DOI: 10.14569/IJACSA.2024.0150169

PDF

A Novel Approach to Data Clustering based on Self-Adaptive Bacteria Foraging Optimization

Author 1: Tanmoy Singha Author 2: Rudra Sankar Dhar Author 3: Joydeep Dutta Author 4: Arindam Biswas

International Journal of Advanced Computer Science and Applications(IJACSA), Volume 15 Issue 1, 2024.

Abstract and Keywords | How to Cite this Article | {} BibTeX Source

Abstract: Data clustering reduces the number of data objects by grouping similar data objects together. In this process, data are divided into valuable groups (clusters) or expressive without at all previous information. This manuscript represents a different clustering algorithm based on the technique of the adaptive strategy algorithm known as Self-Adaptive Bacterial Foraging Optimization (SABFO). It is a streamlining strategy for bunching issues where a cluster of bacteria forages to converge to definite locations as ultimate group communities by limiting the fitness function. The superiority of this method is assessed on numerous famous benchmark data sets. In this paper, the authors have compared the projected technique with some well-known advanced clustering approaches: the k-means algorithm, the Particle Swarm optimization algorithm, and the Fitness-Based Adaptive Differential Evolution (FBADE) Scheme. An experimental finding demonstrates the usefulness of the projected algorithm as a clustering

Upcoming Conferences

Computer Vision Conference (CVC) 2026

16-17 April 2026 Berlin, Germany

Outline

Show full outline

Cited by (42)

Figures (6)






Tables (10)

Table 1
Table 2
Table 3
Table 4
Table 5
Table 6

Expert Systems with Applications
Volume 237, Part B, 1 March 2024, 121605

A new correlation-based measure on Fermatean fuzzy applied on multi-criteria decision making for electric vehicle selection

Soumendu Golui [a b], Biplab Sinha Mahapatra [c], Ghanshaym Singha Mahapatra [d]

Show more

https://doi.org/10.1016/j.eswa.2023.121605

Abstract

Purpose:

Since the pollution from the transportation sector has become intolerable in urban areas, many authorities are beginning to ban vehicles powered by fossil fuels. In this scenario, electric vehicle (EV) mobility is the only viable option for the transportation sector. Despite the fact that EVs offer a number of advantages over fuel-powered vehicles, it can be challenging for a purchaser to select a model due to its technical features and their lack of knowledge about EVs. This article aims to assist purchasers of EV by constructing an MCDM problem with multiple features as criteria and EV models as alternatives.

Design/methodology/approach:

The Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) method ranks alternatives to a multi-criteria decision-making (MCDM) problem based on the distance between the positive and negative ideal solutions. Even though the TOPSIS methodology has several fuzzy enhancements, it is difficult to select an appropriate distance measure in an uncertain context. To replace the distance measure, we introduced an improved correlation coefficient measure in fermatean fuzzy contexts by considering the hesitancy function of fermatean fuzzy sets (FFS). First, we establish the proposed correlation coefficient by defining its main characteristics, including the weighted correlation coefficient, type I and type II closeness measures, and the weighted index coefficient. Then, the TOPSIS method is extended using the proposed correlation measure in a fermatean fuzzy environment. There is an algorithm that presents the proposed fermatean fuzzy TOPSIS (FF-TOPSIS) method. The proposed approach is used to

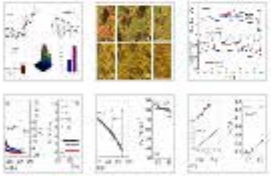
Recommended a

MsGEN: Measuring nutrient value pred
Expert Systems with App
Gordana Ispirova, ..., Ba
View PDF

A consolidated MCI performance assess
Renewable and Sustaina
Fatih Ecer

A sustainability eva the urban energy in
Expert Systems with App
Yang Yang, ..., Yuqiang Z
View PDF

Show 3 more articles



Research article

Ferroelectric and antiferroelectric chiral multilactate liquid crystalline materials with negative dielectric anisotropy

Priyanta Barman [a], Malay Kumar Das [a], Banani Das [b], Sergei Mironov [c], Vera Hamplova [c], Alexej Bubnov [c]

Show more

https://doi.org/10.1016/j.nxmate.2024.100208

Get rights and content

Under a Creative Commons license

Open access

Highlights

- The physical properties of two chiral multilactate liquid crystals have been studied.
- The compounds show SmA*, SmC* and SmC_A^* phases.
- DSC, electro-optic and dielectric spectroscopy measurements were performed.
- Compounds show large spontaneous polarization and smaller response time.
- 3D plots of the dielectric loss clearly demonstrated the existence of SmC_{Re}^* phase.

Abstract

In this work, the mesomorphic, electro-optic and dielectric properties have been discussed in the light of molecular structure-property correlations of two chiral multilactate liquid crystalline materials possessing the orthogonal paraelectric Smectic A* phase, tilted ferroelectric Smectic C* phase and the tilted antiferroelectric Smectic C_A^* phase, over a substantially broad temperature range. Interestingly, a reasonably rare re-entrant Smectic C* phase (SmC_{Re}^*) has also been identified in one of the investigated materials. These materials differ in their linkage groups (keto or ether) and an additional chiral unit in the terminal chain. The phase transition temperatures and transition enthalpies were determined from Polarizing Optical Microscopy and Differential

interface on 4.5V $LiCoO_2$ cathode to realiz...

Next Materials, Volume 5, 2024, Article 100228

Keding Chen, ..., Wei Zhang

View PDF

Effect of Zn doping on structural, morphological, optical and electrical...

Next Materials, Volume 5, 2024, Article 100234

Nargis Fatima Khatoon, ..., Muhammad Zulfequar

View PDF

High-efficiency laminated luminescent solar concentrators based on carbon dots...

Next Materials, Volume 5, 2024, Article 100277

Donzhou Huang, ..., Jianying Wang

View PDF

Show 3 more articles

View PDF | Download full issue

Outline

Show full outline

Cited by (4)

Figures (17)

Show 11 more figures

Computer Networks
Volume 238, January 2024, 110113

PF-IBDA: Provably secure and pairing-free identity-based deniable authentication protocol for MANET environments

SK Hafizul Islam [a, 1], Krittibas Paral [b], Daya Sagar Gupta [c, 1]

Show more

Add to Mendeley | Share | Cite

https://doi.org/10.1016/j.comnet.2023.110113

Get rights and content

Full text access

Abstract

Mobile Adhoc Network (MANET) is used in various real-time applications, such as e-voting, army tactical communication, health-care applications, disaster rescue, online message exchange, etc. However, source authentication and deniability are essential properties in such applications. Typically, these properties can be achieved using a deniable authentication (DA) protocol. With the help of a DA protocol, a mobile receiver node can directly verify the source, another mobile node, of a message without consulting a trusted third party (TTP). Recently, many identity-based deniable authentication (IBDA) protocols have been proposed. Most of these protocols are insecure and computationally expensive since they use costly operations, such as bilinear pairing and map-to-point hash function. We proposed a pairing-free identity-based deniable authentication (PF-IBDA) protocol for MANET environments. We proved that the PF-IBDA protocol could provide indistinguishability against adaptive chosen ciphertext attack (IND-CCA2) in the random oracle model (ROM) based on the hardness assumption of the elliptic curve computational Diffie–Hellman (ECCDH) problem. We have computed the execution time of PF-IBDA protocol in different security levels: 80-bit, 112-bit, 128-bit, 192-bit, and 256-bit on a mobile device using the JPBC library and compared it with the state-of-the-art IBDA protocols. We found that the proposed PF-IBDA protocol is more efficient than the existing IBDA protocols.

Previous article in issue | Next article in issue

Recommended articles

A smart contract-based robotic surgery authentication system for healthcare usin...
Computer Networks, Volume 238, 2024, Article 110133
Neeraj Kumar, Rifaqat Ali
View PDF

Unlocking QoS Potential: Integrating IoT services and Monte Carlo Control for...
Computer Networks, Volume 238, 2024, Article 110134
Imane Chakour, ..., Mohamed Baslam
View PDF

Unavailability-aware allocation of backup resources considering failures of virtual a...
Computer Networks, Volume 239, 2024, Article 110141
Naoomi Kita, Eiji Oki
View PDF

Show 3 more articles

IoT-ID3PAKA: Efficient and Robust ID-3PAKA Protocol for Resource-Constrained IoT Devices

Publisher: IEEE Cite This PDF

Krittibas Parai ; Daya Sagar Gupta ; SK Hafizul Islam **All Authors**

Abstract:
The Internet of Things (IoT) is an emerging technology that has become popular in many applications, such as transportation, agriculture, healthcare, industrial automation, robotics, etc. IoT devices are interconnected via the Internet, and secure message communication between them is a challenging task. An authenticated key agreement (AKA) protocol can solve such an issue. This article designed and implemented an identity-based three-party AKA (IoT-ID3PAKA) protocol to establish a shared session key among three IoT devices. The current state-of-the-art identity-based 3PAKA (ID-3PAKA) protocols are unsuitable for resource-constrained IoT devices because almost all of them undergo various security attacks and require higher execution and communication overheads. The provable security of the proposed IoT-ID3PAKA protocol relies on the hardness assumption of the elliptic curve-based computational Diffie–Hellman problem. The execution time of IoT-ID3PAKA for the security levels: 80, 112, 128, 192, and 256 bits on a Raspberry Pi 4 device is estimated and compared with the existing ID-3PAKA protocols.

Published in: IEEE Internet of Things Journal (Volume: 11 , Issue: 6, 15 March 2024)

More Like This

Fuzzy Elliptic Curve Cryptography for Authentication in Internet of Things
IEEE Internet of Things Journal
Published: 2022

Revisting of elliptical curve cryptography for securing Internet of Things (IOT)
2018 Advances in Science and Engineering Technology International Conferences (ASET)
Published: 2018

Show More

Future Generation Computer Systems
Volume 154, May 2024, Pages 453-464

A deep learning-based authentication protocol for IoT-enabled LTE systems

A. Sai Venkateshwar Rao [a], Prasanta Kumar Roy [b], Tarachand Amgoth [a], Ansuman Bhattacharya [a]

Show more

+ Add to Mendeley Share Cite

https://doi.org/10.1016/j.future.2024.01.014

Highlights

- Authentication and key agreement protocol.
- Deep learning-based key generation technique.
- Security and privacy in large scale heterogeneous IoT-enabled LTE system.
- Comparatively higher attack detection rate and lower attack detection time.

Abstract

The connected devices in Internet-of-Things (IoT)-enabled systems are continuously increasing nowadays, and likely to grow exponentially worldwide in near future. Hence, the next generation IoT-enabled mobile networks (e.g., 5G onward) are expected to provide higher system capacity and ultra-low latency to deal with. According to the Third Generation Partnership Project (3GPP), Long-Term Evolution (LTE) technology can serve the purpose efficiently, and also bridge the gap between earlier and future generation mobile networks. However, the network may face problems associated with privacy and security, as the underlying communication is mostly wireless. Thus, a secure and efficient Authentication and Key Agreement (AKA) protocol is desirable. Recently, many protocols have been proposed to address these goals. Unfortunately, the security and efficiency of such protocols are still in doubt. This paper introduces a deep learning-based AKA protocol for IoT-enabled LTE systems. The proposed protocol can address mutual authentication among the communicating entities. It employs a Deep Residual Network

DOI: 10.14569/IJACSA.2024.0150169

PDF

A Novel Approach to Data Clustering based on Self-Adaptive Bacteria Foraging Optimization

Author 1: Tanmoy Singha Author 2: Rudra Sankar Dhar Author 3: Joydeep Dutta Author 4: Arindam Biswas

International Journal of Advanced Computer Science and Applications(IJACSA), Volume 15 Issue 1, 2024.

Abstract and Keywords | How to Cite this Article | {} BibTeX Source

Abstract: Data clustering reduces the number of data objects by grouping similar data objects together. In this process, data are divided into valuable groups (clusters) or expressive without at all previous information. This manuscript represents a different clustering algorithm based on the technique of the adaptive strategy algorithm known as Self-Adaptive Bacterial Foraging Optimization (SABFO). It is a streamlining strategy for bunching issues where a cluster of bacteria forages to converge to definite locations as ultimate group communities by limiting the fitness function. The superiority of this method is assessed on numerous famous benchmark data sets. In this paper, the authors have compared the projected technique with some well-known advanced clustering approaches: the k-means algorithm, the Particle Swarm optimization algorithm, and the Fitness-Based Adaptive Differential Evolution (FBADE) Scheme. An experimental finding demonstrates the usefulness of the projected algorithm as a clustering method that can operate on data sets with different densities, and cluster sizes.

Next Materials 5 (2024) 100308

Contents lists available at ScienceDirect

Next Materials

journal homepage: www.sciencedirect.com/journal/next-materials

Research article

Ferroelectric and antiferroelectric chiral multilactate liquid crystalline materials with negative dielectric anisotropy

Priyanta Barman [a], Malay Kumar Das [a,*], Banani Das [b], Sergei Mironov [c], Vera Hamplova [c], Alexej Bubnov [c]

[a] Department of Physics, University of North Bengal, Siliguri, West Bengal 734013, India
[b] Department of Physics, Siliguri Institute of Technology, Siliguri, West Bengal 734009, India
[c] Institute of Physics, Czech Academy of Sciences, Prague 18221, Czech Republic

ARTICLE INFO

Keywords:
Chiral liquid crystals
Mesomorphic properties
Electro-optical measurement
Dielectric spectroscopy
Structure-property relationship
Re-entrant SmC* phase

ABSTRACT

In this work, the mesomorphic, electro-optic and dielectric properties have been discussed in the light of molecular structure-property correlations of two chiral multilactate liquid crystalline materials possessing the orthogonal paraelectric Smectic A* phase, tilted ferroelectric Smectic C* phase and the tilted antiferroelectric Smectic C_A* phase, over a substantially broad temperature range. Interestingly, a reasonably rare re-entrant Smectic C* phase (SmC_{re}*) has also been identified in one of the investigated materials. These materials differ in their linkage groups (keto or ether) and an additional chiral unit in the terminal chain. The phase transition temperatures and transition enthalpies were determined from Polarizing Optical Microscopy and Differential Scanning Calorimetry (DSC) measurements. The compounds exhibit negative dielectric anisotropy ($\Delta\varepsilon$) throughout the mesomorphic range (maximum −18 and −4 in SmA* for both the compounds) and moderately high values of spontaneous polarization (−153 nC/cm^2 in SmC_{re}* phase). The temperature dependence of the response time (τ), bulk viscosity (η) and the activation energies (E_a) throughout the mesomorphic phase have been determined from the spontaneous polarization measurements. To emphasize the structure-property correlations in more detail, dielectric spectroscopy measurement has also been performed to measure the dielectric strength, dielectric loss, frequency dependent permittivities, relaxation time and relaxation frequencies. The clear evidence of the relatively rare SmC_{re}* phase has also been confirmed from the temperature and frequency dependence of the dielectric permittivity. These results shed important light on the emergence of these materials as a smart alternative for their application in multicomponent mixtures targeted for advanced electro-optic and photonic devices.

LIQUID CRYSTALS
https://doi.org/10.1080/02678292.2023.2275745

Taylor & Francis
Taylor & Francis Group

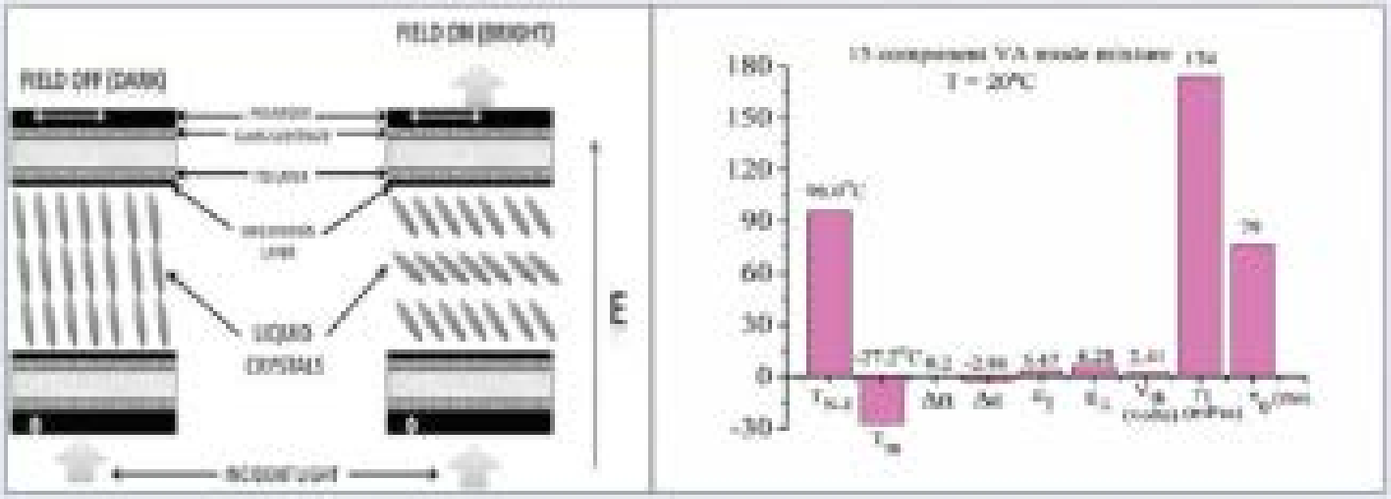
Novel properties of high-performance multi-component mixture for Vertically Aligned mode LCDs

Prajnamita Dasgupta[a], Sarmistha Mondal[b], Banani Das[c] and Malay Kumar Das[d]

[a]Department of Chemistry, North Bengal University, Siliguri, India; [b]Department of Electronics and Communication Engineering, Siliguri Institute of Technology, Siliguri, India; [c]Department of Physics, Siliguri Institute of Technology, Siliguri, India; [d]Department of Physics, North Bengal University, Siliguri, India

ABSTRACT

Vertically Aligned mode Liquid Crystal Displays (VALCDs) which have generated huge research interest due to their excellent contrast and wide viewing angle require materials with negative dielectric anisotropy. This work highlights the systematic development of a fifteen-component mixture from pure liquid crystalline compounds comprising laterally fluorinated bi-, tri- phenyl, tolane, bicyclohexane compounds and non-mesogenic compounds exhibiting negative dielectric anisotropy. The temperature dependence of birefringence (Δn), dielectric anisotropy ($\Delta\varepsilon$), threshold voltage (V_{th}), bend elastic constant (K_{33}), relaxation time (τ_d) and rotational viscosity (γ_1) as a function of temperature of this fifteen-component nematic mixture have been reported. This mixture exhibits a high Figure of Merit (FoM) which is desirable for reducing the device response time. Additionally, the orientational order parameter (OOP) values, activation energy (E_a), visco-elastic co-efficient (γ_1/K_{33}) and material parameters (A_0) have also been reported. The effect of pretilt angle in the alignment layers on the threshold voltage (V_{th}) and switching time (τ_d) to ascertain the applicability of this material in Vertically Aligned mode Liquid Crystal Displays (VALCDs) have also been discussed.



ARTICLE HISTORY
Received 28 July 2023
Accepted 23 October 2023

KEYWORDS
VA-LCDs; multi-component mixture; negative dielectric anisotropy; birefringence; bend elastic constant; pretilt

International Journal of Computational and Applied Mathematics.
ISSN 1819-4966 Volume 18, Number 2 (2023), pp. 183-187

http://www.ripublication.com

An Extension of Method of Proportion for Solving Nonlinear Equations

Jayanta Dutta
Department of Mathematics, Siliguri Institute of Technology, Siliguri-734009, India.

Abstract

In this paper an iterative method is presented for solving nonlinear equations based on the proportion of two real parameters, associated with the given equations. In the proposed method, a single iterative formula is generated by considering the additional terms in an expression given in the method of proportion developed earlier. It is also shown that the number of iterations decreases with the increases of the number terms in the right hand side of a key expression. The methods are supported by various numerical examples and shown that the new proposed methods are effective and comparable to the well-known Newton's method.

Key words: Nonlinear equation, Proportion, Iterative method, Newton's method.

NMES

About
Aims and Scope
Editorial Board
Instructions for Authors
Article Processing Charge
Publication Ethics
Submission
Current Issue
Archive
Citation List

Load Frequency Control in Renewable Energy Penetrated Hybrid Power Systems

Indrajit Koley* | Asim Datta | Goutam Kumar Panda

Corresponding Author Email: indrajit.koley@gmail.com

Page: 268-276 **DOI:** https://doi.org/10.14447/jnmes.v26i4.a05

Received: 18 August 2022 **Revised:** 29 June 2023 **Accepted:** 7 July 2023 **Available online:** 15 November 2023

Citation

DOWNLOAD PDF

OPEN ACCESS

Abstract:

In order to ensure zero steady-state error in multi-area hybrid power systems, load frequency control is implemented in the power system. However, variations in load due to cyclic amplitude deviation create frequency fault leading to unscheduled tie-line power. Hence a novelOperational Load Forecasting Approach is utilized in which objective function in support vector regression predicts load demand and generation based on temporalcharacteristicsand utilize parallel processing to tolerate the acceptable error margin. Moreover, the uncertainties of active power generation in islanding mode make the estimation of frequency response deviation under decentralized islanding modes difficult. Hence a novelDifferential ControllerAlgorithm has been proposed in which the sigmoidal range function determines the optimal amplitude value from individual areasand the controller predicts the high load demand area that exceeds the threshold limit and isolatesthat area until the deviation is rectified. Low tie-line power, frequency, and settling time deviations were accomplished using the proposed methodologies as they were simulated using the Simulink platform.

Keywords:

Unaccustomed Earth: The Saga of Alienation and Broken Myths and the Emergence of a New Immigrant Culture.

Rimni Chakravarty
Asst professor, Humanities
Department of Engineering Sciences and Humanities
Siliguri Institute of Technology

Abstract

Literature ,since time immemorial has always portrayed life in its varied aspects presenting the culture of the time .By culture it can be understood the values,beliefs,ideas,thoughts,emotions of the particular society where the author pens down in a picturesque manner . Culture is reflected in everything: language, literature, visual arts, verbal and non-verbal attitude of the people of the society. Cultures may differ in conducts, food habits, dressing style, way of expression, courtesies, management of time and. The manner of presenting the self based on thoughts and beliefs. The present paper emphasizes on the novel *Unaccustomed Earth* the second short story collection by critically acclaimed Bengali-American author Jhumpa Lahiri. Published in 2008 about the struggle of the Indians settled in America with the American culture as also their own tradition which they try hard to cast aside yet their own customs, surface when confronted with different situations. This collection of short stories paints the life in the Indian American Diaspora. The author pictures the struggle of the two generations of the Indian Immigrants who have settled in America where most of the protagonists belong to the second generation trying to adjust themselves in the American culture yet totally could not negate the Indian tradition of hospitality. The article finds out how the different characters struggle adopting the culture of the land they have settled in and projecting their own Indian culture which they have inherited by birth. The article projects how complexities arise in relationships where the characters feign to be contented in their adopted life style. The article also finds how restless the characters are and as they are torn and tossed between the east and west which they struggle hard to identify and find their own identity in the world where there is only struggle for existence .Here they search for the roots to carve a niche in the new world they have moved for future The article arrives at a conclusion that perpetual bliss is utopia and that in this exile one can surrender to Time for the pursuit of peace and happiness. This is the modern culture which the article has endeavored to bring out as reflected in *Unaccustomed Earth* reflecting modern life.

Key Terms: Literature, Culture, Bengali-American, complexities, modern, peace.

Introduction

Realizing Spirituality in Every Moment of Life

Rimni Chakravarty
Asst .Professor
Humanities
Siliguri Institute of Technology

Abstract

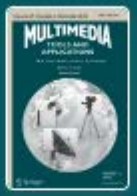
Spirituality as the dictionary states is "the quality of being concerned with the human spirit or soul as opposed to material or physical things" .The term spirituality has become very much vogue in every sector of life .In fact spirituality has become a subject of discussion in every seminar, conference with some purpose to solve the problems persisting in our society and lead life that help every human being to prosper with mental satisfaction. The aim of this article is to discuss what is the meaning of spirituality and how it was practiced through ages in our Indian culture and the ways individuals can practice to connect the self with the others known or unknown to feel united and attain bliss for developing a world where one can connect oneself with the other in a harmonious manner .It would be a world where through spiritual practice there would be a feeling of one ness or the "we attitude" that benefit the society at large. It is also an attempt to find out how various issues can be solved by being spiritual in everyday situation. It is also an attempt to discuss how the path of spirituality guide students as well as the professionals to utilize their energy for developing positive attitude and building conducive environment for smooth ,flawless communication and also solve physical and mental disturbances by being treading on to the path of spirituality. The study concludes with the recommendation that spiritual education need to be mandatory in every school college and even important for parents to follow so they become the role models who pass on the legacy to their next generation for a world of peace and harmony

Key words: spirituality, culture, legacy, peace, harmony

Predictive framework for crime data analysis using a hybrid logistic regression — support vector machine based ensemble classifier powered by CART (LR-SVM^{CART})

Published: 17 March 2023

Volume 82, pages 35357–35377, (2023) Cite this article



Multimedia Tools and Applications

Aims and scope →

Submit manuscript →

Anupam Mukherjee & Anupam Ghosh

Abstract

Significant rise in illegal activity has directly impacted socioeconomic growth and quality of life. In this article, a predictive crime data analysis framework has been proposed that can resolve the problem of scalability issues and accuracy rate. This paper proposed a hybrid ensemble machine learning classifier to identify authentic crime activities. A series of experiments are used to verify the efficiency of our proposed algorithms. Three datasets of different countries are used for this experiment purpose. All the datasets are tested successfully on our proposed framework and novel ensembles classifier. The result produced by our proposed hybrid ensemble classifier mostly outperforms the performance of most of the existing machine learning approaches. This work aims to identify geospatial crime data intensity where we can anticipate the recurrence of a certain crime in the city using geospatial technology, allowing the police force to take the required precautions to avoid it.

Computer Networks
Volume 238, January 2024, 110113

PF-IBDA: Provably secure and pairing-free identity-based deniable authentication protocol for MANET environments

SK Hafizul Islam [a 1], Krittibas Paral [b], Daya Sagar Gupta [c 1]

https://doi.org/10.1016/j.comnet.2023.110113

Abstract

Mobile Adhoc Network (MANET) is used in various real-time applications, such as e-voting, army tactical communication, health-care applications, disaster rescue, online message exchange, etc. However, source authentication and deniability are essential properties in such applications. Typically, these properties can be achieved using a deniable authentication (DA) protocol. With the help of a DA protocol, a mobile receiver node can directly verify the source, another mobile node, of a message without consulting a trusted third party (TTP). Recently, many identity-based deniable authentication (IBDA) protocols have been proposed. Most of these protocols are insecure and computationally expensive since they use costly operations, such as bilinear pairing and map-to-point hash function. We proposed a pairing-free identity-based deniable authentication (PF-IBDA) protocol for MANET environments. We proved that the PF-IBDA protocol could provide indistinguishability against adaptive chosen ciphertext attack (IND-CCA2) in the random oracle model (ROM) based on the hardness assumption of the elliptic curve computational Diffie–Hellman (ECCDH) problem. We have computed the execution time of PF-IBDA protocol in different security levels: 80-bit, 112-bit, 128-bit, 192-bit, and 256-bit on a mobile device using the JPBC library and compared it with the state-of-the-art IBDA protocols. We found that the proposed PF-IBDA protocol is more efficient than the existing IBDA protocols.

IoT-ID3PAKA: Efficient and Robust ID-3PAKA Protocol for Resource-Constrained IoT Devices

Publisher: IEEE Cite This PDF

Krittibas Parai ; Daya Sagar Gupta ; SK Hafizul Islam **All Authors**

Abstract:
The Internet of Things (IoT) is an emerging technology that has become popular in many applications, such as transportation, agriculture, healthcare, industrial automation, robotics, etc. IoT devices are interconnected via the Internet, and secure message communication between them is a challenging task. An authenticated key agreement (AKA) protocol can solve such an issue. This article designed and implemented an identity-based three-party AKA (IoT-ID3PAKA) protocol to establish a shared session key among three IoT devices. The current state-of-the-art identity-based 3PAKA (ID-3PAKA) protocols are unsuitable for resource-constrained IoT devices because almost all of them undergo various security attacks and require higher execution and communication overheads. The provable security of the proposed IoT-ID3PAKA protocol relies on the hardness assumption of the elliptic curve-based computational Diffie–Hellman problem. The execution time of IoT-ID3PAKA for the security levels: 80, 112, 128, 192, and 256 bits on a Raspberry Pi 4 device is estimated and compared with the existing ID-3PAKA protocols.

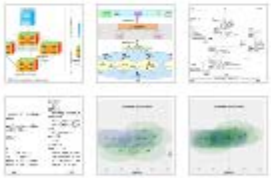
Published in: IEEE Internet of Things Journal (Volume: 11 , Issue: 6, 15 March 2024)

More Like This

Fuzzy Elliptic Curve Cryptography for Authentication in Internet of Things
IEEE Internet of Things Journal
Published: 2022

Revisting of elliptical curve cryptography for securing Internet of Things (IOT)
2018 Advances in Science and Engineering Technology International Conferences (ASET)
Published: 2018

Show More



Research article

DC-IIoT: A Secure and Efficient Authentication Protocol for Industrial Internet-of-Things Based on Distributed Control Plane

Rakesh Salam, Prasanta Kumar Roy, Ansuman Bhattacharya

Show more

https://doi.org/10.1016/j.iot.2023.100782

Get rights and content

Full text access

Highlights

- Improved network performance and system availability.
- Logically centralized and physically distributed SDN controllers.
- Prevention of node-compromised attack and detection of cloning attack.
- Proper access control and communication security.
- Compatibility with resource-constrained IIoT environments.

Abstract

Proper access control and communication security are the key requirements for real-time data-transfer in Industrial Internet-of-Things (IIoT). Besides, the system reliability and robustness may be affected, as the traffic volume is increasing gradually, and there may be heterogeneous IoT-devices in the network. Hence, a global control over the entire network becomes crucial to ensure Quality-of-Service (QoS). As the IoT-devices operate from a remote location with no (or minimum) human intervention, they may be compromised easily. Hence, it becomes essential to guarantee the system security even if one or more IoT-devices are compromised unexpectedly. Recently, some Software-Defined Networking (SDN)-based approaches have been proposed to ensure communication security and global control over heterogeneous IoT-devices. However, they may suffer from single-point-of-failure due to the use of a centralized SDN controller. In this article, we put forward a secure and efficient authentication protocol

Computer Networks, Volume 223, 2023, Article 109579
Evrim Guler, ..., Suleyman Uludag

View PDF

BDPC: Controlling application delay in 6TiSCH networks for the industrial Intern...

Internet of Things, Volume 22, 2023, Article 100778
Lucas Almurello, Diego Dujovne

View PDF

Matchmaker: Maintaining network programmability for Software-Defined...

Computer Networks, Volume 192, 2021, Article 108045
Songshi Dou, ..., Yuanqing Xia

View PDF

Show 3 more articles

Future Generation Computer Systems
Volume 154, May 2024, Pages 461-464

A deep learning-based authentication protocol for IoT-enabled LTE systems

A. Sai Venkateshwar Rao [a], Prasanta Kumar Roy [b], Tarachand Amgoth [a], Ansuman Bhattacharya [a]

Show more

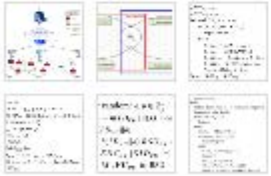
https://doi.org/10.1016/j.future.2024.01.014

Highlights

- Authentication and key agreement protocol.
- Deep learning-based key generation technique.
- Security and privacy in large scale heterogeneous IoT-enabled LTE system.
- Comparatively higher attack detection rate and lower attack detection time.

Abstract

The connected devices in Internet-of-Things (IoT)-enabled systems are continuously increasing nowadays, and likely to grow exponentially worldwide in near future. Hence, the next generation IoT-enabled mobile networks (e.g., 5G onward) are expected to provide higher system capacity and ultra-low latency to deal with. According to the Third Generation Partnership Project (3GPP), Long-Term Evolution (LTE) technology can serve the purpose efficiently, and also bridge the gap between earlier and future generation mobile networks. However, the network may face problems associated with privacy and security, as the underlying communication is mostly wireless. Thus, a secure and efficient Authentication and Key Agreement (AKA) protocol is desirable. Recently, many protocols have been proposed to address these goals. Unfortunately, the security and efficiency of such protocols are still in doubt. This paper introduces a deep learning-based AKA protocol for IoT-enabled LTE systems. The proposed protocol can address mutual authentication among the communicating entities. It employs a Deep Residual Network



Future Generation Computer Systems
Volume 163, February 2025, 107520

ZeroVCS: An efficient authentication protocol without trusted authority for zero-trust vehicular communication systems

Prasanta Kumar Roy [a], Pankaj Kumar [b], Ansuman Bhattacharya [c]

Show more

https://doi.org/10.1016/j.future.2024.107520

Highlights

- Zero-trust vehicular communication systems.
- Authentication without trusted authority.
- STRIDE-based threat modeling and security.
- Malicious node tracing.
- Performance improvement and quality of service.

Abstract

Vehicular communication systems can provide two types of communications: Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V). However, in both cases, there is zero-trust between the communicating entities. This may give privilege to the unauthorized vehicles to join the network. Hence, a strong authentication protocol is required to ensure proper access control and communication security. In traditional protocols, such tasks are typically accomplished via a central Trusted Authority (TA). However, communication with TA may increase the overall authentication delay. Such delay may be incompatible with the future generation vehicular communication systems, where dense deployment of small-cells are required to ensure higher system capacity and seamless mobility (e.g., 5G onward). Further, TA may suffer from denial-of-service when the number of access requests becomes excessively large, because each request must be forwarded to TA for authentication and access control. In this article, we put forward an efficient authentication protocol without trusted authority for zero-trust