SECURE DATA GROUP SHARING AND CONDITIONAL DISSEMINATION WITH MULTI OWNER WITH CLOUD COMPUTING

A Project Report submitted in partial fulfillment of the requirements

for the award of the degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

By

VEMUGANTI SHIRISHA (21S41D5819)

Under the Guidance of

Dr. GULAB SINGH

Associate Professor

Department of Computer Science & Engineering

VAAGESWARI COLLEGE OF ENGINEERING

(Affiliated to JNTUH Hyderabad, Approved by AICTE and Accredited with NAAC A+ Grade)

Ramakrishna colony, Karimnagar-505481

2022-2023

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

Department of Computer Science & Engineering

VAAGESWARI COLLEGE OF ENGINEERING

(Affiliated to JNTUH Hyderabad, Approved by AICTE and Accredited with NAAC A+ Grade)

Ramakrishna colony, Karimnagar-505481

CERTIFICATE

This is to certify that the project report entitled **"SECURE DATA GROUP SHARING AND CONDITIONAL DISSEMINATION WITH MULTI OWNER WITH CLOUD COMPUTING"** submitted by following student in partial fulfillment of the requirements for the award of the Degree of Master of Technology in CSE, and is a bonafide record of the work performed by her.

VEMUGANTI SHIRISHA (21S41D5819)

The work embodied in this project report has not been submitted to any other institution for the award of any degree.

INTERNAL GUIDE **HEAD OF THE DEPARTMENT**

EXTERNAL EXAMINER **PRINCIPAL**

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

CONCLUSION

Customers are concerned about the safety and confidentiality of their data when they use cloud computing. The challenge of protecting sensitive information while also satisfying the demands of several owners for their privacy is complex. This paper presents a secure method for group data sharing and conditional dissemination in cloud computing with multiple owners. Our proposal calls for the data owner to encrypt their data using the IBBE approach before making it easily accessible to several data accessors simultaneously.By using attribute-based CPRE, the data owner may establish fine-grained access controls to the ciphertext, ensuring that only data disseminators with matching characteristics can re-encrypt it. We also offer a way for several parties to regulate who may access the ciphertext, which is useful for data co-owners who want to set their own access policies. We also present three methods for policy aggregation—full permission, owner priority, and majority consent—to handle privacy concerns. Our long-term goal is to make it even better by enabling keyword searches on top of the encrypted material.

ABSTRACT

Thanks to cloud computing, the number of cloud services has grown rapidly, which has allowed for the exchange of massive data volumes. Although cloud computing relies on cryptographic methods to secure user data, current systems do not let co-owners control who may access what data by putting privacy issues on ciphertext that is associated with many owners. Secure group data sharing and conditional dissemination in cloud computing with numerous owners is proposed in this work. Here, data owners may safely share sensitive information with a group of users over the cloud, and then those who distribute the data can reassign it to a new group of users whose attributes satisfy the requirements for deciphering the ciphertext. We provide a method for controlling who has access to the distributed ciphertext and allow data co-owners to tailor it to their own privacy needs by introducing new rules. To address the issue of privacy conflicts induced by different access rules, three solutions for policy aggregation are presented: owner priority, majority permit, and entire permission. After extensive testing, our system has shown to be beneficial for many owners' secure cloud data sharing needs.

WEB BASED COLLABORATE BIG DATA ANALYTICS ON BIG DADA

A Project Report submitted in partial fulfillment of the requirements

for the award of the degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

By

SAMREEN SULTHANA (21S41D5814)

Under the Guidance of

Dr. N.CHANDRAMOULI

Associate Professor & HOD

Department of Computer Science & Engineering

VAAGESWARI COLLEGE OF ENGINEERING

(Affiliated to JNTUH Hyderabad, Approved by AICTE and Accredited with NAAC A+ Grade)

Ramakrishna colony, Karimnagar-505481

2022-2023

Department of Computer Science & Engineering

VAAGESWARI COLLEGE OF ENGINEERING

(Affiliated to JNTUH Hyderabad, Approved by AICTE and Accredited with NAAC A+ Grade)

Ramakrishna colony, Karimnagar-505481

CERTIFICATE

This is to certify that the project report entitled **"WEB BASED COLLABORATE BIG DATA ANALYTICS ON BIG DADA"** submitted by following student in partial fulfillment of the requirements for the award of the Degree of Master of Technology in CSE, and is a bonafide record of the work performed by her.

SAMREEN SULTHANA (21S41D5814)

The work embodied in this project report has not been submitted to any other institution for the award of any degree.

INTERNAL GUIDE **HEAD OF THE DEPARTMENT**

EXTERNAL EXAMINER **PRINCIPAL**

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

ABSTRACT

Data storage, analysis, and sifting through such enormous volumes of information has emerged as a new challenge in the wake of the rise of cloud computing and social media. The inadequacy of traditional technology to handle massive data sets has led to the development of big data platforms. Through the use of big data platforms, users may develop analytical services with more efficiency. Data collecting, analytics service building, and algorithm development all still take a long time. We provide a collaborative big data analytics platform built for big data as a service. Through the platform's ability to enable the interchange of data, algorithms, and services, developer cooperation is greatly enhanced. Consequently, this article details a big data analytics platform that facilitates web-based cooperation among data owners, data scientists, and service developers; it also aids in handling massive amounts of data and developing analytics algorithms and applications. The platform is completed with the introduction of a CCTV metadata analytics solution.

9. CONCLUSION AND FUTURE ENHANCEMENT

9.1 Conclusion:

In this piece, we laid up the groundwork for a collaborative big data analytics system. On the big data platform, you may access two web portals: one for analytics, which is for BDaaS application development, and another for web service collaboration. With the help of YARN for multi-tenancy and enhanced access control, we have made it easier for participants to work together on the platform. The use of a web service portal is commonplace when dealing with services online. The analytics portal, which is part of the web service portal, gives users access to many tools for working with big data, both in terms of management and development. We concluded by showcasing CCTV metadata analytics as an analytics service. We have been enhancing the streaming processing system to provide a platform for real-time analytics.

9.2 Future steps for improvement:

In the future, researchers will look at other types of service-generated big data, such as service trace logs, information on service quality, and service relationships. A number of approaches to service-generated big data analytics will get more in-depth investigation. Beyond the confines of this paper, we shall investigate security issues and lay out the technologies at play in great depth.

SPAMMER DETECTION AND FAKE USER IDENTIFICATION ON SOCIAL NETWORKS

A Project Report submitted in partial fulfillment of the requirements

for the award of the degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

By

AYESHA FATIMA (21S41D5821)

Under the Guidance of

Dr.E.SRIKANTH REDDY

Associate Professor

Department of Computer Science & Engineering

VAAGESWARI COLLEGE OF ENGINEERING

(Affiliated to JNTUH Hyderabad, Approved by AICTE and Accredited with NAAC A+ Grade)

Ramakrishna colony, Karimnagar-505481

2022-2023

Department of Computer Science & Engineering
VAAGESWARI COLLEGE OF ENGINEERING
(Affiliated to JNTUH Hyderabad, Approved by AICTE and Accredited with NAAC A+ Grade)
Ramakrishna colony, Karimnagar-505481

CERTIFICATE

This is to certify that the project report entitled **"SPAMMER DETECTION AND FAKE USER IDENTIFICATION ON SOCIAL NETWORKS"** submitted by following student in partial fulfillment of the requirements for the award of the Degree of Master of Technology in CSE, and is a bonafide record of the work performed by her.

AYESHA FATIMA **(21S41D5821)**

The work embodied in this project report has not been submitted to any other institution for the award of any degree.

INTERNAL GUIDE **HEAD OF THE DEPARTMENT**

EXTERNAL EXAMINER **PRINCIPAL**

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

ABSTRACT

Every day, people from all around the globe utilise social media. The way people use social media sites like Facebook and Twitter may greatly affect their everyday life, and that can be a problem at times. On well-known social media platforms, spammers are proliferating and inundating users with harmful and unnecessary messages. As an example, Twitter's recent meteoric rise to fame has led to an overwhelming amount of spam. Spammy tweets promoted by fake accounts harm legitimate users and squander resources. In addition, people are more likely to be exposed to hazardous material due to the spread of false information via fake identities.

Researchers often look at modern OSNs for ways to identify Twitter spammers and imposters. We investigated every possible avenue in our quest to identify the Twitter spammer. The following is a taxonomy of Twitter spam detection algorithms: I for algorithms that can identify phoney content; II for algorithms that can detect spam within URLs; III for algorithms that can detect spam inside popular topics; and IV for algorithms that can detect fake accounts. Users, content, graphs, structures, and temporal aspects are only a few of the metrics used to evaluate the presented methods. We want for this study to be the definitive source for academics looking for up-to-date information on Twitter spam detection.

9.CONCLUSION

The purpose of this study was to examine the existing approaches to detecting Twitter spammers. In addition, we supplied a taxonomy of Twitter spam detection approaches, categorising them as follows: methods for identifying fraudulent material, methods for identifying spam connected to trending topics, methods for identifying spam based on URLs, and methods for identifying phoney users. In order to compare the offered techniques, we employed a number of parameters, such as user, content, graph, structure, and temporal characteristics. Furthermore, the datasets used and the aims intended to be accomplished were the evaluative criteria for the techniques. With this review presented as is, researchers should have an easier time finding in-depth resources on state-of-the-art Twitter spam detection algorithms.Although academics have developed efficient and effective approaches for Twitter spam detection and fake user identification, there are still some unsolved concerns that need more research [34]. Here is a brief rundown of the problems:Investigating the issue of detecting fake news on social media networks is warranted due to the substantial personal and societal effects of such misinformation [25]. Another relevant topic that needs exploring is where rumours on social media first appear. Some studies have attempted to trace the origins of rumours using statistical methods, but more recent approaches based on social networks have been much more fruitful.

DIGITISED AND DECENTRALIZED BLOCKCHAIN TECHNOLOGY

A Project Report submitted in partial fulfillment of the requirements

for the award of the degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

By

DOMKONDAWAR VAISHNAVI (21S41D5824)

Under the Guidance of

Dr.E.SRIKANTH REDDY

Associate Professor

Department of Computer Science & Engineering

VAAGESWARI COLLEGE OF ENGINEERING

(Affiliated to JNTUH Hyderabad, Approved by AICTE and Accredited with NAAC A+ Grade)

Ramakrishna colony, Karimnagar-505481

2022-2023

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

Department of Computer Science & Engineering

VAAGESWARI COLLEGE OF ENGINEERING

(Affiliated to JNTUH Hyderabad, Approved by AICTE and Accredited with NAAC A+ Grade)

Ramakrishna colony, Karimnagar-505481

CERTIFICATE

This is to certify that the project report entitled **"DIGITISED AND DECENTRALIZED BLOCKCHAIN TECHNOLOGY"** submitted by following student in partial fulfillment of the requirements for the award of the Degree of Master of Technology in CSE, and is a bonafide record of the work performed by her.

DOMKONDAWAR VAISHNAVI (21S41D5824)

The work embodied in this project report has not been submitted to any other institution for the award of any degree.

INTERNAL GUIDE **HEAD OF THE DEPARTMENT**

EXTERNAL EXAMINER **PRINCIPAL**

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

ABSTRACT

If a reliable third party is still needed to avoid double-spending, even with digital signatures, the major advantages will be rendered useless. Hence, we suggest an alternative to traditional financial institutions a decentralized, peer-to-peer electronic payment system.

8. CONCLUSION AND FUTURE ENHANCEMENT

8.1 Conclusion:

Our proposal might pave the way for trustless electronic transactions. Digital signature coins were our first approach. While they provide strong ownership control, they don't prevent duplicate spending.

Our proposed solution is a proof-of-work network, in which all nodes publicly record all transactions. The majority of the nodes are trustworthy, therefore altering this history would be computationally impossible for an attacker.The disorganisation of the network is really one of its strengths. Each node works both alone and in combination.

Since the messages are not intended for a particular recipient, their identification is moot. What matters is that they convey them as efficiently as possible.

Blockchain technology presents a possible answer to the long-standing issue of central banking, notwithstanding these disadvantages.

8.2 Future-Proof Enhancements: Blockchain ensures the safety and security of all transactions between nodes. Traditional banking systems' two biggest problems—the time and money needed to complete transactions—are therefore reduced. Being a relatively new technology, there may be a lot more upgrades down the line.

ANDROID MALWARE DETECTION USING GENETIC ALGORITHM BASED OPTIMIZED FEATURE SELECTION AND MACHINE LEARNING

A Project Report submitted in partial fulfillment of the requirements

For the award of the degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

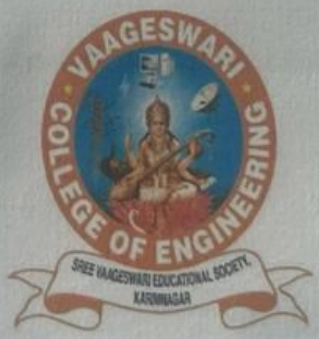
By

PILLI MADHAVI (21S41D5811)

Under the guidance of

Mrs. Y. SUSHEELA

Associate Professor



DEPARTMENT OF COMPUTER SCIENCES & ENGINEERING

VAAGESWARI COLLEGE OF ENGINEERING

(Affiliated to JNTU Hyderabad &Approved by AICTE and Accredited with NAAC A+ Grade)

Ramakrishna colony, Karimnagar-505481

2022-2023

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

DEPARTMENT OF COMPUTER SCIENCES & ENGINEERING

VAAGESWARI COLLEGE OF ENGINEERING

(Affiliated to JNTU Hyderabad, Approved by AICTE And Accredited with NAAC A+ Grade)

Ramakrishna colony, Karimnagar-505481

CERTIFICATE

This is to certify that the project report entitled **'ANDROID MALWARE DETECTION USING GENTIC ALGORITHM BASED OPTIMIZED FEATURE SELECTION AND MACHINE LEARNING'** submitted by following student in partial fulfillment of the requirements for the award of the Degree of Master of Technology in CSE and is a bonafide record of the work performed by her.

PILLI MADHAVI **(21S41D5811)**

The work embodied in this project report has not been submitted to any other institution for the award of any degree

INTERNAL GUIDE

HEAD OF THE DEPARTMENT

EXTERNAL EXAMINER

PRINCIPAL

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

ABSTRACT

The Android platform has the most market share internationally because to its open source status and Google's support. Malware authors have started using it as a vector to disseminate their wares because to its massive user base. Using an evolutionary genetic algorithm for discriminating feature selection, this research presents a machine-learning-based strategy for Android malware detection that has been effective. We train machine learning classifiers using features extracted from genetic algorithms and evaluate their malware-identification skills before and after feature selection. The experimental findings show that the genetic algorithm successfully reduces the feature dimension to less than half by offering the most optimum subset of the original collection of characteristics. Classifiers trained using machine learning have the potential to lower the processing cost of learning by a large margin, operate on a much reduced feature dimension, and still retain a classification accuracy of over 94% even after feature selection.

We cover a lot of ground, including genetic algorithms, reverse engineering, feature selection, and Android malware research.

8.CONCLUSION AND FUTURE ENHANCEMENT

Conclusion

As the number of threats to Android platforms continues to rise, largely as a result of malicious applications, there is an immediate need to create a framework that can reliably detect malware on these systems. In cases when conventional approaches relying on malware signatures fail to detect zero-day threats, techniques derived from machine learning are used. The proposed method employs an evolutionary genetic algorithm in an effort to derive the optimal feature subset for use in training machine learning algorithms.

Future Improvements

Using SVM and NN classifiers on a lower-dimensional feature-set lowers the classifiers' training complexity while keeping a strong classification performance of over 94%, as shown experimentally. The future of Genetic Algorithm research depends on expanding its datasets and investigating its interplay with other ML algorithms.

CREDIT CARD FRAUD ANALYSIS BY USING XGBOOST ALGORITHM

A Project Report submitted in partial fulfillment of the requirements

for the award of the degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

By

ANUMANDLA NIROSHA (21S41D5801)

Under the Guidance of

Dr. GULAB SINGH

Associate Professor

Department of Computer Science & Engineering

VAAGESWARI COLLEGE OF ENGINEERING

(Affiliated to JNTUH Hyderabad, Approved by AICTE and Accredited with NAAC A+ Grade)

Ramakrishna colony, Karimnagar-505481

2022-2023

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

Department of Computer Science & Engineering
VAAGESWARI COLLEGE OF ENGINEERING
(Affiliated to JNTUH Hyderabad, Approved by AICTE and Accredited with NAAC A+ Grade)
Ramakrishna colony, Karimnagar-505481

CERTIFICATE

This is to certify that the project report entitled **"CREDIT CARD FRAUD ANALYSIS BY USING XGBOOST ALGORITHM"** submitted by following student in partial fulfillment of the requirements for the award of the Degree of Master of Technology in CSE, and is a bonafide record of the work performed by her.

ANUMANDLA NIROSHA (21S41D5801)

The work embodied in this project report has not been submitted to any other institution for the award of any degree.

INTERNAL GUIDE **HEAD OF THE DEPARTMENT**

EXTERNAL EXAMINER **PRINCIPAL**

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

ABSTRACT

The study primarily aims to improve methods for detecting credit card fraud in practical settings. At the same time that the amount of credit card transactions has skyrocketed, the frequency of fraudulent operations has also been on the rise. The objective here is to acquire unauthorized access to funds or merchandise. The only way for credit card issuers to keep their losses down is to implement robust fraud detection systems. The fact that the card and its owner don't need to be present for the transaction creates a big hurdle for the business. As a result, the store can't verify the buyer's identity at any point throughout the purchase. To make fraud detection more accurate, the proposed technique uses random forest and the Xgboost algorithm. Xgboost and random forest classification analysis of the user's present dataset and other datasets. Finally, check that the data findings are correct to the best of your ability. The effectiveness of the procedures is evaluated using measures such as precision, sensitivity, and accuracy. After analysing a subset of the provided features, the next step is to build the graphical model visualisation, which signals fraud detection. The effectiveness of the procedures is evaluated using measures such as precision, sensitivity, and accuracy. The accuracy that XgBoostst obtained was second only to that of random forest.

8.CONCLUSION AND FUTURE ENHANCEMENT

8.1 conclusion:

Improving the xgboost algorithm's performance requires more training data, which in turn slows down testing and application. Using additional pre-processing steps might also be advantageous. More data preparation may have enhanced the findings, even if SVM delivers good results. The SVM approach still has issues with imbalanced datasets, which is why this happens.

8.2 Future Enhancements:

Following this article's methods, researchers will concentrate on online learning models. Also, we will look at different ways of teaching and learning online. One potential benefit of online education is the increased speed and, maybe, real-time detection of fraud scenarios. Consequently, the financial sector will suffer fewer daily losses as a consequence of improved fraud identification and prevention.

Department of Computer Science & Engineering
VAAGESWARI COLLEGE OF ENGINEERING
(Affiliated to JNTUH Hyderabad, Approved by AICTE and Accredited with NAAC A+ Grade)
Ramakrishna colony, Karimnagar-505481

CERTIFICATE

This is to certify that the project report entitled **"MINING USERS TRUST FROM E-COMMERCE REVIEWS BASED ON SENTIMENT SIMILARITY ANALYSIS"** submitted by following student in partial fulfillment of the requirements for the award of the Degree of Master of Technology in CSE, and is a bonafide record of the work performed by her.

SAMALA VASUDHA **(21S41D5813)**

The work embodied in this project report has not been submitted to any other institution for the award of any degree.

INTERNAL GUIDE

HEAD OF THE DEPARTMENT

EXTERNAL EXAMINER

PRINCIPAL

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

MINING USERS TRUST FROM E-COMMERCE REVIEWS BASED ON SENTIMENT SIMILARITY ANALYSIS

A Project Report submitted in partial fulfillment of the requirements

for the award of the degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

By

SAMALA VASUDHA (21S41D5813)

Under the Guidance of

Dr. GULAB SINGH

Associate Professor

Department of Computer Science & Engineering

VAAGESWARI COLLEGE OF ENGINEERING

(Affiliated to JNTUH Hyderabad, Approved by AICTE and Accredited with NAAC A+ Grade)

Ramakrishna colony, Karimnagar-505481

2022-2023

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

ABSTRACT

In e-commerce platforms, reviews written by actual customers may influence users' opinions and ultimately their purchasing decisions. All this data may be seen as an expression of the interests, attitudes, and views of consumers. Several studies have shown that people are more likely to trust others who share their opinions on similar topics. According to our findings, there must be some level of trust between businesses and their consumers if they are prepared to provide feedback via online shopping platforms. This viewpoint suggests a sentiment similarity analysis approach based on E-commerce system reviews mining to examine the degree to which users are similar and trustworthy. We primarily focus on two forms of trust: direct trust and propagation of trust, which indicates a trust link between two individuals. We provide a method for mining sentiment-based entity-word pairings for similarity characteristics; the direct trust degree is then calculated from this similarity. We may find the trust propagation using the transitivity characteristic. Using the proposed trust representation model, we give a better shortest route method for determining the propagation trust link between users and apply it to the definition of trust tightness. We collect data from a large dataset of online shop reviews to see how the algorithms perform and if the models are practical. Experimental results suggest that sentiment similarity analysis could be a powerful method for winning over sceptical internet consumers.

9.CONCLUSION

Finding out how trusting customers are of an online store is a problem that we address in our research. By excluding two kinds of trust relationships—direct trust and propagation trust—we move the emphasis from studying user trust to finding out how much their reviews agree on a sentiment. You can find out how similar two reviews are in terms of sentiment using entity-sentiment word pairs mining, and you can find out how trustworthy someone is using sentiment similarity analysis, which takes ratings and feelings into account. Combining these two criteria allows you to study the sentiment direct trust link. We established a model for weighted trust graph-based propagation trust computation. Trust that may spread from one person to another is called propagation trust. When two people don't know one other personally but may create indirect trust via third parties who do, they can build this kind of trust. The propagation trust calculation technique's time complexity is O(V2), where V is the number of nodes in the network, and it is based on the upgraded shortest route approach. More research into methods to increase the computational complexity of the algorithm is required because of the comparatively large number of users in present e-commerce platforms.