data. Application of Privacy preserving Data mining algorithms (PPDM) [12] primary task is to get pertinent information from large datasets while protecting thoughtful information. Real world applications always have information that is sensitive e.g. bank transactions and medical records. Public disclosure of these records can have serious consequences of privacy. Various privacy preserving techniques are available but they have some bottlenecks too.

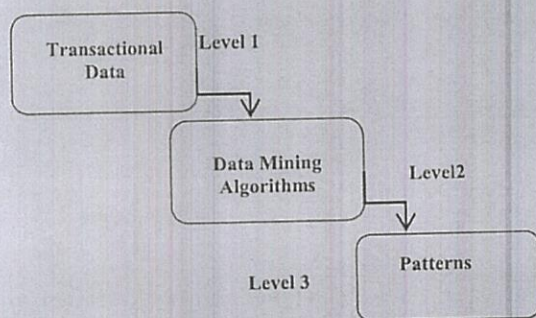


Fig 1.1 PPDM Framework

ICIA-16, August 25-26, 2016, Pondicherry, India
© 2016 ACM. ISBN 978-1-4503-4756-3/16/08...\$15.00
DOI: <http://dx.doi.org/10.1145/2980258.2980345>

Usefulness of the data is reduced when privacy preserving technique applies some kind of transformation on the data. PPDM techniques are also context dependent i.e. certain data values are private or certain classification rules and associations are private. Data mining methods not only discover valuable information but it is vulnerable to misuse. The purpose of this study is to find out what will be the effect of randomization on data mining algorithms and pattern evaluation.

PPDM framework is discussed [10] in which various stages have been explained. Collection of raw data imported from multiple databases, data marts and data transformed into some suitable format which may useful for analytics. Privacy concerns are required also at data collection stage. In second level various processes i.e. blocking, suppression, perturbation, modification, generalization, sampling, anonymization etc. can be applied to sanitize the data[6,14]. The basic advantage of this stage is that after this data can be revealed to untrustworthy data miners. To discover the knowledge from processed data mining algorithms are applied. In the last stage information which is revealed is going to be checked towards risk disclosure.

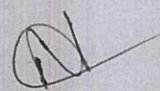
2. PREVIOUS WORK

Jaideep Vaidya, Chris Clifton[1] discussed the possibility of large scale data mining without violating the privacy issues of data. Data perturbation methods and Secure Multiparty computation discussed in essence the various trade-offs among i.e. efficiency, privacy, accuracy and security depending on what kind of approach we have chosen.

Lei Xu, et al [2]discussed growing popularity of data mining technologies is bringing threat to the security of individual's sensitive information and how to protect that sensitive information from individual. They identified various types of users involved in whole data mining process i.e. data provider, data collector, data miner, and decision maker. There are various privacy concerns which relate to every type of user and various methods that can be adopted to protect sensitive information.

A. K. Upadhyay et al[3] mentioned privacy preservation which is one of the major concerns in data mining process. They developed and introduced a novel ICT (inverse cosine based transformation) method to preserve the privacy before sending it to any data mining task analysis. This technique 'privacy preserved k-clustering algorithm' (PrivClust) is developed by embedding K-means clustering algorithm with ICT. While designing this algorithm the most important thing was to preserve privacy with clustering tasks as well. Their analysis showed that this algorithm efficiently preserves the sensitive information with valid cluster results.

Chris Clifton et al [4]focused on the thing that sharing of data can be reason of privacy disclosure and if knowledge discovery can be done in proper manner then we can get rid of this issue. In this paper, they introduced a generalized privacy preserving approach for vertically partitioned data that is distributed over two or more


HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala



Available online at www.sciencedirect.com

ScienceDirect

Energy Procedia 00 (2016) 000–000

Energy

Procedia

www.elsevier.com/locate/procedia

Special Section on: Current Research Topics in Power, Nuclear and Fuel Energy, SP-CRTPNFE 2016, from the International Conference on Recent Trends in Engineering, Science and Technology 2016, 1 June 2016, Hyderabad, India

Comment [S1]: Elsevier to update with volume and page numbers.

Comment [S2]: Elsevier to update with Conference title per issue prior to sharing with authors.

DESIGN AND ANALYSIS OF SECURE ROUTING PROTOCOL FOR MOBILE ADHOC NETWORK

Raman Kumar^a and Manisha Sharma^b

^a*Department of Computer Science and Engineering*

^a*I K Gujral Punjab Technical University, Kapurthala, Punjab, India*

^b*D A V Institute of Engineering and Technology, Jalandhar, Punjab, India*

^a*er.ramankumar@aol.in*

Abstract

With the advancement in the technology, communication becomes a very essential part of the human life and this will result with the new emerging technologies like MANETs where users can communicate with each other but with infrastructure less network. MANETs are the dynamic network where topology can change with respect to time. So, the network topology becomes unstructured and node enters or leaves the network according to their need. As per considered a dynamic network, it is very difficult to maintain routing and transmission processes in this type of networks. Also there is a lack of security in this network because MANETs are vulnerable to various attacks. So, there is a need to overcome these challenges. In this paper, various challenges related to routing and security has been discussed with description of various attacks. The main focus of this paper is to discuss the previous scheme and also their weaknesses which will help to generate new best solutions for the same.

© 2017 The Authors. Published by Elsevier Ltd. Peer-review under responsibility of the organizing committee of SP-CRTPNFE 2016.

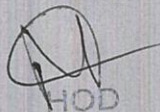
Keywords: MANET (mobile adhoc networks), Security, Routing and Protocols.

Comment [S3]: Elsevier to update with copyright entity, year, copyright company Elsevier Ltd./B.V./Inc. and the conference organizer name.

1. Introduction

The collection of interconnected node is known as network which is classified as wireless and wired. In wireless network the nodes of network are associated by the links which are wireless. The wireless network reduces the costly process of using cabling as compare to wired network so installation process becomes quick and cost effective and it became very easy to connect computer anywhere in home without the use of any wire [36]. During wireless communication the information transferred between two nodes without any electrical equipment. Wireless technologies commonly use radio waves to share information between two devices.

1876-6102 © 2017 The Authors. Published by Elsevier Ltd. Peer-review under responsibility of the organizing committee of [SP-CRTPNFE 2016].


HOD

Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala



Available online at www.sciencedirect.com

ScienceDirect

Energy Procedia 00 (2016) 000–000

Energy

Procedia

www.elsevier.com/locate/procedia

Special Section on: Current Research Topics in Power, Nuclear and Fuel Energy, SP-CRTPNFE 2016, from the International Conference on Recent Trends in Engineering, Science and Technology 2016, 1 June 2016, Hyderabad, India

Comment [S1]: Elsevier to update with volume and page numbers.

Comment [S2]: Elsevier to update with Conference title per issue prior to sharing with authors.

PERFORMANCE ANALYSIS OF SECURE MULTI-SERVER PASSWORD AUTHENTICATED KEY AGREEMENT SCHEME USING DISCRETE LOGARITHM MAPPED ELLIPTIC CURVE CRYPTOGRAPHY

Raman Kumar^a and Sandeep Thakur^b

^{a,b}Department of Computer Science and Engineering

^aI K Gajral Punjab Technical University, Kapurthala, Punjab, India

^bD A V Institute of Engineering and Technology, Jalandhar, Punjab, India

^{a,b}er.ramankumar@aol.in

Abstract

The focus of this paper is to discuss the previous scheme and also their weaknesses which will help to generate new best solutions for the same. In this we used secure multi-server password authenticated key agreement scheme using discrete logarithm mapped elliptic curve cryptography. It provides more security over RSA. Using a smart card together with a user's preferred password, the log-in request message is transmitted securely and the verification can be performed easily. Similarly we have used Discrete Logarithm mapped ECC. In the proposed scheme, both the combiner and the secret share holder can verify the precision of the information that they are receiving from each other. Therefore, the proposed scheme is secure and efficient against notorious conspiracy attacks.

© 2017 The Authors. Published by Elsevier Ltd. Peer-review under responsibility of the organizing committee of SP-CRTPNFE 2016.

Keywords: Security, ECC (Elliptic Curve Cryptography), Discrete Logarithm and Authentication.

Comment [S3]: Elsevier to update with copyright entity, year, copyright company Elsevier Ltd./B.V./Inc. and the conference organizer name.

Introduction

In a network environment, when a user requests a server's service, he must pass examination of user authentication. Through this user authentication process, the server can determine if the user can use the provided services and the exact access rights of this user in these services. When a user uses a service in a server, the transmitted messages between the user and the server must be kept secret. They must negotiate a session key to be used for protecting

1876-6102 © 2017 The Authors. Published by Elsevier Ltd. Peer-review under responsibility of the organizing committee of [SP-CRTPNFE 2016].

HOD
Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

A Literature Survey on various Image Encryption & Steganography Techniques

Madhu Dahiya
Research Scholar

Department of Computer Science and Engineering
I K Gujral Punjab Technical University,
Kapurthala, Punjab, India
madhu.dahiya2588@gmail.com

Raman Kumar

Department of Computer Science and Engineering
I K Gujral Punjab Technical University,
Kapurthala, Punjab, India
er.ramankumar@aol.in

Abstract--In the current world when entire web contains most of multimedia data then protection of that data is our major concern. Different techniques are discovered and developed from time to time to encrypt and decrypt the images for making them more secure. Most of the encryption technique uses secret key to prevent the data from an unauthorized access. In this paper, we study different research papers on various encryption and steganography techniques. Encryption and steganography techniques provides security of images from intruder.

Keywords--- Symmetric key; Asymmetric key; Image Encryption; Image Decryption; Security; Cryptography

I. INTRODUCTION

Network security is an crucial factor in communicating and transferring the data from one public network to another. Steganography & Cryptography are techniques used for network security. Steganography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data. Steganography techniques can be applied to images, a video file or an audio file. Typically, however, steganography is written in characters including hash marking, but its usage within images is also common. At any rate, steganography protects from pirating copyrighted materials as well as aiding in unauthorized viewing.

Cryptography involves creating written or generated codes that allow information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data.

Information security uses cryptography on several levels. The information cannot be read without a key

to decrypt it. The information maintains its integrity during transit and while being stored.

II. CRYPTOGRAPHY

Public Key Encryption: Public key encryption, in which a message is encrypted with a recipient's public key. The message cannot be decrypted by anyone who does not possess the matching private key, who is thus presumed to be the owner of that key and the person associated with the public key. This is used in an attempt to ensure confidentiality.

Private Key Encryption: Here, one single key is used for encryption and second key is used for decryption. Both the senders and receiver share the same key. If the sender encrypts the message by one key then receiver decrypt the message by the same key. Systematic key management or the transfer of key is a major concern while using private key encryption [2].

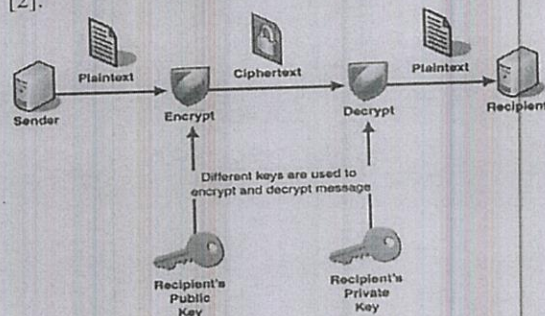


Fig. Working of Cryptography

III. STEGANOGRAPHY

Steganography can be referred as hiding information into another information. That means steganography is an art of hiding one type of data into another type of data. The data which we want to hide is known as hidden data and the data in which the hidden data

[Handwritten Signature]

HOD

Department of Computer Science & Engineering
IKG PTU Main Campus
Kapurthala

Number of books and chapters in edited volumes / books published, and papers in national/international conference

Name of the Teacher	Title of the book/chapters published	Title of the paper	Title of the proceedings of the conference	Name of the conference	National / International	Year of publication	ISBN/ISSN number of the proceeding	Affiliating Institute at the time of publication	Name of the publisher
Reena and Raman Kumar	In ACM Proceedings of the International Conference on Informatics and Analytics (ICIA-16)	Effect of Randomization for Privacy Preservation on Classification Tasks	Effect of Randomization for Privacy Preservation on Classification Tasks	In ACM Proceedings of the International Conference on Informatics and Analytics (ICIA-16)	International	2016	978-1-4503-4756-3	PEC India	ACM
Pooja Sharma		Effective image retrieval using polar cosine transform and local binary patterns	India International Conference on Information Processing	(IICIP), IEEE	International	2016	10.1109/IICIP.2016.7975305	DAV University	IEEE Xplore
Raman Kumar and Karan Verma	3rd International Conference on Electrical, Electronics, Engineering Trends, Communication, Optimization and Sciences (EEECOS–2016)	Analysis and design of scalable and efficient key management using elliptic curve cryptography	Analysis and design of scalable and efficient key management using elliptic curve cryptography	3rd International Conference on Electrical, Electronics, Engineering Trends, Communication, Optimization and Sciences (EEECOS–2016)	International	2016	No info given	SASI Institute of Technology and Engineering, Tadepalligudem, West Godavari District, Andhra Pradesh, India	The Institution of Engineering and Technology, a charity registered in England and Wales (registered number 211014) whose registered office is at Savoy Place, 2 Savoy Place, London WC2R 0BL and whose

Number of books and chapters in edited volumes / books published, and papers in national/international conference

Name of the Teacher	Title of the book/chapters published	Title of the paper	Title of the proceedings of the conference	Name of the conference	National / International	Year of publication	ISBN/ISSN number of the proceeding	Affiliating Institute at the time of publication	Name of the publisher
									office for notices relating to this Agreement is Michael Faraday House, Six Hills Way, Stevenage, Hertfordshire, SG1 2AY
Raman Kumar and Gurpreet Singh	Elsevier Materials Today: Proceedings of Materials, Minerals and Energy: PMME-2016	ANALYSIS AND DESIGN OF AN OPTIMIZED SECURE AUDITING PROTOCOL FOR STORING DATA DYNAMICALLY IN CLOUD COMPUTING	ANALYSIS AND DESIGN OF AN OPTIMIZED SECURE AUDITING PROTOCOL FOR STORING DATA DYNAMICALLY IN CLOUD COMPUTING	Elsevier Materials Today: Proceedings of Materials, Minerals and Energy: PMME-2016	International	2016	No info given	PACE Institute of Technology and Sciences, Ongole, Prakasam, Andhrapradesh, India	Elsevier Materials Today: Proceedings
Reena and Raman Kumar	In ACM Proceedings of the International Conference on Informatics and Analytics (ICIA-16)	Effect of Randomization for Privacy Preservation on Classification Tasks	Effect of Randomization for Privacy Preservation on Classification Tasks	In ACM Proceedings of the International Conference on Informatics and Analytics (ICIA-16)	International	2016	978-1-4503-4756-3	PEC India	ACM

Number of books and chapters in edited volumes / books published, and papers in national/international conference

Name of the Teacher	Title of the book/chapters published	Title of the paper	Title of the proceedings of the conference	Name of the conference	National / International	Year of publication	ISBN/ISSN number of the proceeding	Affiliating Institute at the time of publication	Name of the publisher
Raman Kumar and Sandeep Thakur	International Conference on Recent Trends in Engineering, Science and Technology (ICRTEST), Tamil Nadu, Chennai	PERFORMANCE ANALYSIS OF SECURE MULTI-SERVER PASSWORD AUTHENTICATED KEY AGREEMENT SCHEME USING DISCRETE LOGARITHM MAPPED ELLIPTIC CURVE CRYPTOGRAPHY	PERFORMANCE ANALYSIS OF SECURE MULTI-SERVER PASSWORD AUTHENTICATED KEY AGREEMENT SCHEME USING DISCRETE LOGARITHM MAPPED ELLIPTIC CURVE CRYPTOGRAPHY	International Conference on Recent Trends in Engineering, Science and Technology (ICRTEST), Tamil Nadu, Chennai	International	2016	No info given		Elsevier Energy Procedia
Raman Kumar and Manisha Sharma	International Conference on Recent Trends in Engineering, Science and Technology (ICRTEST), Tamil Nadu, Chennai	DESIGN AND ANALYSIS OF SECURE ROUTING PROTOCOL FOR MOBILE ADHOC NETWORK	DESIGN AND ANALYSIS OF SECURE ROUTING PROTOCOL FOR MOBILE ADHOC NETWORK	International Conference on Recent Trends in Engineering, Science and Technology (ICRTEST), Tamil Nadu, Chennai	International	2016	No info given		Elsevier Energy Procedia

Number of books and chapters in edited volumes / books published, and papers in national/international conference

Name of the Teacher	Title of the book/chapters published	Title of the paper	Title of the proceedings of the conference	Name of the conference	National / International	Year of publication	ISBN/ISSN number of the proceeding	Affiliating Institute at the time of publication	Name of the publisher
Pooja Sharma	Programming in Python				International	2017	978-93-8655-127-6	IKGPTU	BPB Publications, New Delhi
Pooja Sharma	Advanced Concepts in Real-Time Image and Video Processing/Radial Moments for Image Retrieval				International	2017	978-15-2252-849-4	DAV University	IGI Global, USA
Pooja Sharma	Advanced Concepts in Real-Time Image and Video Processing/Recognition of Face Biometrics				International	2017	978-15-2252-849-4	DAV University	IGI Global, USA
Anshu Bhasin		Image Restoration on Mammography Images	(ICCCA)2016	International Conference on Computing, Communication and Automation	International	2017	ISBN: 978-1-5090-1666-2	IKGPTU	IEEE Xplore
Dr. Monika Sachdeva	Next-Generation Networks, Singapore	Detection of hello flood attack on LEACH in wireless sensor networks	--	--	International	2018	978-981-10-6005-2	IKGPTU, Kapurthalla	Springer

Number of books and chapters in edited volumes / books published, and papers in national/international conference

Name of the Teacher	Title of the book/chapters published	Title of the paper	Title of the proceedings of the conference	Name of the conference	National / International	Year of publication	ISBN/ISSN number of the proceeding	Affiliating Institute at the time of publication	Name of the publisher
Dr. Monika Sachdeva	Next-Generation Networks, Singapore	Detection of selective forwarding (Gray Hole) attack on LEACH in wireless sensor networks	--	--	International	2018	978-981-10-6005-2	IKGPTU, Kapurthalla	Springer
Dr. Monika Sachdeva	Networking Communication and Data Knowledge Engineering	Detection and Prevention of DDoS Attacks in Wireless Sensor Networks	--	--	International	2018	978-981-10-4585-1	IKGPTU, Kapurthalla	Springer
Raman Kumar	Cryptanalysis of protocol for enhanced threshold proxy signature scheme based on elliptic curve cryptography for known signers	Cryptanalysis of protocol for enhanced threshold proxy signature scheme based on elliptic curve cryptography for known signers	-	-	International	2018	10.1007/978-981-10-6680-1_10		Springer
Madhu Dahiya and Raman Kumar	IEEE First International Conference on Secure Cyber Computing and Communications (ICSCCC),	A Literature Survey on various Image Encryption & Steganography Techniques	A Literature Survey on various Image Encryption & Steganography Techniques	IEEE First International Conference on Secure Cyber Computing and	International	2018	No info given	NIT Jalandhar	IEEE

Number of books and chapters in edited volumes / books published, and papers in national/international conference

Name of the Teacher	Title of the book/chapters published	Title of the paper	Title of the proceedings of the conference	Name of the conference	National / International	Year of publication	ISBN/ISSN number of the proceeding	Affiliating Institute at the time of publication	Name of the publisher
				Communications (ICSCCC),					
Raman Kumar	Security Analysis and Performance Evaluation of an Enhanced Multi Factor Authentication Scheme based on Elliptic Curve Cryptography	Security Analysis and Performance Evaluation of an Enhanced Multi Factor Authentication Scheme based on Elliptic Curve Cryptography	-	-	National	2018	No info given	-	National Conference, 21 st PSC, PAU Ludhiana, India
Ketanpreet Kaur, Dr. Monika Sachdeva	Lecture Notes in Electrical Engineering, vol 605. Springer, Cham	Fog Computing in IOT: An Overview of New Opportunities.		Proceedings of ICETIT 2019.	International	2019	978-3-030-30577-2	IKGPTU	Springer
Raman Kumar and Uffe Kock Wiil	Recent Advances in Computational Intelligence			-	International	2019	Published (978-3-030-12499-1)		Springer
Raman Kumar and	Design and Analysis of an Enhanced Multifactor Authentication	Design and Analysis of an Enhanced Multifactor	-	-	International	2019	10.1007/978-3-030-12500-4_3		Springer

Number of books and chapters in edited volumes / books published, and papers in national/international conference

Name of the Teacher	Title of the book/chapters published	Title of the paper	Title of the proceedings of the conference	Name of the conference	National / International	Year of publication	ISBN/ISSN number of the proceeding	Affiliating Institute at the time of publication	Name of the publisher
Uffe Kock Wiil	Through a Covert Approach	Authentication Through a Covert Approach							
Stuti Mehla, Anjali Chaudhary, and Raman Kumar	Review on Current Trends of Deep Learning	Review on Current Trends of Deep Learning	-	-	International	2019	10.1007/978-3-030-12500-4_4		Springer
Bijeta Seth, Surjeet Dalal, and Raman Kumar	Hybrid Homomorphic Encryption Scheme for Secure Cloud Data Storage	Hybrid Homomorphic Encryption Scheme for Secure Cloud Data Storage	-	-	International	2019	978-3-030-12500-4_5		Springer
Rishipal, Sweta Saraff and Raman Kumar	A Gamification Framework for Redesigning the Learning Environment	A Gamification Framework for Redesigning the Learning Environment	-	-	International	2019	10.1007/978-3-030-12500-4_6		Springer
Shakti Arora, Surjeet Dalal and	A Variant of Secret Sharing Protected with Poly-1305,	A Variant of Secret Sharing Protected with Poly-1305,	-	-	International	2019	10.1007/978-3-030-12500-4_7		Springer

Number of books and chapters in edited volumes / books published, and papers in national/international conference

Name of the Teacher	Title of the book/chapters published	Title of the paper	Title of the proceedings of the conference	Name of the conference	National / International	Year of publication	ISBN/ISSN number of the proceeding	Affiliating Institute at the time of publication	Name of the publisher
Raman Kumar									
Bijeta Seth, Surjeet Dalal, and Raman Kumar	Securing Bioinformatics Cloud for Big Data: Budding Buzzword or a Glance of the Future	Securing Bioinformatics Cloud for Big Data: Budding Buzzword or a Glance of the Future	-	-	International	2019	978-3-030-12500-4_8		Springer
Raman Kumar and Uffe Kock Wiil	Enhancing Gadgets for Blinds Through Scale Invariant Feature Transform	Enhancing Gadgets for Blinds Through Scale Invariant Feature Transform	-	-	International	2019	10.1007/978-3-030-12500-4_9		Springer
Raman Kumar and Uffe Kock Wiil	Recent Advances in Computational Intelligence			-	International	2019	Published (978-3-030-12499-1)		Springer
Anshu Bhasin	Handbook of Wireless Sensor Networks	Energy Conscious Packet Transmission in Wireless Networks using trust based			International	2020	ISBN: 978-3-030-40305-8	IKGPTU	Springer Nature Switzerland AG

Number of books and chapters in edited volumes / books published, and papers in national/international conference

Name of the Teacher	Title of the book/chapters published	Title of the paper	Title of the proceedings of the conference	Name of the conference	National / International	Year of publication	ISBN/ISSN number of the proceeding	Affiliating Institute at the time of publication	Name of the publisher
		Mechanism: A Cognitive Approach							
Kunal Singh and Raman Kumar	Design of a Low-Cost Sensor-Based IOT System for Smart Irrigation	Design of a Low-Cost Sensor-Based IOT System for Smart Irrigation	-	-	International	2020	978-3-030-35280-6_4		Springer
Anshu Bhasin	Distributed Denial of Service Attacks: Concepts, Mathematical and Cryptographic Solutions	Understanding and implementation of machine learning using support vector machine for efficient DDoS attack detection:			International	2020	https://doi.org/10.1515/9783110619751-002	IKGPTU	De Gruyter, Boston