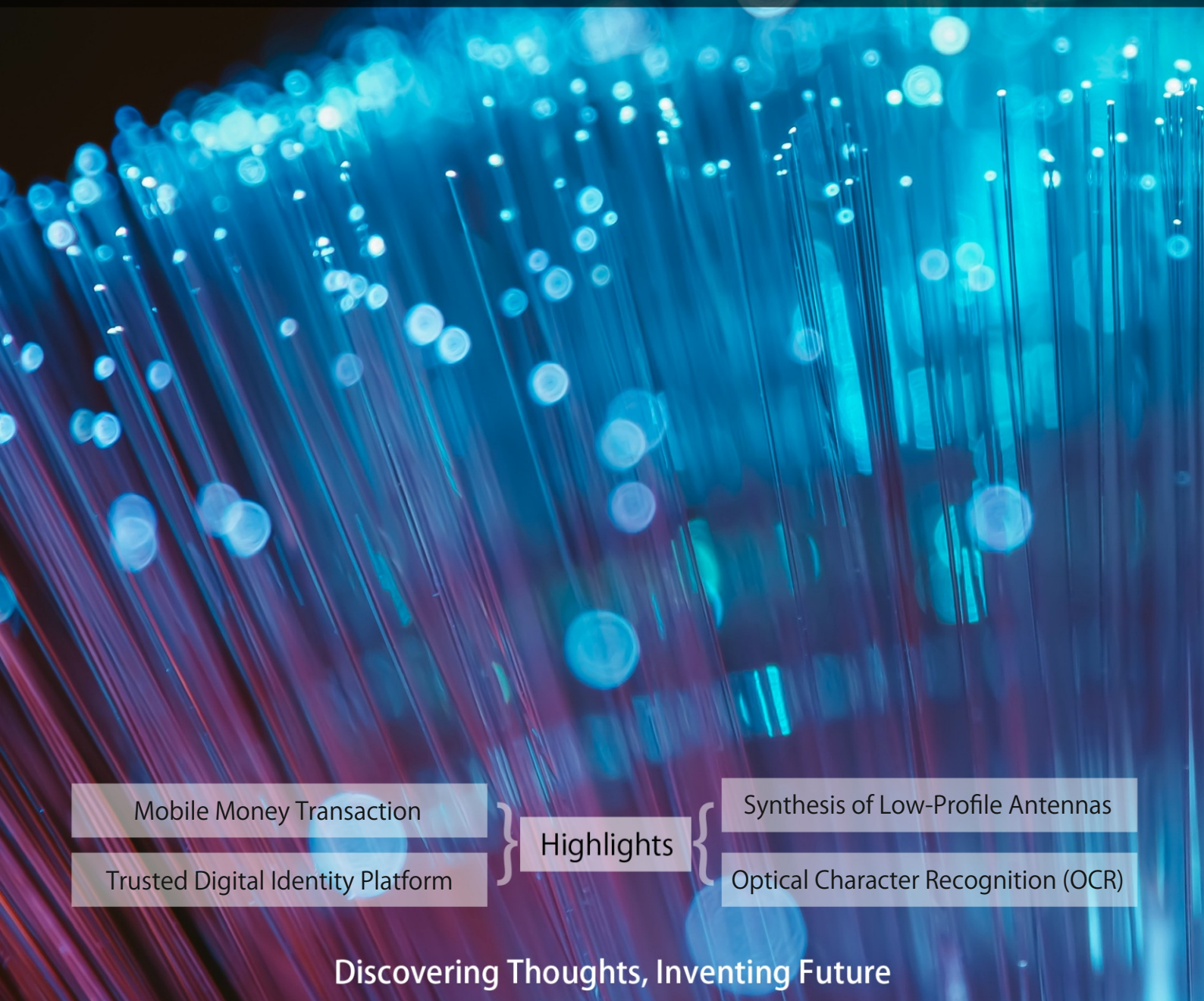
Online ISSN : 0975-4172
Print ISSN : 0975-4350
DOI : 10.17406/GJCST

Global Journal

of Computer Science and Technology: E

Network, Web & Security



Highlights

- Mobile Money Transaction
- Trusted Digital Identity Platform
- Synthesis of Low-Profile Antennas
- Optical Character Recognition (OCR)

Discovering Thoughts, Inventing Future

VOLUME 22 ISSUE 1 VERSION 1.0

Global Journal of Computer Science and Technology: E
Network, Web & Security

Global Journal of Computer Science and Technology: E
Network, Web & Security

Volume 22 Issue 1 (Ver. 1.0)

Open Association of Research Society

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

*(A Delaware USA Incorporation with "Good Standing"; **Reg. Number: 0423089**)*

Sponsors: Open Association of Research Society
Open Scientific Standards

Publisher's Headquarters office

Global Journals® Headquarters
945th Concord Streets,
Framingham Massachusetts Pin: 01701,
United States of America
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Journals Incorporated
2nd, Lansdowne, Lansdowne Rd., Croydon-Surrey,
Pin: CR9 2ER, United Kingdom

Packaging & Continental Dispatching

Global Journals Pvt Ltd
E-3130 Sudama Nagar, Near Gopur Square,
Indore, M.P., Pin:452009, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please email us at *local@globaljournals.org*

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *investors@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Excluding Air Parcel Charges):

Yearly Subscription (Personal & Institutional)
250 USD (B/W) & 350 USD (Color)

Editorial Board

Global Journal of Computer Science and Technology

Dr. Stefano Berretti

Ph.D. in Computer Engineering and Telecommunications, University of Firenze Professor Department of Information Engineering, University of Firenze, Italy

Dr. Abdurrahman Arslanyilmaz

Computer Science & Information Systems Department Youngstown State University Ph.D., Texas A&M University University of Missouri, Columbia Gazi University, Turkey

Dr. Lamri Sayad

Ph.d in Computer science, University of BEJAIA, Algeria

Dr. Tauqeer Ahmad Usmani

Ph.D in Computer Science, Oman

Dr. Hazra Imran

Ph.D in Computer Science (Information Retrieval), Athabasca University, Canada

Dr. Magdy Shayboub Ali

Ph.D in Computer Sciences, MSc in Computer Sciences and Engineering, BSc in Electronic Engineering, Suez Canal University, Egypt

Dr. Nurul Akmar Binti Emran

Ph.D in Computer Science, MSc in Computer Science, Universiti Teknikal Malaysia Melaka, Malaysia

Dr. Asim Sinan Yuksel

Ph.D in Computer Engineering, M.Sc., B.Eng., Suleyman Demirel University, Turkey

Dr. Anis Bey

Dept. of Computer Science, Badji Mokhtar-Annaba University, Annaba, Algeria

Alessandra Lumini

Associate Researcher Department of Computer Science and Engineering University of Bologna Italy

Dr. Rajesh Kumar Rolen

Ph.D in Computer Science, MCA & BCA - IGNOU, MCTS & MCP - MIcrosoft, SCJP - Sun Microsystems, Singhania University, India

Dr. Rajneesh Kumar Gujral

Ph.D in Computer Science and Engineering, M.TECH in Information Technology, B. E. in Computer Science and Engineering, CCNA Certified Network Instructor, Diploma Course in Computer Servicing and Maintenance (DCS), Maharishi Markandeshwar University Mullana, India

Dr. Aziz M. Barbar

Ph.D. IEEE Senior Member Chairperson, Department of Computer Science AUST - American University of Science & Technology Alfred Naccash Avenue Ashrafieh, Lebanon

Dr. Federico Tramarin

Ph.D., Computer Engineering and Networks Group, Institute of Electronics, Italy Department of Information Engineering of the University of Padova, Italy

Dr. Chutisant Kerdvibulvech

Dept. of Inf. & Commun. Technol., Rangsit University Pathum Thani, Thailand Chulalongkorn University Ph.D. Thailand Keio University, Tokyo, Japan

Dr. Roheet Bhatnagar

Ph.D in Computer Science, B.Tech in Computer Science, M.Tech in Remote Sensing, Sikkim Manipal University, India

Contents of the Issue

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 22 Issue 1 Version 1.0 Year 2022
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Synthesis of Low-Profile Antennas using Fractal Analysis

By S. V. Dvornikov, Vi Vlasenko & A. A. Rusin
St. Petersburg State University of Aerospace Instrumentation

Abstract- The results of the synthesis of low-profile antennas based on taking into account the very similarity of their elements are presented. The main disadvantages of low-profile antennas and promising ways to overcome them are considered. The results of calculating their characteristics in the MMANA-GAL and CST Microwave Studio modeling environment are presented. Possibilities of fractal types of low-profile antennas are investigated. The prospects for their application have been determined.

Keywords: *low-profile antennas, fractal antennas, in-phase antenna systems.*

GJCST-E Classification: *I.3.7*

Strictly as per the compliance and regulations of:

Synthesis of Low-Profile Antennas using Fractal Analysis

Синтез низкопрофильных антенн методом фрактального анализа

S. V. Dvornikov [α], Vi Vlasenko [σ] & A. A. Rusin [ρ]

Abstract- ***Представлены результаты синтеза низкопрофильных антенн на основе учета само подобия их элементов. Рассмотрены основные недостатки низкопрофильных антенн и перспективные пути их преодоления. Приведены результаты расчета их характеристик в среде моделирования MMANA-GAL и CST Microwave Studio. Исследованы возможности фрактальных типов низкопрофильных антенн. Определены перспективы их применения.***

Ключевыеслова: низкопрофильные антенны, фрактальные антенны, синфазные антенные системы.

Abstract- The results of the synthesis of low-profile antennas based on taking into account the very similarity of their elements are presented. The main disadvantages of low-profile antennas and promising ways to overcome them are considered. The results of calculating their characteristics in the MMANA-GAL and CST Microwave Studio modeling environment are presented. Possibilities of fractal types of low-profile antennas are investigated. The prospects for their application have been determined.

Keywords: low-profile antennas, fractal antennas, in-phase antenna systems.

I. Ведение

Методы теории фракталов, разработанные Мандельбротом [1], находят самое широкое применение в различных практических приложениях радиотехники. В основе фрактального анализа лежат свойства самоподобия фракталов, как простейших элементов, комбинации которых позволяют синтезировать сложные конструкции с прогнозируемыми желательными свойствами [2, 3]. Строгая иерархия, определяемая фракталами, открывает особенно широкие возможности при построении и разработки излучающих устройств на основе антенных решеток [4].

В частности, анализ работ [5–7] показал, что методы фрактального анализа позволяют получать антенные решетки, обладающие не только гармоничной структурой, но и с необходимой формой диаграмм направленности. Фрактальная геометрия, представленная в [8], показывает, что наиболее просто методы фрактального анализа реализуются в линейных антеннах, состоящих из совокупности самоподобных элементов.

В частности, в [9] обосновано, что такой подход обеспечивает высокое постоянство параметров излучающей системы в очень широком частотномдиапазоне. При этом он позволяет уйти от непосредственного синтеза сигналов [10], к синтезу устройств, что особенно важно для мобильных систем [11].

В настоящее время фрактальный подход успешно используется при разработке логопериодических, биконических и различных спиральных антенн [12]. При этом следует понимать, что такой синтез ведет к увеличению размеров антенных систем, при том, что получаемые таким образом антенны не обладают высокой частотной селекцией, поскольку у них реализован принцип самодополнения. А переход к конечной структуре антенны приводит к ограничению ее диапазонных свойств.

Очевидно, что методы синтеза антенн на основе фрактальных элементов требуют детального теоретического осмысления, с последующим проведением практических экспериментов, направленных тна поиск оптимальных структур.

Учитывая указанные обстоятельства, в настоящей статье представлены результаты исследований, связанных с синтезом низкопрофильных антенных систем на основе фрактальных элементов.

II. Особенности низкопрофильных антенн

Низкопрофильные антенные системы известны достаточно давно и активно применяются как в системах связи, так и радиотехнических системах [13]. Практический аспект их развития связан с необходимостью миниатюризации размеров радиотехнических систем. Как правило, такие антенныизготавливают на основе различных металлических или диэлектрических излучателей, которые располагают на относительно небольшой высоте $h < 0{,}1\lambda$ над металлическим экраном.

Основным достоинством низкопрофильных антенн являются их небольшие габариты и относительно малый вес. Это обеспечивает удобство размещения таких антенн на подвижных

Author α: Ph.D., Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, St. Petersburg, RF. e-mail: practicdsv@yandex.ru

Author σ: St. Petersburg State University of Aerospace Instrumentation, St. Petersburg, Ph.D. tech. Science. e-mail: vlasenko1939@mail.ru

Author ρ: Ph.D. tech. Science, Senior Lecturer of the Department, Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, candidate of technical sciences, associate professor. e-mail: arusin@yandex.ru

радиотехнических объектах, или в местах, с ограниченными геометрическими размерами.

К другим несомненным положительным моментам низкопрофильных антенн, следует отнести простоту их изготовления и достаточно низкую стоимость, обеспечиваемых применением интегральных технологий изготовления печатных плат, совмещенных с излучателем [14].

В настоящее время, актуальность миниатюризации антенн определяется активным развитием беспроводных систем связи [15]. Действительно, если на базе интегральных схем, возможен синтез антенных решеток сравнительно небольшого объема, массы и главное малой высоты, то почему бы их и не использовать.

В общем случае, форма излучателя низкопрофильной антенной решетки не обязательно может быть линейной (в виде вибратора). Как правило, в плоскостной (пластинчатой), щелевой, спиральной структурах используют антенные элементы с самыми различными геометрическими формами.

Вместе с тем, низкопрофильным антеннам присущи и определенные недостатки. К основным из которых следует отнести: узкая полоса рабочих частот; низкая эффективность (малый КПД); побочные излучения ее элементов и высокий уровень кроссполяризации.

В [16, 17] обосновано, что один из путей получения эффективных малогабаритных антенн, связан с использование при их разработке методов фрактальной геометрии.Следовательно, целесообразно рассмотрим возможность применения простых фракционных элементов с целью устранения некоторых недостатков низкопрофильных антенных решеток.

III. Фрактальный синтез низкопрофильных антенн

В качестве примера рассмотрим синфазную антенную систему, состоящую из двух полуволновых вибраторов ($\ell / \lambda = 0,25$) на рабочей частоте f = 750 МГц. Будем полагать, что вибраторы расположены над рефлектором на высоте h = 5 см.

Далее исследуем характеристика такой системы при различном расположении вибраторов. В частности, при использовании однопроводных вибраторов, *V*-образных вибраторов, а также вибраторов, собранных на основе фрактальных элементов.

Модели антенных систем для *V*-образных вибраторов, а также вибраторов, собранных на основе фрактальных элементов,показаны на рис. 1. Справа представлена система на основе *V*-образных вибраторов, а справа – вибраторов, на основе фрактальных элементов.

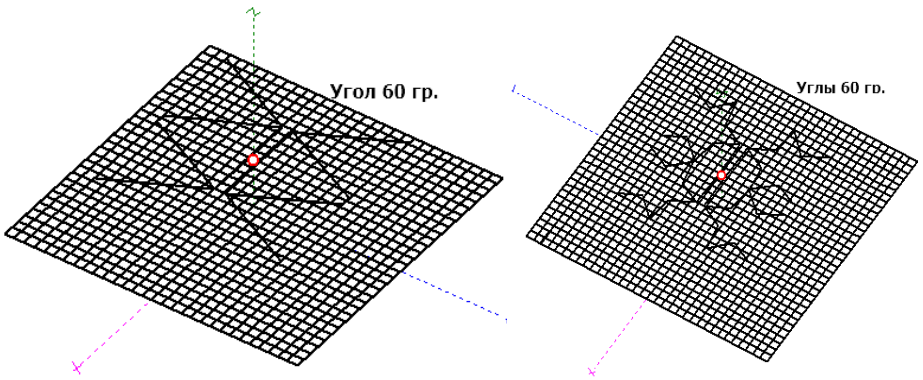
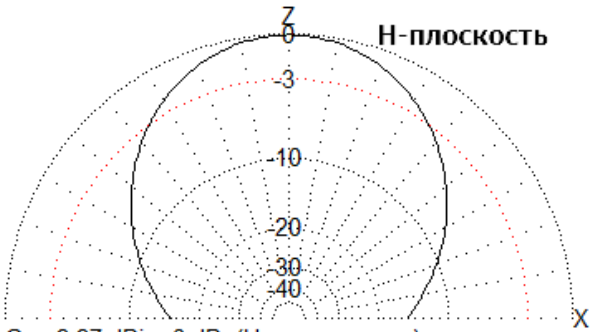


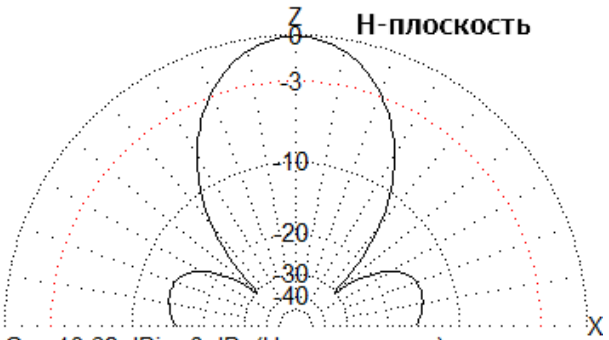
Рис. 1: Структуры элементов антенных решеток

Для получения и последующей оценки количественных параметров рассмотренных антенных систем, была использована компьютерная программа MMANA-GAL.

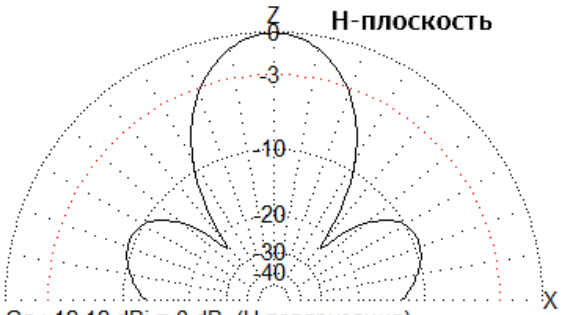
Так, на рис. 2, 3 и 4 показаны рассчитанные диаграммы направленности (ДН) рассматриваемых антенных систем на частотах 750 МГц, 1800 МГц и 2100 МГц. На указанных рисунках ДН приведены по мощности излучения с учетом отражающей поверхности.



Ga : 8.87 dBi = 0 dB (H поляризация)
Gh : 6.72 dBd
F/B: -13.07 dB; Тыл: Азим. 120 гр, Элевация 60 гр
F: 750.000 МГц
Z: 74.285 + j82.443 Ом
КСВ: 2.9 (75.0 Ом).

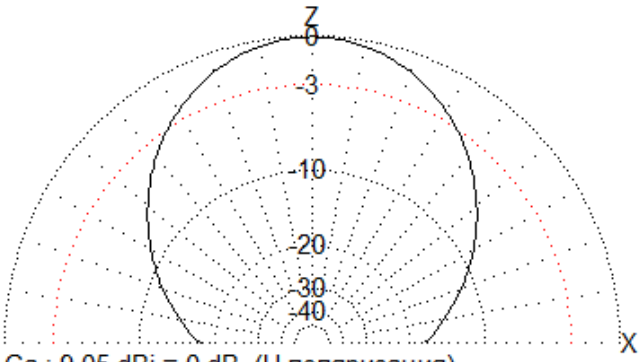


Ga : 13.62 dBi = 0 dB (H поляризация)
Gh : 11.47 dBd
F/B: -8.75 dB; Тыл: Азим. 120 гр, Элевация 60 гр
F: 1800.000 МГц
Z: 20.880 + j62.733 Ом
КСВ: 6.2 (75.0 Ом),

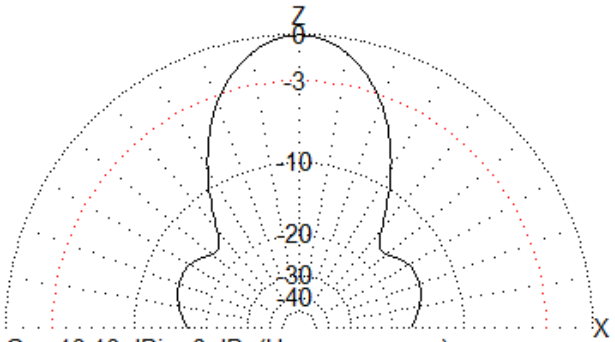


Ga : 12.12 dBi = 0 dB (H поляризация)
Gh : 9.97 dBd
F/B: -4.27 dB; Тыл: Азим. 120 гр, Элевация 60 гр
F: 2100.000 МГц
Z: 142.522 + j147.100 Ом
КСВ: 4.2 (75.0 Ом),

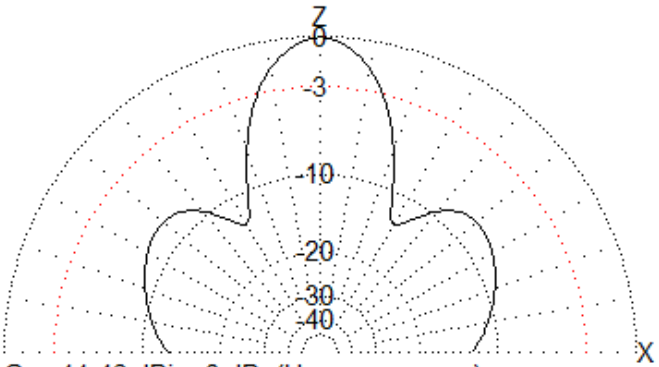
Рис. 2: Характеристики 2-х элементной системы с линейными вибраторами



Ga : 9.05 dBi = 0 dB (H поляризация)
Gh : 6.9 dBd
F/B: -15.07 dB; Тыл: Азим. 120 гр, Элевация 60 гр
F: 750.000 МГц
Z: 218.713 + j105.870 Ом
КСВ: 3.7 (75.0 Ом),

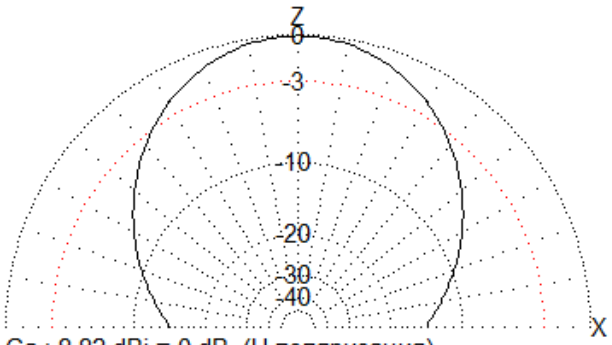


Ga : 13.13 dBi = 0 dB (H поляризация)
Gh : 10.98 dBd
F/B: -8.70 dB; Тыл: Азим. 120 гр, Элевация 60 гр
F: 1800.000 МГц
Z: 83.735 + j71.013 Ом
КСВ: 2.4 (75.0 Ом),

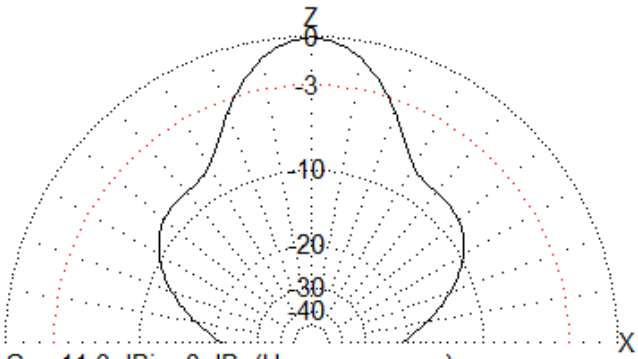


Ga : 11.46 dBi = 0 dB (H поляризация)
Gh : 9.31 dBd
F/B: -5.23 dB; Тыл: Азим. 120 гр, Элевация 60 гр
F: 2100.000 МГц
Z: 96.276 - j19.824 Ом
КСВ: 1.4 (75.0 Ом),

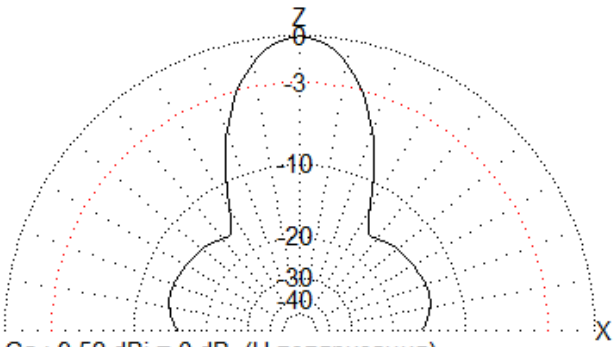
Рис. 3: Характеристики 2-х элементной системы с V-образными вибраторами



Ga : 8.82 dBi = 0 dB (H поляризация)
Gh : 6.67 dBd
F/B: -12.25 dB; Тыл: Азим. 120 гр, Элевация 60 гр
F: 750.000 МГц
Z: 263.748 + j50.955 Ом
КСВ: 3.7 (75.0 Ом),



Ga : 11.3 dBi = 0 dB (H поляризация)
Gh : 9.15 dBd
F/B: -14.36 dB; Тыл: Азим. 120 гр, Элевация 60 гр
F: 1800.000 МГц
Z: 65.739 - j21.987 Ом
КСВ: 1.4 (75.0 Ом),



Ga : 9.58 dBi = 0 dB (H поляризация)
Gh : 7.43 dBd
F/B: -2.57 dB; Тыл: Азим. 120 гр, Элевация 60 гр
F: 2100.000 МГц
Z: 28.618 + j47.560 Ом
КСВ: 3.8 (75.0 Ом),

Рис. 4: Характеристики 2-х элементной системы с фрактальными вибраторами

Анализ полученных результатов позволяет сделать следующее заключение. В ходе моделирования рассматривался достаточно широкий диапазон, с коэффициентом перекрытия равном 2,8. Следует отметить, что в номинальном значении, антенные системы охватывают диапазон работы сетей мобильной связи и широкополосного доступа.

Так, в нижней части (750 МГц) ДН у всех антенных систем примерно одинаковы. Но у 2-х элементной системы с линейными вибраторами величина коэффициента стоячей волны (КСВ) составляет 2.9, при значении комплексного сопротивления $z1 = 74.3 + j82.4$. В то время как у 2-х элементной системы с V-образными вибраторами КСВ равно 3.7, но комплексное сопротивление $z2 = 218.7 + j105.9$. А у 2-х элементной системы с фрактальными вибраторами, соответственно КСВ = 3.7, $z3 = 263.7 + j50.9$.

Так, в средней части (1800 МГц) ДН у 2-х элементной системы с линейными вибраторами разваливается на три лепестка. Причем затухание у крайних лепестков на 15 дБ выше, относительно центрального. У 2-х элементной системы с V-образными вибраторами при таком же уровне затухания, крайние лепестки ДН более локализованы. При том, что у 2-х элементной системы с фрактальными вибраторами уровень по крайним лепесткам составляет всего минус 8 дБ, относительно центрального. А ДН не имеет провалов. Следует отметить, что фрактальная система имеет самый низкий КСВ = 1.4. У 2-х элементной системы с V-образными вибраторамион в 1.7 раза выше, а 2-х элементной системы с линейными вибраторами – в 3 раза.

В верхней части (2100 МГц), наиболее цельная ДН у 2-х элементной системы с V-образными вибраторами, ее КСВ = 1.4. У фрактальной системы КСВ в 2.7 раза выше, а у 2-х элементной системы с линейными вибраторами в 3 раза.

Для повышения надежности результатов, дополнительно были проведены расчеты с использованием компьютерной программыCST MicrowaveStudio. Согласно проведенным расчетам, характеристики ДН по двум компьютерным программам дают примерно одинаковые результаты. В качестве примера, на рис. 5 приведены характеристики излучения той же 2-х элементной антенной системы с фрактальными вибраторами, что и на рис. 4.

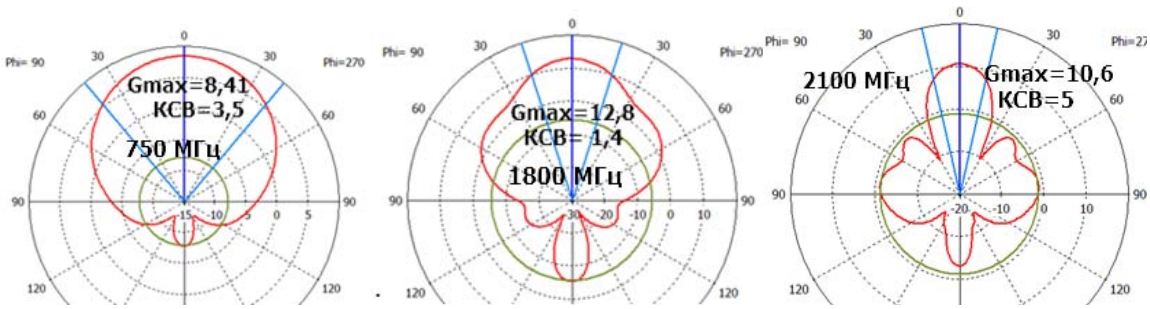


Рис. 5: Характеристики 2-х элементной системы

с фрактальными вибраторами

В целом, все рассмотренные системы не являются оптимальными при работе в таком широком диапазоне частот. Но требования работоспособности сохраняют.

IV. Заключение

В заключении следует подчеркнуть, что коэффициент усиления всех рассмотренных антенных систем лежит в пределах 9…13 дБ. По условию согласования с фидером 75 Ом в диапазоне частот от 750 МГц до 2100 МГцлучшим вариантом является антенная система с *V*-образными вибраторами. Это объясняется тем, что в *V*-образном вибраторе, как и в биконическом, происходит трансформация волнового сопротивления, в результате чего наблюдается компенсация отраженной волны. Вофрактальной системе при увеличении частоты также наблюдается эффект четвертьволнового трансформатора, что приводит к улучшению условия согласования.

Таким образом, можно заключить, что применение фрактальных вибраторов в низкопрофильных антенных системах требует дополнительного согласования с линиями питания элементов системы.

Очевидно, что использованиефрактальных излучателей в низкочастотных диапазонах усложняет конструкцию антенн и снижает их надёжность, поэтому даже с учётом достижения незначительного положительного эффекта применение таких антеннтребует дополнительного обоснования.

Дальнейшие исследования авторы связывают с анализом широкодиапазонных антенн, построенных на основе фрактального синтеза.

СПИСОКЛИТЕРАТУРЫ

1. **Mandelbrot B. B**. Lex objets fractals: Forme, Hasanl el Dimension (Paris: Flammarion, 1975).
2. **Дворников С.В., Сауков А.М.** Метод распознавания радиосигналов на основе вейвлет-пакетов. Научное приборостроение. 2004. Т. 14. № 1. С. 85-93.

3. **Короленко П.В., Мишин А.Ю.** Физические аспекты феномена красоты фракталов. Международный научно-исследовательский журнал. 2019. № 1-1 (79). С. 7-11.
4. **Саяпин В.Н., Дворников С.В., Симонов А.Н., Волков Р.В.** Метод пространственно-временной фильтрации радиосигналов на основе антенных решеток произвольной пространственной конфигурации. Информация и космос. 2006. № 3. С. 83-89.
5. **Нудьга А. А., Савочкин А. А.** Разработка фрактальной антенны круговой поляризации. СВЧ-техника и телекоммуникационные технологии. 2020. № 1-1. С. 235-236.
6. **Ландышев Ф.А.** Анализ подходов к разработке фрактальных антенн для решения задач беспроводной связи. Инженерные кадры - будущее инновационной экономики России. 2020. № 3. С. 75-78.
7. **Айкашев П.В**. Методы фрактальной геометрии в теории антенн. Modern Science. 2020. № 10-1. С. 362-369.
8. **Бойков И.В., Айкашев П.В.** К вопросу об анализе и синтезе фрактальных антенн. Известия высших учебных заведений. Поволжский регион. Технические науки. – 2018. – № 1 (45). С. 92–110.
9. **Крупенин С.В.** Моделирование фрактальных антенн. Радиотехника и электроника. 2006. Т. 51. № 5. С. 561-568.
10. **Dvornikov S.V., Dvornikov S.S., Kriachko A.F.** Digital synthesis of signals with a low level of manifestation of edge effects. Всборнике: 2020 Wave Electronics and its Application in Information and Telecommunication Systems, WECONF 2020. 2020. С. 9131500.
11. **Власенко В.И., Дворников С.В.** Двухполяризационная антенна для базовой станции подвижной радиосвязи. Телекоммуникации. 2021. № 5. С. 8-16.
12. **Евтихиев (ст.) Н.Н., Засовин Э.А., Кравченко В.Ф., Соколов А.В.** Моделирование фрактальных антенн. Радиотехника. 2007. № 9. С. 14-18.
13. **Виноградов, А. Ю., Кабетов Р.В., Сомов А.М.** Устройства СВЧ и малогабаритные антенны : Учеб.пособие для вузов под ред. А. М. Сомова. – М. : Горячая линия – Телеком, 2012. 440 С.
14. **Гончаренко И.В.** Антенны КВ и УКВ (Компьютерное моделирование) М. ИП Радио Софт, 2004. 124 С.
15. **Ефремова, А. О.** Применение фрактальных антенн для беспроводных широкополосных сетей четвертого поколения / А. О. Ефремова, О. А. Белоусов, С. Н. Калашников, О. А. Казарян // Вопросы современной науки и практики. Университет им. В. И. Вернадского. – 2014. – № 3 (53). С. 56–61.
16. **Кравченко В.Ф., Масюк В.М**. Современные методы аппроксимации в теории антенн. Кн. 3. Новый класс фрактальных функций в задачах анализа и синтеза антенн. Радиотехника, М:, 2002. 75 С.
17. **Дворников С.В., Власенко В.И.** Энергетический расчет радиолиний военного назначения: Учеб.пособие. – СПб.: ВАС, 2020. 180 С.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 22 Issue 1 Version 1.0 Year 2022
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Website Text Translation and Image Translation from a URL using Optical Character Recognition (OCR)

By A.H.M. Saiful Islam, Eshita Agnes Purification, Fahima Akter Anni & Kishor K. Baroi

Notre Dame University

Abstract- Now-a-days we are almost completely dependent on information system for our day-to-day work. Almost every organization of different sectors has their own website. These websites are visited not only by the native people but also by the foreigners. But sometimes they are unable to do so because of language barrier. At present, many translating tools are available but they are either for translating text of a website or translating text from an image. At some cases people have to copy the text and then translate it separately which is a lot of hassle and time consuming. We aim to implement a website translator which will take the URL of any website and translate it in any language. It can also translate the text of the images of that website. We have also created some more new algorithms for URL translation, English to Bangla number translation and English to Arabic number translation.

GJCST-E Classification: I.7.5

WEBSITETEXTTRANSLATIONANDIMAGETRANSLATIONFROMAURLUSINGOPTICALCHARACTERRECOGNITIONOCR

Strictly as per the compliance and regulations of:

Website Text Translation and Image Translation from a URL using Optical Character Recognition (OCR)

A.H.M. Saiful Islam [α], Eshita Agnes Purification [σ], Fahima Akter Anni [ρ] & Kishor K. Baroi [ω]

Abstract- Now-a-days we are almost completely dependent on information system for our day-to-day work. Almost every organization of different sectors has their own website. These websites are visited not only by the native people but also by the foreigners. But sometimes they are unable to do so because of language barrier. At present, many translating tools are available but they are either for translating text of a website or translating text from an image. At some cases people have to copy the text and then translate it separately which is a lot of hassle and time consuming. We aim to implement a website translator which will take the URL of any website and translate it in any language. It can also translate the text of the images of that website. We have also created some more new algorithms for URL translation, English to Bangla number translation and English to Arabic number translation.

I. Introduction

We live in a world of information system at present. We are very dependent to various websites for information about almost everything. For this purpose, people all over the world goes through numerous websites every day. But all websites are not available in their native languages. Around 75% of the world's population does not speak in English according to BBC - UK report1[2]. Here comes the need for translating the contents of the websites. Also, sometimes the images of the websites contain texts which are also need to be translated.

Google translator is widely used for this translation purpose. It can translate texts of any websites using the url of the website. But it doesn't translate the texts inside the images of that website. If anyone searches for an educational website and there is an image of a notice, he/she will not be able to read it as it won't be translated using google translator.

For image translation there are also many apps and websites which are widely used to translate the texts inside of an image to any desired language. But they only deal with images. OCR (Optical Character Recognition) is widely used for the image translation method. It is a technology that recognizes text within a digital image [4]. It is commonly used to recognize text in scanned documents and images [4].

In our work, we tried to create a platform where the users will be able to translate the whole website in any language using the URL and they will also be able to translate the image texts too.

We have also created a platform which will convert random images where the numbers will also be translated from English to any languages. We worked with only Bangla and Arabic numbers here. But English numbers can also be translated to other language numbers too only by editing the algorithm we created.

We organized this paper in this way:

Section

1. Gives the introduction of our work, section.
2. Eplains the implementation details of our website, section.
3. Includes the three algorithms we created, section.
4. Presents the outcomes of the experiments, as well as a comparison to the current procedures and the last section.
5. Contains the conclusion and future work.

II. Implementation Details

In our work, we create three types to translate such as website URL translation, image URL translation and image file (.png or .jpg) translation. Firstly, for website URL translation, we take a website URL as input to call that website from google website and run in our website along with a translation tool to translate that website in any language we want and we can see as figure 1.

Author α: Notre Dame University. e-mail: saiful@ndub.edu.bd

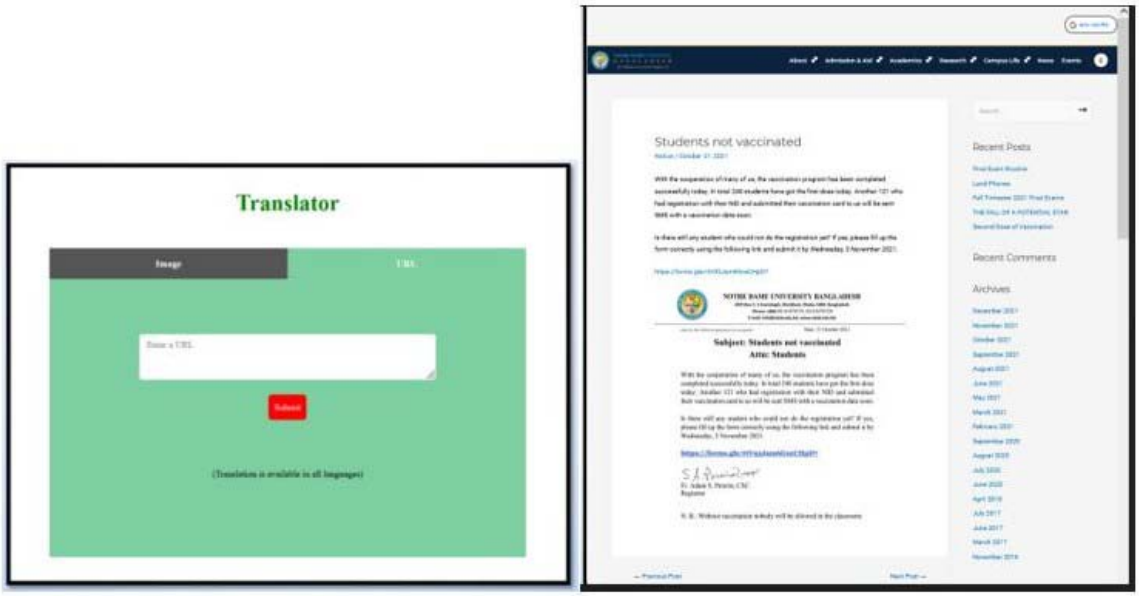
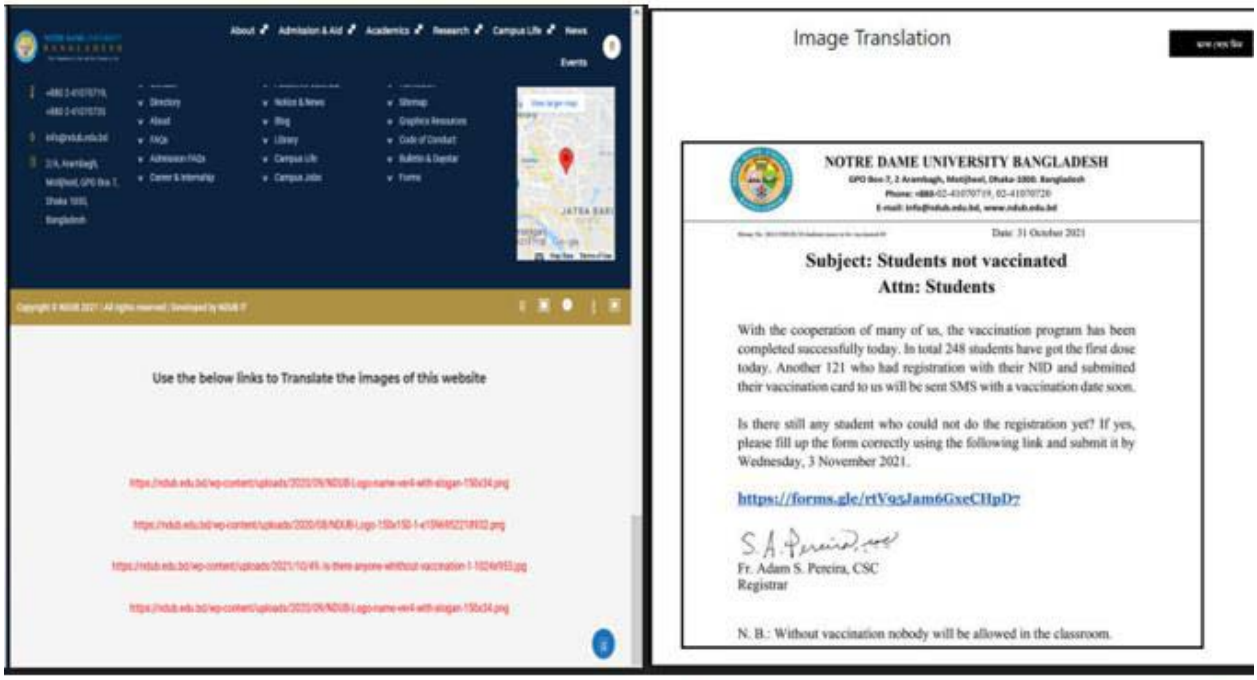


Figure 1: The homepage of the website and the website url to be tested

Secondly, for image URL translation, when we put a website URL and run that in our website it also collects all the image URL that website has and show it at the end of our website. By selecting an image URL, we collect the image from google and convert it to word by using tesseract OCR and save it in a file. After that we call the .txt file and show it to our website. When we select an image URL, we see that .txt file along with the image and translation tool. Now we can translate the image and read the image text in any language. The figure 2 portrays the translation process of the text from an image url. We also show the image text in a format so that it is easy to understand and easy to read.



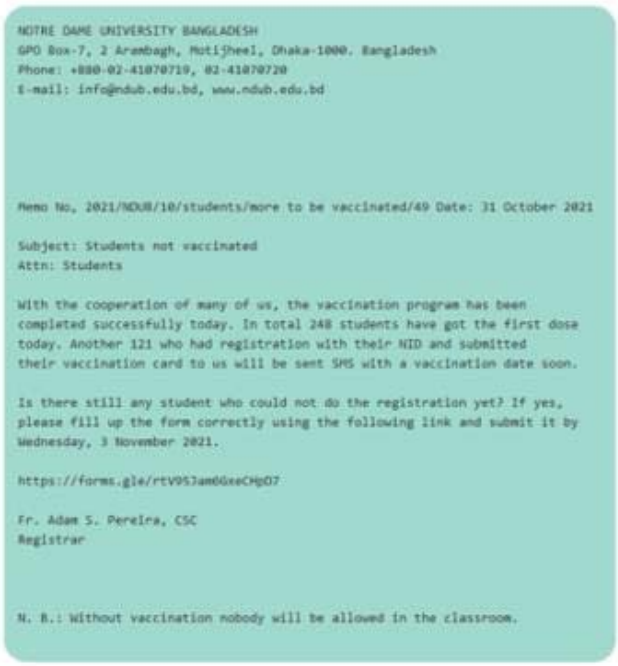


Figure 2: Translation of the text from the image from a website

Lastly, for image translation, we take an image as an input to translate the image text along with numbers. We use our own algorithm to translate the image text and numbers as a sample we use English to Bengali or English to Arabic/Persian Language translation. When we put an image, it converts the image to text and put it in a .txt file. Then using a function to convert the numbers from English to Bengali or Arabic/Persian numbers and show the whole file in our website after converting the numbers and we get the following results in figure 3. And figure 4 shows the translated view of an image sample from English to Bengali and from English to Arabic respectively.

Figure 3: View of the image insert module of the website

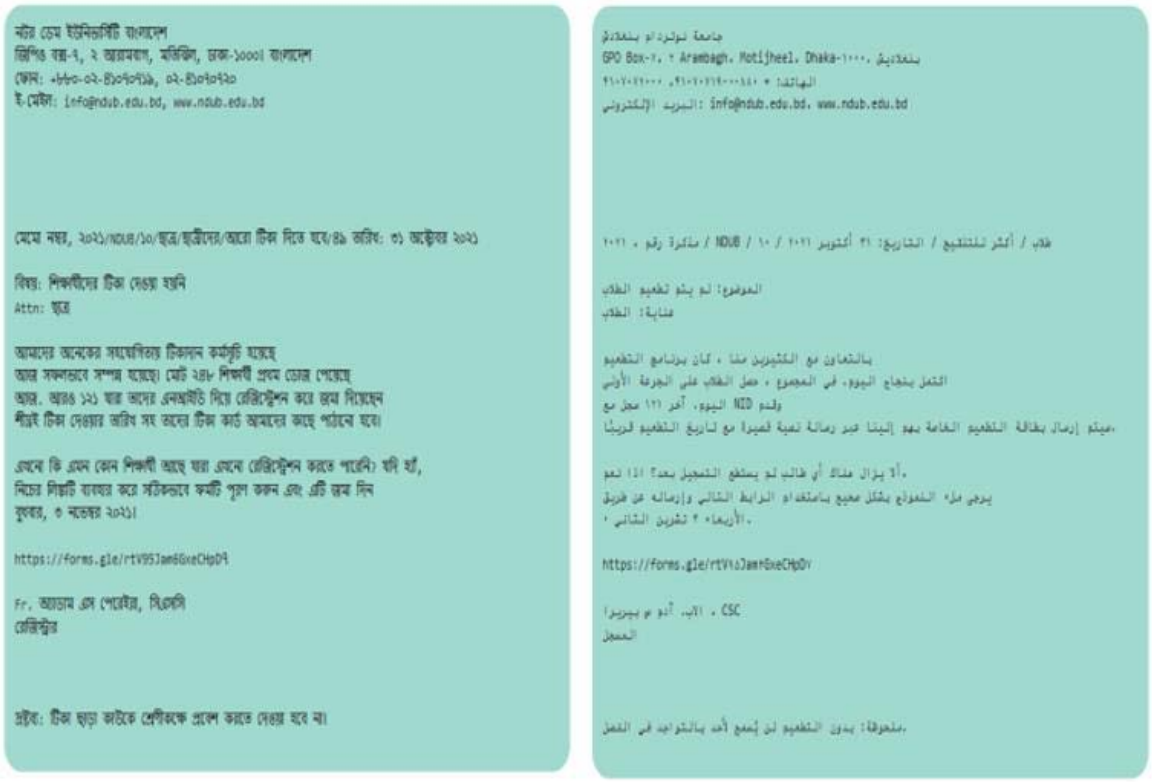


Figure 4: Translated view of the image in Bangla and Persian from English

III. Algorithms

In this section our own algorithms are discussed. We have implemented these three algorithms in our website. Figure shows the first algorithm which is used for translating texts of a random image from English to Bangla.

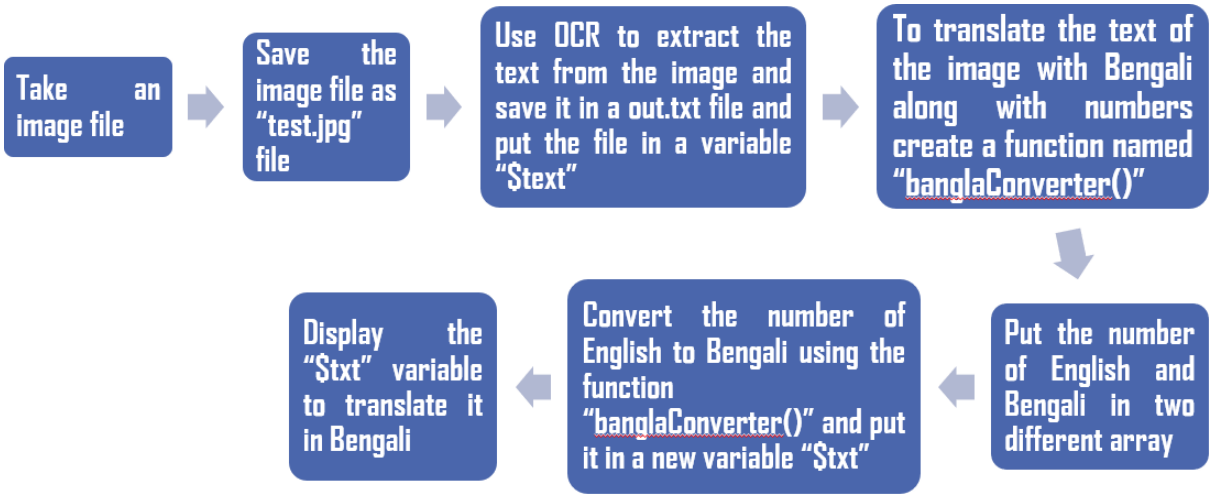


Figure 5: Algorithm to Image Translation (English to Bengali)

Figure 6 describes the algorithm to translate the text of a random image from English to Persian.

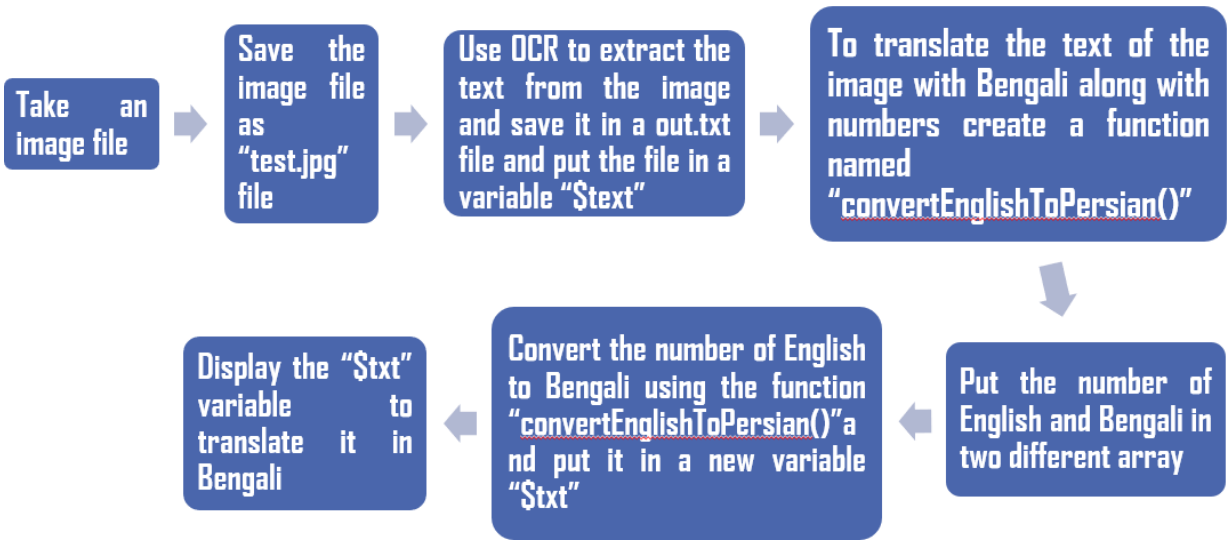


Figure 6: Algorithm to Image Translation (English to Persian)

Figure 7 describes the algorithm to translate the text of an image from a website url from English to any language.

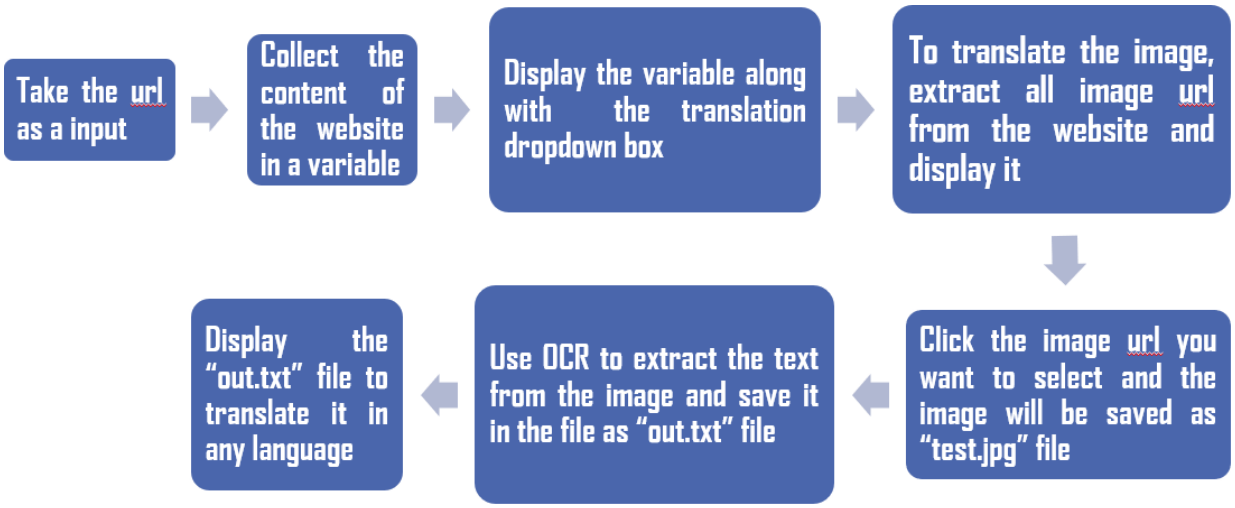


Figure 7: Algorithm for URL Translation

IV. Results Analysis

This section describes the results of our works. In all three sectors of our work, we used the term Accuracy to calculate the performance of them.

Accuracy: It is defined as the ratio of translated words and total words. Here w is the number of properly translated words, and W is the number of total words.

$$\text{Accuracy} = w / W$$

We have experimented Up to 70 websites and up to 50 random images with our approach. Our website reaches almost 83 percent accuracy in the field of website translation and 85 percent in the field of translation of images from those websites. The accuracy of the translation of the random images from English to Bangla reaches 98 percent and from English to Persian it reaches almost 93 percent. We tested this approach with various text fonts, and our website accurately translated them all.

V. Conclusion and Future Work

We have implemented an easier and user-friendly website which takes an url as input and translate the website in any desired language. Using this platform, users will be able to get the information of any website in their comfortable language and it is also time-saving as it translates any website using only a URL. It also translates the texts inside the images of the website. The users are also able to extract the texts of a random image and we have used our own algorithm to translate the English numbers to Bangla and Arabic numbers.

In future, this paper will be helpful to build a mobile application where one can add camera module to take an image and translate it through the app where they can translate numbers too. This paper can also help to build an app or a website that will be able to take any url from any barcode and translate both the text and images. In future this paper will be helpful to create a new algorithm to translate text of all the images of the website in a single webpage along with the web text just like the original website.

References Références Referencias

1. Shruthi Kubatur, Suhas Sreehari, Rajeshwari Hegde "An Image Processing Approach to Linguistic Translation", Dept. of Electrical & Computer Engg, University of Windsor, Windsor, Canada Dept. of Telecommunication Engg, B.M.S. College of Engineering, Bangalore, India, December 2011.
2. Rijwan Khan, Aryan Kaushal, Ayush Agarwal, Avdhesh Kumar "Tourist's Translator based on Digital Image Processing and Hybrid Translation", International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-9 Issue-5, March 2020.
3. G. R. Hemalakshmi, M. Sakthimanimala, J. Salai Ani Muthu "Extraction of Text from an Image and its Language Translation Using OCR", International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), ISSN: 2394-2320, Volume-4 Issue-4, April 2017.
4. https://www.necc.mass.edu/wp-content/uploads/accessible-media-necc/uncategorized/resources/What-is-OCR.pdf.
5. Azmi Can Özgen, Mandana Fasounaki, Hazim Kemal Ekenel, "Text detection in natural and computer-generated images" 2017.
6. R. Smith, "An overview of the Tesseract OCR engine", Document Analysis and Recognition 2007. ICDAR 2007. Ninth International Conference on, vol. 2, pp. 629- 633, 2007, September.
7. A. Canedo-Rodriguez, S. Kim, J. H. Kim, and Y. Blanco-Fernandez, "English to Spanish translation of signboard images from a mobile phone camera," IEEE Southeastcon 2009, Atlanta, GA, 2009, pp. 356-361. DOI: 10.1109/SECON.2009.5174105.
8. Seethalakshmi R., Sreeranjani T.R., Balachandar T., Abnikant Singh, Markandey Singh, Ritwaj Ratan, and Sarvesh Kumar, "Optical Character Recognition for printed Tamil text using Unicode," Journal of Zhejiang University SCIENCE, ISSN 1009-3095, 2005.
9. S.K, Vijaya Kumar, et al., "FLD based Unconstrained Handwritten Kannada Character Recognition," International Journal of Database Theory and Application, December 2000.
10. Pratik Madhukar Manwatkar, Dr. Kavita R. Singh, "A technical review on text recognition from images," IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO), 2015.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 22 Issue 1 Version 1.0 Year 2022
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Performance Evaluation for Ad hoc Routing Protocol in Vehicular Ad hoc Network (VANET)

By Dr. Gurjeet Singh
MK Group of Institutes

Abstract- In this paper we researched about different ad hoc routing protocols for VANET. The main aim of our study was to identify which ad hoc routing technique has better execution in highly mobile environment of VANET. To measure the performance of routing protocols in VANET, we considered two different situations i.e. city and highway. Routing protocols were selected carefully after carrying out literature review. The selected protocols were then evaluated through simulation in terms of performance metrics i.e. throughput and packet drop. From results, we observe that A-STAR shows better performance in form of high throughput and low packet drop as compare to AODV and GPSR in city environment, while GPSR shows better performance as compare to AODV in both highway and city environment of VANET.

Keywords: *VANET, routing protocols, MANET.*

GJCST-E Classification: *C.2.2*

Strictly as per the compliance and regulations of:

Performance Evaluation for Ad hoc Routing Protocol in Vehicular Ad hoc Network (VANET)

Dr. Gurjeet Singh

Abstract- In this paper we researched about different ad hoc routing protocols for VANET. The main aim of our study was to identify which ad hoc routing technique has better execution in highly mobile environment of VANET. To measure the performance of routing protocols in VANET, we considered two different situations i.e. city and highway. Routing protocols were selected carefully after carrying out literature review. The selected protocols were then evaluated through simulation in terms of performance metrics i.e. throughput and packet drop. From results, we observe that A-STAR shows better performance in form of high throughput and low packet drop as compare to AODV and GPSR in city environment, while GPSR shows better performance as compare to AODV in both highway and city environment of VANET.

Keywords: VANET, routing protocols, MANET.

I. Introduction

VANET is a specific instance of remote multihop network, which has the imperative of quick geography changes because of the great hub portability. With the increasing number of vehicles equipped with computing technologies and wireless communication devices, inter vehicle communication is becoming a promising field of research, standardization, and development. VANETs empower a wide scope of utilizations, for example, counteraction of crashes, security, blind intersection, dynamic course planning, continuous traffic condition checking. Another important application for VANETs is providing Internet connectivity to vehicular nodes. Figure 1 shows an example of a VANET. Because of high portability, successive changes in geography and restricted life time are such attributes of this network that settle on steering choices really testing. A few different factors, for example, street design and various conditions, for example, city and roadway makes directing more testing in VANET. As opposed to topology based routing of MANET, VANET uses position information of the participating nodes within the network to take routing decisions. Further we will discuss how position based routing used for VANET.

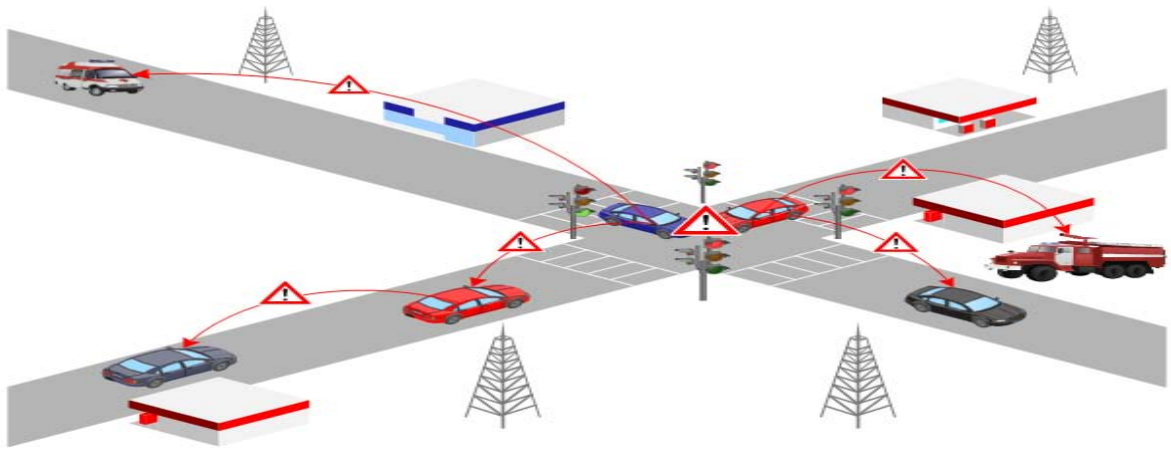


Figure 1: Example of VANET

II. Routing in Vanet

VANET uses position information of the participating nodes within the network to take routing decisions. Further we will discuss the routing used for VANET.

a) Position Based Routing (PBR)

The dynamic and profoundly versatile nature of VANET, where hubs act exceptionally quick and changes its area as often as possible requests such routing technique that can manage the climate of such organization. These demands tend the researchers to use positions of nodes in order to provide successful communication from source to destination. Such method in which geographical positions of nodes are used to perform data routing from source to destination

Author: Associate Professor, Department of Computer Science & Engineering, MK Group of Institutes, Amritsar.
e-mail: hi_gurjeet@rediffmail.com

is called position based routing. Position based routing accepts that every hub know about its physical/geographic situation by GPS or by some other position deciding administrations. In it each node also has the knowledge of source, destination and other neighboring nodes. As compared to topology based routing, position based routing uses the additional information of each participating node to applicable in VANET, that additional information is gathered through GPS. Position based routing gives hop-by-hop communication to vehicular organizations. A position based steering convention comprises of many significant parts, for example, "beaconing", "area administration and servers" and "recuperation and sending systems".

- *Beaconing:* In it a node forwards packet with the current physical position and the unique id (IP ADDRESS). If node receives beacon from its neighbor's then it updates its information in location table. Thus beaconing is used to gather information of node's one-hop neighbor or node's next hop neighbor.
- *Location service and servers:* When a node does not contain current physical position of a specific node in its location table or want to know current physical position of any specific node then location service assisted to find current position of a specific node.
- *Forwarding and Recovery strategy:* Forwarding and recovery strategy are used to forward data from source to destination node.

b) Greedy Perimeter Stateless Routing (GPSR)

Greedy Perimeter Stateless Routing (GPSR) is one of the best examples of position based routing. GPSR involves nearest neighbor's data of objective to advance bundle. This technique is otherwise called ravenous sending. In GPSR every hub knows about its present actual position and furthermore the adjoining hubs. The knowledge about node positions provides better routing and also provides knowledge about the destination. Then again adjoining hubs likewise helps to settle on sending choices all the more accurately without the impedance of topology data.

c) Geographic Source Routing (GSR)

Because of lacks of GPSR in presence of radio obstructions, network requested new steering procedures that can contend with moves occured because of radio deterrents. Along these lines, Geographic Source Routing (GSR) is proposed. It manages high versatility of hubs on one hand, then again it utilizes streets design to find courses. GSR finds the destination node using "Reactive Location Service (RLS)". GSR combines both geographic routing and road topology knowledge to ensure promising routing in the presence of radio obstacles.

d) Anchor-based Street and Traffic Aware Routing (A-STAR)

Anchor-based Street and Traffic Aware Routing (A-STAR) is position based directing protocol. The improvement of A-STAR was inconsideration with city climate. In city area, almost all roads and streets are covered by big buildings and there are close ends in the streets and so frequent stop signal, turns and speed breakers make routing more challenging. Problems faced by the position based routing protocols in city environment defined before in GSR. The capability of A-STAR protocol to overcome these problems will be defined here. A-STAR is anchor based routing protocol. In anchor based routing before to communicating the packet, source hub address include the header of packet and data of all middle hub intersection that parcel should venture out to arrive at the destination. To use city maps and road information of town to make routing decisions called "Spatial Aware Routing". Spatial awareness is used to get topology information and different nodes position in the network.

III. Simulation Model

Simulation is the procedure of taking care of issues by the perception of the exhibition, throughout the time, of a powerful model of the framework. Reproduction for the most part addresses the connection between the frameworks and models. A framework is the collection of parts that are interrelated and associated so that it recognizes the framework from its current circumstance.

a) Performance Metrics

In this paper we have selected throughput and packet drop to check the performance of VANET routing protocols against each other. The justification for the choice of these presentation measurements is to really take a look at the exhibition of steering conventions in exceptionally versatile climate of VANET. Moreover, these performance metrics are used to check the effectiveness of VANET routing protocols.

b) Implementation

In this step we produce the simulation results and run simulation for two unique situations to assess the presentation of routing protocols for VANET as far as various execution boundaries that is throughput and packet drop. We designed two unique networks for these situations the two of them comprises of vehicular hubs.

i. *Highway Scenario*

The highway situation we chose 25 hubs with the total area of 1400 x 700 meters. Distances between the vehicles are arbitrarily chosen. In first case, vehicles move with most extreme speed of 25 m/s and in later case vehicles move with speed of 30 m/s. All out reenactment time for every situation is 450 seconds. The

motivation of simulation for highway situations is to check the conduct of AODV and GPSR routing protocols for VANET as far as throughput and packet drop.

Table 1: Input parameter for highway scenario

Parameter	Setting
Environment size	1400 x 700 meters
Total no of nodes	25
Node Type	Highly Mobile nodes
Node Speed	25 m/s
Packet Type	UDP
Packet Size	1400 Bytes
Simulation Time	300 seconds
No of Receiver	One

In this situation every simulation was performed for 300 seconds. 25 nodes (vehicles) were chosen as the members of organization and every node development was profoundly portable. Every node furnished with 802.11b wireless module for communication with different nodes. Nodes move with speed of 25 m/and 30 m/s. In this simulation AODV and GPSR routing protocols were chosen for simulation and their performance will be checked as far as throughput and packet drop.

a. *Throughput*

Throughput is the normal number of effectively delivered data packets on a communication network or organization node. At the end of the day throughput portrays as the all out number of received packets at the objective out of complete sent packets. Throughput is calculated in bytes/sec or information packets per second.

$$\text{Throughput (bytes/sec)} = \frac{\text{Total number of received packets at destination} * \text{packet size}}{\text{Total simulation time}}$$

If network throughput is high it means most of the sent packets to destination has been received, thus this factor reduce delay as packet receive success rate is high.

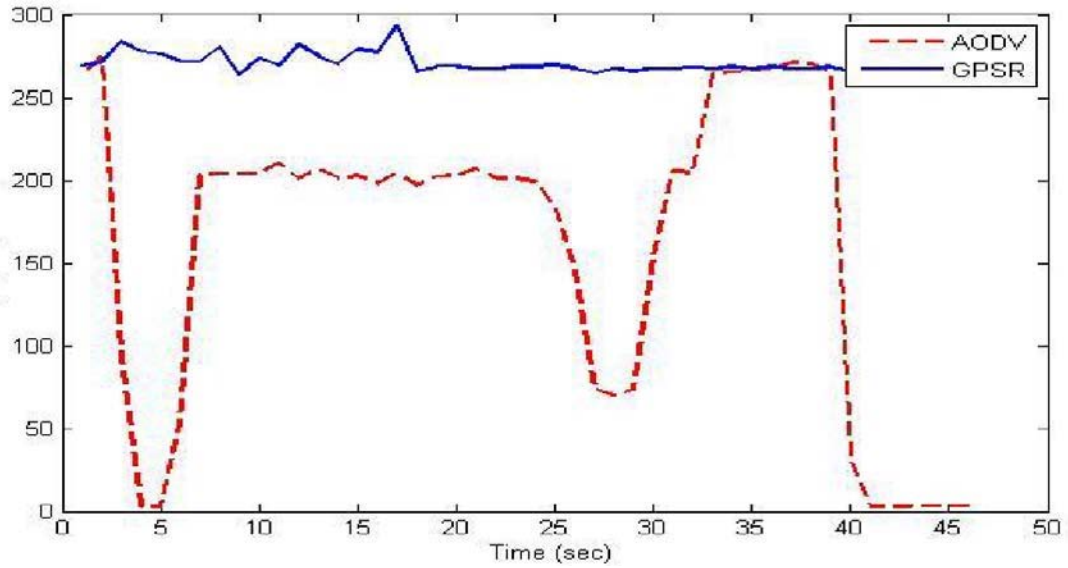


Figure 2: Throughput with 25 m/s node speed

Figure 2 depicts the organization throughput of AODV and GPSR routing protocols with the node speed of 25m/s on highway. For this situation we can see that AODV throughput rate begins with the roughly 275 Kbytes/sec and inside matter of seconds the throughput rate tumble to the least level for example roughly 5 KB/sec. In spite of the fact that AODV is one of the most amazing illustration of receptive routing techniques yet in the profoundly mobile environment of VANET its performance decline abruptly to the least level as far as throughput. AODV throughput rate become higher after some time and maintain its throughput rate for some time this is due to the feature of AODV in which it repeatedly sent the request for forwarding packets towards destination but its disadvantage is that it uses more network resources to resend the route request. As compared to AODV, GPSR shows higher throughput rate in entire simulation time. GPSR throughput rate in the highly mobile environment of VANET is constant. GPSR uses greedy forwarding with the combination of perimeter forwarding to ensure maximum delivery of packets at destination.

b. *Packet Drop*

Packet drop shows total number of data packets that could not reach destination successfully. The reason for packet drop may arise due to congestion, faulty hardware and queue overflow etc. Packet drop affects the network performance by

consuming time and more bandwidth to resend a packet. Lower packet drop rate shows higher protocol performance.

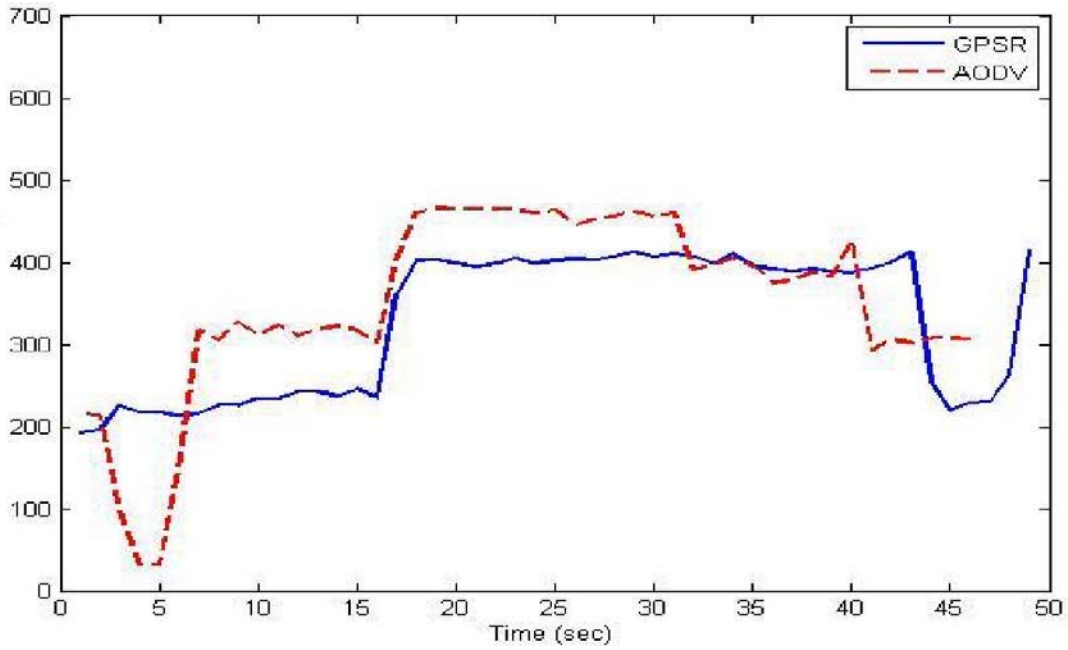


Figure 3: Packet Drop at 25 m/s node speed

Figure 3 shows behavior of AODV and GPSR as far as packet drop at most extreme node speed of 25 m/s. For AODV routing protocol the bundle drop rate for initial 5 seconds diminished from approx 225 to 25 parcels. However, this decline in packets is just briefly and in a matter of moments the packet drop proportion of AODV becomes higher to 300 bundles drop and it bit by bit increment with the time. The reason for the higher packet drop in AODV is expected to the multi-bounce nature of the organization.

In this way in highway situation with the nodes most extreme speed of 25 m/s there is just a slight distinction in AODV and GPSR in term of packet drop proportion. In general in this situation GPSR has dropped lower number of parcels when contrasted with AODV. Besides, in thruway situation we determined just those drop bundles that lost between the last moderate hub to objective. Consequently, in the present circumstance a throughput and drop bundles don't have any immediate connection.

ii. *City Scenarios*

An organization to actually take a look at execution of routing protocols within the sight of various radio impediments for example (totally block signals, for example, structures and so forth The primary intend to plan this organization is to check how unique directing conventions experienced the radio snags and which steering convention has better adaptability in city streets.

In this scenario each simulation were performed for 300 seconds. 25 nodes (vehicles) were selected randomly and each vehicle equipped with IEEE 802.11 (b) wireless module. Nodes move with maximum speed of 10 km/h. 1500 meters of total simulation area were selected. 15 different completely block radio obstacles (consider them as buildings etc) were placed aside the roads to interrupt the communication. In this scenario A-STAR, GPSR and AODV routing protocols were selected to check their performance in terms of throughput and packet drop. Each input parameter for city scenario is shown in the following table:

Table 2: Input parameter for city scenario

Parameter	Setting
Environment Size	1500 meter
Total no of nodes	25
No of radio obstacles	15
Node Type	Highly mobile nodes
Node Speed	10 m/s
Packet Type	UDP
Packet Size	1200 bytes
Simulation Time	300 seconds
No of Receiver	One

a. *Throughput*

Figure 4 shows performance of AODV, GPSR and A-STAR as far as throughput within the sight of radio obstructions at city streets. AODV begins with the high throughput rate yet inside a few seconds its throughput rate significantly diminished to nothing.

Furthermore, there was sudden rise and fall in the throughput rate and at approximately 25 seconds throughput rate of AODV suddenly reached at the maximum level where the throughput rate was 300 KB/sec but this rate only for couple of seconds then its again dramatically decreased to zero and for the rest of communication there was only a short increase in the AODV throughput.

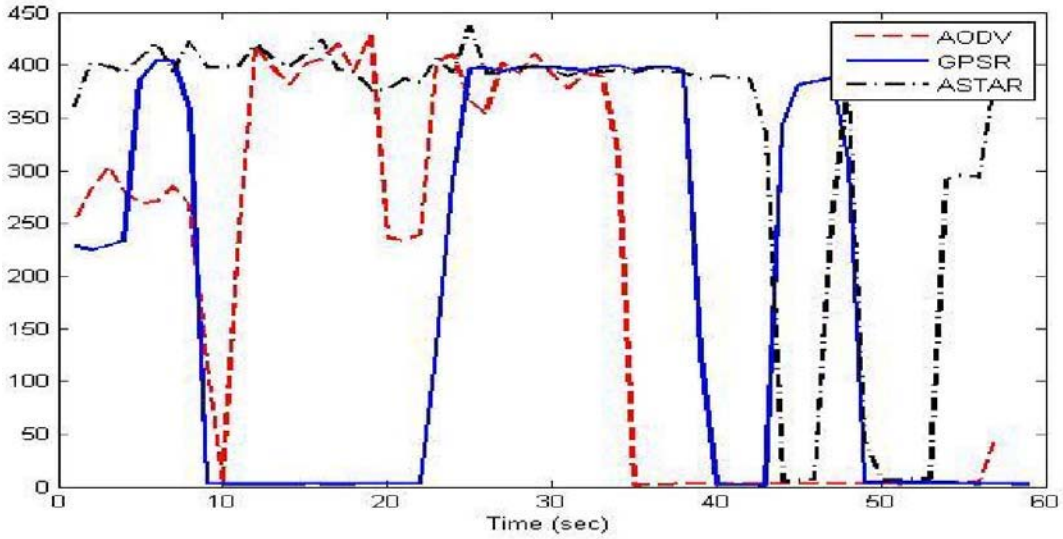


Figure 4: Throughput in City Scenario

On the other hand GPSR shows the average throughput results in the city scenario. There were also some dramatically changes in the performance of GPSR shown in Figure 4. Although GPSR is a position based routing protocol but its performance was average and at some level throughput rate reduced to zero.

On the whole it can be concluded that A-STAR has better performance in terms of throughput as compared to GPSR and AODV where there is number of obstacles interrupt the communication. Furthermore, GPSR outperformed AODV in terms of throughput.

b. *Packet Drop*

The normal number of dropped packets by AODV, GPSR and A-STAR routing protocols within the sight of deterrents. Figure 5 shows unsteadiness in the exhibition of every one of the three routing protocols as far as packet drop. AODV packet drop rate was high than GPSR and A-STAR. While AODV showed unforeseen outcomes in the enormous city conditions by dropping less number of packets for the initial 25 seconds. As distance between the nodes with in the city environments are less and also the vehicles moved with low speed that is why AODV successful to deliver some packets to the destination as it received RREP from the closed nodes immediately. But this low drop packet rate only for the short time interval after some time AODV had highest number of dropped packets, it may due to the communication obstacles between the nodes.

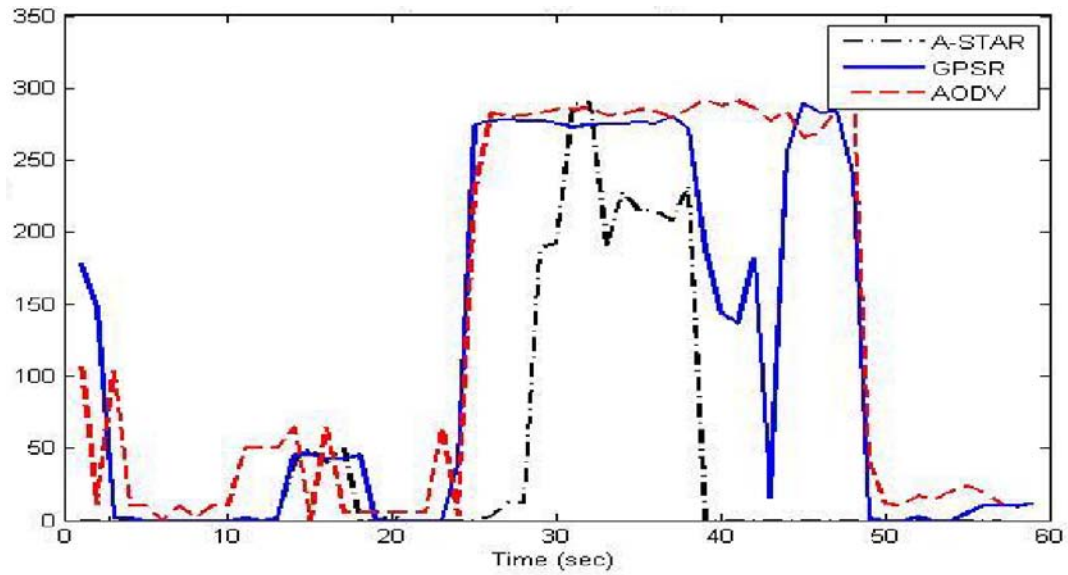


Figure 5: Packet Drop in city scenario

A-STAR has less number of drop packets at the start but there was sudden change in its performance and number of drop packets increased. Sudden increment in drop packet rate may be due to the packet traverse to such anchor path that is temporarily marked as "out of service" by A-STAR.

IV. Conclusion

It was observed that position based routing protocols shows preferable outcomes over customary specially appointed adhoc routing protocols in VANET. We evaluate two position based routing protocols that are GPSR and A-STAR in two unique situations of VANET. GPSR beats AODV totally in both roadway and city conditions of VANET. While GPSR affected with the involvement of obstacles in the large city environments. On the other hand A-STAR outperforms both GPSR and AODV in city environments of VANET. As A-STAR uses the anchored based street information to find the routes in large city 52 environments, therefore it is not an alternative for highway scenarios. So we understood that A-STAR is versatile for such conditions of VANET where quantities of hubs are higher and radio obstructions required, while GPSR is solid for direct correspondence among nodes. Besides, all position based routing protocols can't manage all different conditions of VANET.

References Références Referencias

1. S.-Y. Wang and C.-L. Chou., "NCTUns Simulator for Wireless Vehicular Ad Hoc Network Research" In J. N. Turner and C. S. Boyer, editors, Ad Hoc Networks: New Research. Nova Science Publishers, 2009.
2. B.-C. Seet, G. Liu, B.-S. Lee, C. H. Foh, K. J. Wong, K.-K. Lee, "A-STAR: A Mobile Ad Hoc Routing Strategy for Metropolis Vehicular Communications". NETWORKING 2004.
3. Tee, C.A.T.H.; Lee, A.C.R., "Survey of position based routing for Inter Vehicle Communication system", Distributed Framework and Applications, 2008. DFmA 2008. First International Conference on, pp.174-182, 21-22 Oct. 2008.
4. Takano, A.; Okada, H.; Mase, K., "Performance Comparison of a Position-Based Routing Protocol for VANET", Mobile Adhoc and Sensor Systems, 2007. MASS 2007. IEEE Internatonal Conference, pp.1-6, Oct. 2007.
5. Shrestha, Rakesh, Rojeena Bajracharya, and Seung Yeob Nam. "Challenges of future VANET and cloud-based approaches." Wireless Communications and Mobile Computing 2018 (2018).
6. Liang, Wenshuang, Zhuorong Li, Hongyang Zhang, Shenling Wang, and Rongfang Bie. "Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends." International Journal of Distributed Sensor Networks 11, no. 8 (2015): 745303.
7. Kumar, Vishal, Shailendra Mishra, and Norottam Chand. "Applications of VANETs: present & future" Communications and Network, 5, no. 01(2013):12.
8. Kelareshtaghi, kavehBaksh, et al. "survey on vehicular adhoc networks and its access Technologies Security Vulnerabilities and Countermeasures." arXiv preprint arXiv:1903.01541 (2019).
9. S. Zeadally, RHunt, Y-S. Chen, A, Irwin, A. Hassan. "vehicular adhoc Networks:status, Results, Challenges" Springer Science, 2010.
10. Kaur, R., Singh, T. P. & Khajuria, V. (2018, May). "Security issues in vehicular ad-hoc network (VANET). In 2018 2nd International conference on trends in Electronics and Informatics (ICOEI), pp.884-889.IEEE, 2018.
11. M. Raya, P. Papadimitratos, and JP. Hubaux, "Securing vehicular communications," IEEE Wireless Communication., vol.13, no.5, pp.8-15, oct 2006.
12. Salem, Ahmed H., Ayman Abdel-Hamid, and Mohamad Abou El-Nasr." The case for dynamic key distribution for PKIbased VANETS." arXiv preprint arXiv: 1605.04696 (2016).
13. Qu, Fengzhong, Zhihui Wu, Fei-Yue Wang, and Woong Cho. "A security and privacy review of VANETs." IEEE Transactions on Intelligent Transportation Systems 16, no. 6 (2015): 2985-2996.
14. Laberteaux, K. P., Hu, Y. C., & Haas, J. (2016). U.S. Patent No. 9,461,827. Washington, DC: U.S. Patent and Trademark Office.

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 22 Issue 1 Version 1.0 Year 2022
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

"TrustPass" – Blockchain based Trusted Digital Identity Platform towards Digital Transformation

By Kalpa Dissanayake, Pavan Somarathne & Ushan Fernando
Sri Lanka Institute of Information Technology

Abstract- According to the United States Census Bureau, by June 2019 world population on earth was 7.5 billion, which exceeds the world population of 7.2 billion as of 2015. Each of these citizens needs to prove their identity in order to fulfill their day-to-day routine. In this current digital revolution whole world is transforming to digitalization. Therefore, proving someone's identity in the digital space is a must, because being able to track a person digitally can result in elimination of the identity theft and most incidents related to online harassments, while focusing on data privacy and security of citizens, we have proposed ''Trust Pass'': Cyber Security Intelligence based trusted digital identity platform capable of registering and verifying service providers based on document validation neural network model (95.4% accuracy) and allowing citizens to authenticate themselves to service providers with three factor biometrics authentication with liveness detection neural network model (99.8% accuracy).

Keywords: *cyber security intelligence, blockchain, cyber threat, three-factor biometric, data security and privacy, digital identity, neural networks.*

GJCST-E Classification: *I.3.5*

Strictly as per the compliance and regulations of:

"TrustPass'' – Blockchain based Trusted Digital Identity Platform towards Digital Transformation

Kalpa Dissanayake [α], Pavan Somarathne [σ] & Ushan Fernando [ρ]

Abstract- According to the United States Census Bureau, by June 2019 world population on earth was 7.5 billion, which exceeds the world population of 7.2 billion as of 2015. Each of these citizens needs to prove their identity in order to fulfill their day-to-day routine. In this current digital revolution whole world is transforming to digitalization. Therefore, proving someone's identity in the digital space is a must, because being able to track a person digitally can result in elimination of the identity theft and most incidents related to online harassments, while focusing on data privacy and security of citizens, we have proposed ''Trust Pass'': Cyber Security Intelligence based trusted digital identity platform capable of registering and verifying service providers based on document validation neural network model (95.4% accuracy) and allowing citizens to authenticate themselves to service providers with three factor biometrics authentication with liveness detection neural network model (99.8% accuracy). The requests of the whole system are secured with Cyber Security Threat Intelligence System and unusual activities of users are monitored through Informative Data Analytics Engine. All the sensitive user data is being saved using a blockchain to ensure user privacy while reducing the system open to vulnerabilities.

Keywords: cyber security intelligence, blockchain, cyber threat, three-factor biometric, data security and privacy, digital identity, neural networks.

I. Introduction

In day-to-day life verifying our identity or proving who we are is an inevitable factor. [1] Every Sri Lankan citizen should have a valid document with them that can prove their identity at all times. In Sri Lanka every citizen who is above 16 years of age must obtain a National Identity Card which can prove their identity anywhere in the country. [1] By the age of 18 citizens can apply for the driving license card which also can be used as a proof of identity. Furthermore, citizens can obtain and use their passport as a proof of identity as well. According to our survey [2] most people in Sri Lanka use their National Identity Card as their proof of identity. However, when entire world is moving towards a digital transformation being able to prove our identity remotely will give us a huge advantage. In traditional document-based identity proving system we can't do remote verifications to prove our identity we must physically present with our id document to prove our identity. This can be very troublesome on many occasions. according to our survey [2], clear majority of Sri Lankan citizens prefer to get services that require identity verifications via online remote delivery method rather than spending hours of their valuable time in government or private offices. Currently there is no any system that provide remote identity verifications for citizens of Sri Lanka. Many other countries have developed similar systems.

- Sing Pass in Singapore [3]
- Digital Id in Australia [4]
- Accenture KTDI in USA [5]
- Yoti in United Kingdom [6]
- SmartID in United Kingdom [7]

Developing a comparable but more locally compatible digital identity system in a developing country like Sri Lanka can be a challenging task. Currently in Sri Lanka only two out of five people has digital literacy [8]. and moreover, Sri Lanka don't have a very sophisticated digital infrastructure. To develop a system that can overcome these challenges and facilitate maximum user convenience, we must study deep into other existing systems and popular research work.

II. Background and Literature Review

a) Service Provider Management with Document Validater

Service Providers or the relying parties (RPs) like examination centers, Banks, Police etc. are one of the most required user groups which we are facilitating the services through our system. According to our survey [2] local and government service providers got very average level of significance because they do not have the facility to authenticate user details without manual inspection and it takes more time to accommodate the request. Since we are creating a secure, authenticated platform between users and RPs, RPs could be able to develop their performances without wasting users' time.

Because of that RPs need to register to our system to authenticate users through our system to their system. Since we are enabling RPs to register online, they must provide valid documents to Trust Pass system. We are introducing a Image Based Document Validator which can identify invalid document and invalidate the registration without wasting further personal and infrastructure resources in the registration process.

Author: Sri Lanka Institute of Information Technology.
e-mail: it17185394@my.sliit.lk

For the document validator we have created a Convolutional Neural Network (CNN). Performance of the CNN have gained tremendous success within last decades [9]. However, to gain a high accuracy and the performance the architecture of the CNN has a definite impact. On the other hand, we must have a large number of pre classified dataset to get a good output and it prevents the usage of many off the shelf state-of-art CNNS like Alex Net, VGG, ResNet being applied in classification problems and it may affect for the overfitting of the model too [10].

Although there are state-of-art CNNs in the market according to these researches [11] [12] that has been carried our regarding image classification Alex Net is the widely used CNN which has five convolutional layers and 3 fully connected layers.

b) Three Factor Biometric Authentication

On service providers requests citizens should be able to authenticate their details securely because of this implementing a fast, user-friendly, and secure authentication method that can be integrated with any smartphone is a crucial requirement of our system. according to statistics [13] at the end of 2018, more than 60% of smartphones are developed with an integrated fingerprint sensor and the present data suggests that by the 2023, more than 80% of smartphones will have some form of biometric hardware installed. [14]

In this research[15] researchers were able to develop a face detection and recognition system that have an accuracy of 90%. According to their research to achieve a better accuracy and solid reliability they propose to integrate an iris scanner to the system. They have stated that without matching iris data this system is not suitable for use as an authentication method for ATM Machines or other high security systems.

Face Net is a face recognition model developed by google according to their research [16] Face Net is 99.63% accurate in distinguishing different faces and identifying them . Face Net is developed using a deep convolutional network with two different architectures The Zeiler & Fergus type [16] which can have many parameters and large number of Flops [16] and the Inception type [16] which can have few parameters. Zeiler & Fergus is more suitable for run in datacenter while Inception is proposed to run on mobile devices because of less memory usage.

Although accuracy of the biometric is a concern, we are primarily focused on developing a solution that will facilitate maximum security and verify the live presence of the user. According to this study [17]spoofing a 2D (two dimensional) face recognition which only incorporates a selfie camera and no special hardware similar to 3D (three dimensional) face recognition is a fairly easy task, getting access to user's photograph or recorded video clip is enough to launch a presentation attack [18].

c) Blockchain based Cyber Security Inteligence

The identity of living beings on earth depends on the characteristics of the body. The identity of the human body depends on the biological and social nature of the body. People have to deal with different people in their day-to-day activities and personal identity is very important. Humans' physical bodies reflect inherent traits and identities of humans. When a person thinks of himself as Who Am I, personal identity is reflected and this is unique ownership for each person. The characteristic that can be seen here is that the human's identity is indefinite and temporary. This can change over time. What is the answer we can give to the question of whether we were in a certain place, one day? It's really hard. This is due to the lack of definite identity. Therefore, physical identity is studied. Although efforts have been made to identify a person by his appearance, they have not been successful. Why is identity necessary? The main reason for the problem is the population. The Earth is now estimated to have a population of over 7 billion. Over time, the identification of identities can lead to many problems. Person identities can be mainly categorized into age, class, gender, national, regional, spiritual groups. The solution was to introduce document base methods such as National identity card, Passport, driving license, etc. There were various data privacy and security problems with these methods. Therefore, although it was possible to provide digitized solutions to personal identities, it was not possible to provide a reliable, effective, usability solution due to technical issues.

d) Analysis of user behavior and usage patterns

As the research block chain based trusted digital ID platform concerns regarding the usage of the digital identity by users. Usage pattern of the digital identity explains the user's usage of the digital identity platform. It's a fact that not every user's usage is equivalent, as the user's usage differ and vary from each other. In order to clearly analyze the data regarding the user's usage, analysis of usage patterns of the user can be introduced.

Analyzing of data includes data manipulation, data transformation, and data visualization in order to make a meaningful result from specific data set. These meaningful insight of data helps to make decisions. Therefore, it enables commercial fields, individuals and the governments make decisions from the insights, acquired from the data analysis.[19] The data analysis has the ability to come to apprehensive conclusions by the use of graphs.

Analysis of the usage pattern consists of the concept of collecting real usage data from the registration process. As an example, over one month of period. That real usage of data will have each user's

usage pattern. The usage patterns mainly analyzed by the interaction between the digital identity and the user.

III. Methodology

The research which is discussed in this paper is a combination of improvements based on different key areas like Biometric Authentication, Neural Networks, Cyber Threat Intelligence. With the ambition of developing a Trusted Digital Identity Platform for Sri Lanka. But the idea and the essence of this research can be applied to any other domain or mobile application. Following given "Fig 1" shows a high-level diagram of our system and it is followed by comprehensive description of each research component with the flow of the system.

a) Service Provider Management with document validator

One of the unique features of our system when comparing to existing solutions in the market is we are providing access to the service providers to register to our system online while

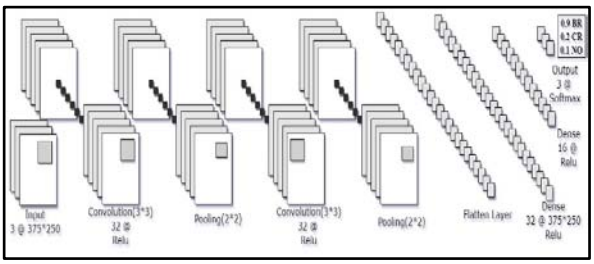


Figure II: Neural Network Architecture in Document Validator

providing the necessary documentation. Since a large number of service providers are using this feature, we have to eliminate illegitimate registration attempts to minimize wastage in resources and time of administrators.

In this research part, we are introducing a Document Validator that can identify business documents that are uploaded by customers to the system as valid business registration documents or not. In the Sri Lankan context, there are two main business registration documents namely Business Registration (BR) and Company Registration (CR). This document validator has the capability to identify the uploaded document as CR, BR, or An Image with low details or not a correct document.

1) Dataset and Preprocessing

We have created a dataset of 318 original images with 98 CR images 106 of BR images and 114 images which can be classified as either of these two categories. After the data augmentation using rotation, scale, shearing we collected around 1000 images. Data augmentation has been done in small amounts because the edges of the document get exempted otherwise.

2) Model creation and Training

The data set was divided into two parts, 25% as validation and 75% as training where 25% of the dataset is used to evaluate the model. Here we are creating a Convolutional Neural Network with a Sequential Model.

CNN architecture that has provided the best outcome contains following (Fig II).

- *Input layer:* Loading of the input and producing an output that going to be an input for convolutional layers is carried out in this layer. We are using 375* 250 resized three channel (RGB) images as our input because The documents which we are classifying are mostly in A4 paper size.
- *Convolutional layers:* A set of learnable filters will be formed from the input image is the function of this layer. We have used two convolutional layers with the kernel size of 3x3 and the same padding. These two convolutional layers learn 32 filters in each one. As the activation function we used Rectified Linear Unit (ReLU) for both of layers because given an value of z and the neuron's output is $f(z)$, if $z>0$ $f(z) = z$, if $z<0$ $f(z) = 0$[20].
- *Pooling layers:* Pooling layers are responsible for downscaling the volume of the neural network by reducing small features. We have used one pooling layer after eachconvolutional layer. Both of them are max pooling layers which are set to 2 x 2 pooling windows with no strides.
- *Flatten layer:* Is used to flatten pooled feature map to a single column which can be fed to a fully connected layer or hidden layers.
- *Hidden Layers:* There were used to get the output as a single vector by inputting a single vector. In here we have used three hidden layers which first two have the ReLU as the activation function with 32 layers and 16 layers respectively while the output layer has Softmax as the activation function with three filters in it. We used the Softmax function for the multi-class classification because it scales the numbers and returns probabilities related to each class.

Superviced is the trainig protocol we used for this classification. Adam is the optimizer that we have used for finding optimal model parameters which extends the functionality of Stochastic Gradient Decent.

b) Three Factor Biometric Authentication

Ensuring the trust of both citizens and service providers is the key priority of our system. Authentication is the process that allows both parties to verify their trust consequently, developing an authentication system in a way that protect the trust of both parties is crucially important. To achieve this, we introduce 3 factor

biometric authentication system which consist of three validation metrics.

- Confirm the live presence of the user using face recognition.
- Verify only a real person can authenticate to the system through liveness detection.
- Verify the authenticity of the user by using the biometrics available on the device or using pin number.

In face recognition, we have used Multi-Task Cascaded Convolutional Neural Network (MTCNN) [21] to extract faces from the video and Facenet model [16] to extract features of the face and create the face embeddings for the face recognition. Facenet is a deep convolutional neural network trained via a triplet loss function, according to this benchmark Facenet have an accuracy of 99.63% [22] compared to other similar face recognition models such as deepface model [23] by facebook with 98.37% accuracy [24] and openface model [25] with 92.92% benchmark accuracy [24], Facenet provides the highest accuracy. Another major concern in selecting Facenet method is that Facenet supports extra training data compared to other high-performance models like VarGFaceNet [26] we can train Facenet model with our own datasets to improve accuracy.

For the liveness detection we are using a combination of heuristic face movement detection and face texture analysis with a convolutional neural network CNN to differentiate real and spoofed faces. With the help of real time face contour detection in android ML kit [27] we can capture the face landmarks of the users face and predict the movement of the face. If any movement is detected, then the recorded video of the face will send the face recognition and texture-based liveness detection system hosted in the cloud. then convolutional neural network (CNN) will examine the texture of the detected face and differentiate if the detected face is real or spoof. CNN is trained using a dataset containing over10000 images containing both real and spoofed face images captured in different lightning conditions and reflections. Dataset contains images belongs to different skin colors while majority of images comprising brown skin color because we are specifically training this model to validate Sri Lankan citizens. CNN model architecture is similar to VGGNet model with less complex layers set because we need real time performance.

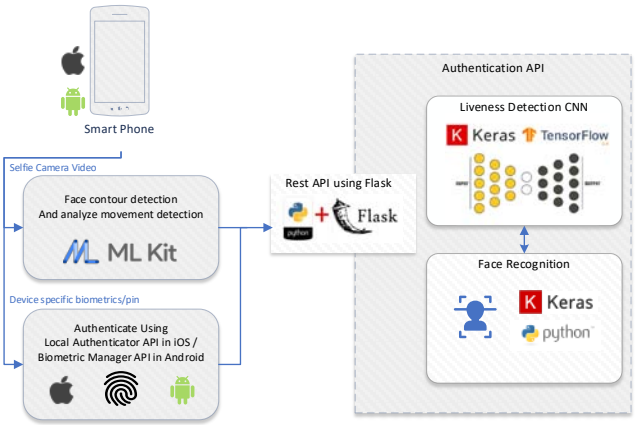


Figure III: Three Factor Biometrics model overview

c) *Blockchain based Cyber Security Inteligence*

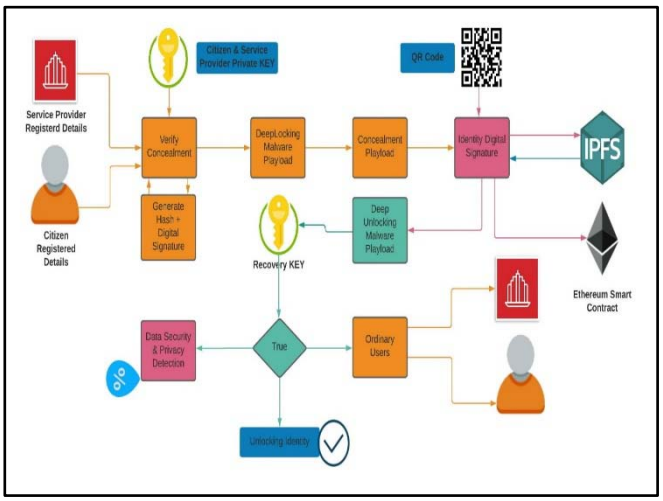


Figure IV: High level diagram of CTI System with Deep Locking

Trust Pass is a digital identity system used in digital transformation. This system is used in the transformation of data in digital services between the citizen and the service provider. trust pass always protects users from real time threats. There are various difficulties in using traditional methods day to day life. DNA and fingerprints are used for the most important human identities. There are two main types of users in our system as citizen and service provider. There is the ability to authenticate the accuracy of documents such as the service provider's business registration. Therefore, the citizen will not meet fake service providers. In this process the accuracy of the documents is checked using image processing.

After authentication of user data, the security intelligence process minimizes threats. In this process, users are given a unique private key. The user's hash function is activated and the hash value is returned after the data is sent to the concealment mechanism. The hash value can be identified as the identity of each user. Introducing Deep locking malware using security

intelligence. The user data is designed to not be compromised by an unauthorized person. Using deep neural networks (DNN) has deepened the locking malware mechanism. Here, cyber security intelligence is used to analyse the threat environment and minimize threat attacks. Attempts have been made to increase the accuracy of the user's documentation by using digital signatures. QR code is used to authenticate documents. The interplanetary file system is used to store system data. The hash function allows the user to retrieve stored data. [28]

Ethereum virtual machine (EVM) has been used to power the IPFS process when using blockchain. The user can use deep unlocking to recover deeply locked data. The user's public key or recovery key is used. The security and privacy value of the user's data is always taken into consideration. User usage pattern analysis is a feature that is embedded in the system. Analyses the behaviour of users using the system. The purpose is to analyse the number of users using the system, the services received, and customer feedback. Therefore, system vulnerabilities can be identified. The overall system seeks to minimize the impact on the security and privacy of the user's real-time data. Our aim is to provide maximum security services to the user during digital transformation. It focuses on the threat environment and uses the cyber threat intelligence mechanism to minimize the threat impact on the system. Therefore, the behaviour of threats is monitored and analysed to prepare the system for future threats. Because the behaviour of threats is vulnerable, deep locking malware has been used to prevent this process from becoming a threat to threats throughout the system. Security intelligence has the potential to enhance the security and privacy of system data using the aforementioned user usage pattern analysis process conclusions. [29]

d) Analysis of user behavior and usage patterns

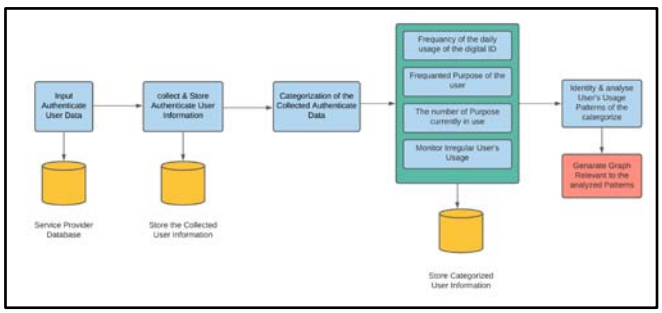


Figure V: High level diagram of Informative Data Analytics

The Blockchain based trusted digital identity platform is designed to ensure the privacy of the digital identity users. In this methodology the focused function is "Analyzing individual user's usage and usage pattern of digital ID by Collecting, Storing, and accessing data through digital identity management". In order to initiate the above-mentioned function, the first step is started from inputting the authenticated user's data, all authenticated user data will be gathered, and the collected authenticated data will be stored in a dataset. (The data for the dataset will be taken from the database). The next phase is to categorize the collected authenticated data relevant to the user. After gathering the relevant data, the gathered datasets will be categorized as mentioned in the high-level diagram. The analysis will mainly fall in to four types which are i). frequency of the daily usage of the user, Fig V). frequented purpose of use (ex – bank, health), iii) analyzing customer feedback, and iv). identifying irregular usage of the user. Identifying the irregular users help to analyze the misuse of the identity as the user doesn't use the digital identity on regular basis.

Then, according to the categorized data in the dataset, the analysis process will initiate while analyzing, the user's usage will be identified according to the categorized data.

The categorized data will be analyzed using Arima Model [30] (Autograssive Integrated moving average). The Arima Model is also a form of Machine Learning. The analysis of user's usage will depend on the amount of the users who use the digital ID platform. The analysis of the usage patterns will be generated in to Arima Model (Statistical analysis model). Arima Model is a statistical analysis model used to predict the future values based on past values. Arima Model consists of different Models as an example Sarima and Sarimax can be defined. In here Sarimax Model of Arima Model will help to understand the data patterns and predict the analysis based on time series forecasting as the mentioned categories i). frequency of the daily usage of the user, ii). frequented purpose of use (ex – bank, health), iii) analyzing customer feedback, and iv). identifying irregular usage of the user, are predicted for duration of three months by using the dummy data in the dataset. In this Fig V here the data is stationary as the P – value is less than 0.05.

```
1. ADF :  -6.554680125068782
2. P-Value :  8.675937480199415e-09
3. Num Of Lags :  12
4. Num Of Observations Used For ADF Regression and Critical Values Calculation : 1808
5. Critical Values :
    1% :  -3.433972018026501
    5% :  -2.8631399192826676
    10% :  -2.5676217442756872
```

Figure VI: Stationary of the Data

The graphs will be generated through the analysis which is done by using Arima Model; the generated graphs will help to define the analysis of the usage patterns.

IV. Experiments and Results

a) Service provider management with Document Validater

For the evaluation process we have used categorical cross entropy as the loss function because we have implemented a multiclass classification. Following figure depicts that we have achieved an overall training accuracy as 99% and 95% as the validation accuracy.

```
loss: 0.0734 - accuracy: 0.9975 - val_loss: 0.1480 - val_accuracy: 0.9545
```

Figure VI: Accuracy of document validator

b) Three Factor Biometric Authentication

With ADAM optimizer we were able to achieve atraining accuracy of 98.6% and validation accuracy of 99.8% for texture-based liveness detection CNN. we used total of 10680 training samples to achieve this result. (Fig VIII)

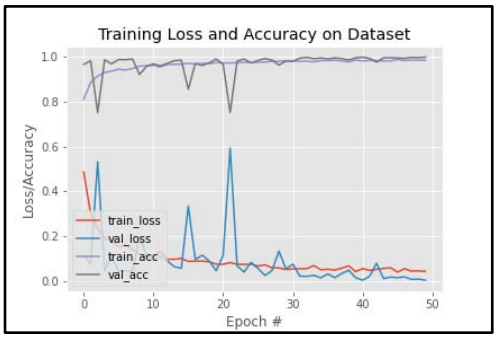


Figure VIII: Loss Accuracy Graph of CNN

c) Blockchain based Cyber Intelligence

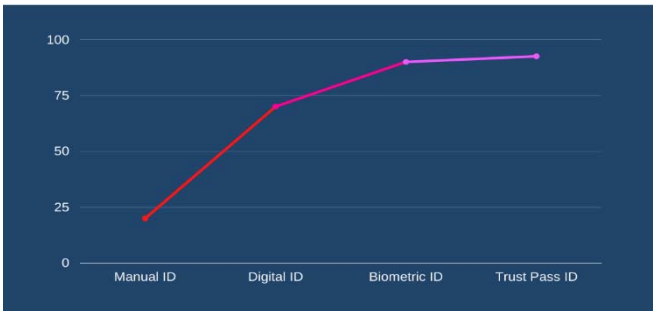


Figure IX: User's Data Security and Privacy

In this process, Security intelligence is considered to be the key to protecting a user's data and minimizing the impact of threats on privacy. Deep Locking Malware Algorithm protects user data from threats. Data security and privacy can also be enhanced by using the user's hash function and digital signature when storing data. Using Blockchain and Decentralized storage minimizes threats by storing user data. The primary purpose of these Trust Pass identity systems is to open up space for the user to navigate freely within the digital transformation process.

d) Analysis of user behaviour and usage patterns

The Arima model is used to perform the analyzation. [30] Arima model has the ability to convey the details of analyzation by adopting to time series of data as in the analyzation. It can be defined as a statistical analysis model which utilizes time series of data whether to comprehend the dataset properly or in order to predict the values of future accurately. Therefore, the Arima model has the ability to forecast values based on past time series. As mentioned above the analyzation results are conveyed by using Arima model (Sarimax results). Sarimax model come under Arima model. It is a model which derived from Arima model.

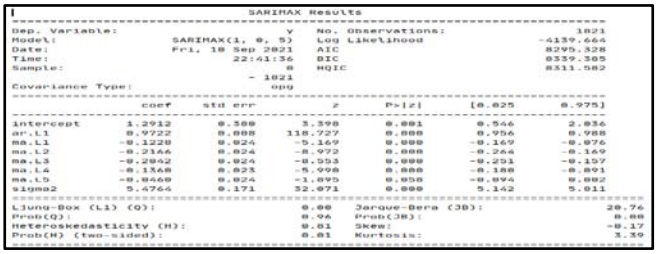


Figure X: SARIMAX results

V. Conclusion

By paving thoughts toward the digital transformation of Sri Lanka, our intention is to create a decentralized digital Identity Platform that can be accessed from anywhere from any citizen that has enhanced security through cyber threat intelligence and threat intrusion analysis system. Our three-factor biometric feature extends the User side authorization to a next level on the other hand time and integrity of the Service providers would be saved with the automated document validator. All of the users will be secured using blockchain technology to minimize the threat from attackers while implementing user privacy.

References Références Referencias

1. "The Government Information Center." http://www.gic.gov.lk/gic/index.php/en/component/info/?id=416&task=info (accessed Feb. 26, 2021).
2. "Digital Identity Survay form (Responses) - Google Drive." https://docs.google.com/spreadsheets/u/2/d/e/2PACX-1vTXlGdWY4VCbIExzDiRWMpYhqG0-9pTGNevOaHbKxfKulbLM-4-HMFdjpypfiNVMu8pRnPbET5lLD4f/pubhtml (accessed Sep. 06, 2021).
3. "SingPass Mobile." https://app.singpass.gov.sg/ (accessed Feb. 24, 2021).
4. "Digital iD™ - ID on Your Phone - Australia Post." https://www.digitalid.com/ (accessed Feb. 24,2021).
5. "Blockchain for Digital Identity | Accenture." https://www.accenture.com/us-en/services/blockchain/digital-identity (accessed Feb. 24, 2021).

6. "Digital identity as a force for good • Yoti." https://www.yoti.com/ (accessed Feb. 24, 2021).
7. "Smart ID | Deloitte UK." https://www.deloitte.co.uk/smartid/ (accessed Feb. 26, 2021).
8. Department of Census and and Statistics, "Computer literacy statistics 2019 (annual)," vol. 2019, pp. 2012–2015, 2019, [Online]. Available: http://www.statistics.gov.lk/ComputerLiterarcy/BuletinComputerLiteracy.pdf.
9. Y. Sun, B. Xue, M. Zhang, G. G. Yen, and J. Lv, "Automatically Designing CNN Architectures Using the Genetic Algorithm for Image Classification," *IEEE Trans. Cybern.*, vol. 50, no. 9, pp. 3840–3854, 2020, doi: 10.1109/TCYB.2020.2983860.
10. D. Han, Q. Liu, and W. Fan, "A new image classification method using CNN transfer learning and web data augmentation," *Expert Syst. Appl.*, vol. 95, pp. 43–56, 2018, doi: 10.1016/j.eswa.2017.11.028.
11. S. Kido, Y. Hirano, and N. Hashimoto, "Detection and classification of lung abnormalities by use of convolutional neural network (CNN) and regions with CNN features (R-CNN)," *2018 Int. Work. Adv. Image Technol. IWAIT 2018*, pp. 1–4, 2018, doi: 10.1109/IWAIT.2018.8369798.
12. H. Lee and H. Kwon, "Going Deeper with Contextual CNN for Hyperspectral Image Classification," *IEEE Trans. Image Process.*, vol. 26, no. 10, pp. 4843–4855, 2017, doi: 10.1109/TIP.2017.2725580.
13. "• Smartphone fingerprint sensor penetration worldwide 2014-2018 | Statista." https://www.statista.com/statistics/804269/global-smartphone-fingerprint-sensor-penetration-rate/ (accessed Aug. 19, 2021).
14. "Juniper Research: Mobile Biometrics to Authenticate $2 Trillion of Sales by 2023, Driven by Over 2,500% Growth in Remote Biometric Transactions | Business Wire." https://www.businesswire.com/news/home/20180724005050/en/Juniper-Research-Mobile-Biometrics-Authenticate-2-Trillion (accessed Aug. 19, 2021).
15. G. Singh and A. K. Goel, "Face Detection and Recognition S.
16. F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, vol. 07-12-June, pp. 815–823, 2015, doi: 10.1109/CVPR.2015.7298682.
17. B. Biggio, Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Security evaluation of biometric authentication systems under real spoofing attacks," *IET Biometrics*, vol. 1, no. 1, pp. 11–24, 2012, doi: 10.1049/iet-bmt.2011.0012.
18. I. Chingovska, A. R. Dos Anjos, and S. Marcel, "Biometrics evaluation under spoofing attacks," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 12, pp. 2264–2276, 2014, doi: 10.1109/TIFS.2014.2349158.
19. Q. Stokkink and J. Pouwelse, "Deployment of a Blockchain-Based Self-Sovereign Identity," *Proc. - IEEE 2018 Int. Congr. Cybermatics 2018 IEEE Conf. Internet Things, Green Comput. Commun. Cyber, Phys. Soc. Comput. Smart Data, Blockchain, Comput. Inf. Technol. iThings/Gree*, pp. 1336–1342, 2018, doi: 10.1109/Cybermatics_2018.2018.00230.
20. "Activation Functions in Neural Networks | by SAGAR SHARMA | Towards Data Science." https://towardsdatascience.com/activation-functions-neural-networks-1cbd9f8d91d6 (accessed Sep. 05, 2021).
21. K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, "Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks," *IEEE Signal Process. Lett.*, vol. 23, no. 10, pp. 1499–1503, 2016, doi: 10.1109/LSP.2016.2603342.
22. "Labeled Faces in the Wild Benchmark (Face Verification) | Papers With Code." https://paperswithcode.com/sota/face-verification-on-labeled-faces-in-the (accessed Sep. 14, 2021).
23. Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: Closing the gap to human-level performance in face verification," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, pp. 1701–1708, 2014, doi: 10.1109/CVPR.2014.220.
24. "Labeled Faces in the Wild Benchmark (Face Verification) | Papers With Code".
25. T. Baltrusaitis, P. Robinson, and L. P. Morency, "OpenFace: An open source facial behavior analysis toolkit," *2016 IEEE Winter Conf. Appl. Comput. Vision, WACV 2016*, no. January 2018, 2016, doi: 10.1109/WACV.2016.7477553.
26. M. Yan, M. Zhao, Z. Xu, Q. Zhang, G. Wang, and Z. Su, "VarGFaceNet: An efficient variable group convolutional neural network for lightweight face recognition," *Proc. - 2019 Int. Conf. Comput. Vis. Work. ICCVW 2019*, pp. 2647–2654, 2019, doi: 10.1109/ICCVW.2019.00323.
27. "ML Kit | Google Developers." https://developers.google.com/ml-kit (accessed Sep. 11, 2021).
28. S. Choudhari, S. K. Das and S. Parasher, "Interoperable Blockchain Solution For Digital Identity Management".
29. L. Guo and C. Lan, "A New Signature Based on Blockchain," *2020 International Conference on Intelligent Computing, Automation and Systems (ICICAS)*, 2020, pp. 349-353, doi: 10.1109/ICICAS51530.2020.00079.
30. L. R. Amofah, "ARIMA Model in Time Series Analysis." 2020.
31. G. C. Tiao, "Time Series: ARIMA Methods," in *International Encyclopedia of the Social & Behavioral Sciences: Second Edition*, 2015, pp. 316–321.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 22 Issue 1 Version 1.0 Year 2022
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

An Analysis of the Potential Risk and Fraud Involved in Mobile Money Transaction in Freetown Sierra Leone

By Morris Ayodele Peacock
Port Loko University College

Abstract- The research work focused on looking at an analysis of the potential risk and fraud involved in mobile money transactions in Sierra Leone with a focus on Orange and Africell mobile telecommunication companies. The implementation of mobile money service like any other financial service faces risks and challenges. This research addresses fraud as a challenge in the provision of mobile money service to customers in Sierra Leone. Mobile money usage for transactions is steadily growing across Africa with the potential to revolutionize the cash-dominant economy of this continent to be cashless. With the increased use of mobile money services and number of business use cases designed each day, it is imperative to design a holistic approach to mobile money risk, security that will reduce security exposures and prevent fraud, as some mobile money service providers have lost millions of Leones to this growing threat. This research, therefore, examines the measures that mobile network operators providing mobile money services can employ to prevent fraud.

GJCST-E Classification: H.2.4

Strictly as per the compliance and regulations of:

An Analysis of the Potential Risk and Fraud Involved in Mobile Money Transaction in Freetown Sierra Leone

A Case Study of: Orange and Africell Mobile Telecommunication Company in Freetown, Sierra Leone

Morris Ayodele Peacock

Abstract- The research work focused on looking at an analysis of the potential risk and fraud involved in mobile money transactions in Sierra Leone with a focus on Orange and Africell mobile telecommunication companies. The implementation of mobile money service like any other financial service faces risks and challenges. This research addresses fraud as a challenge in the provision of mobile money service to customers in Sierra Leone. Mobile money usage for transactions is steadily growing across Africa with the potential to revolutionize the cash-dominant economy of this continent to be cashless. With the increased use of mobile money services and number of business use cases designed each day, it is imperative to design a holistic approach to mobile money risk, security that will reduce security exposures and prevent fraud, as some mobile money service providers have lost millions of Leones to this growing threat. This research, therefore, examines the measures that mobile network operators providing mobile money services can employ to prevent fraud. The study also discusses the mobile money users' perception about the linkage between mobile phone protection and security of the mobile money service on their phones. The research was a case study of Orange and Africell mobile telecommunication company in Sierra Leone and used qualitative and quantitative data collected through questionnaires and structured interviews of key staff of the mobile network operator (MNO), mobile money subscribers and agents of these services. Some of the main findings of this research include the general perception that there is no direct linkage between mobile phone protection and mobile money risk/security. It was further identified that one of the major causes of consumer driven fraud is PIN sharing giving it to MNO agents. In addressing mobile money fraud, it is suggested that the service provider should give mobile money security tips to the users at least twice in a year through short message service (SMS) to alert them of ways to enhance the security of their mobile phones.

Author: Faculty of Engineering and Technology, Ernest Bai Koroma University of Science and Technology, Port Loko University College. e-mail: mpeacock@ebkustsl.edu.sl

I. Introduction

Mobile money is the use of telecommunication platforms or networks by mobile phone subscribers to perform banking services. In short, mobile money enables subscribers to bank directly from their mobile phones without physically being in a financial institution to pay bills, receive money, and transact business all through virtual mobile accounts known as mobile money wallets. The use of mobile money for transactions has been steadily growing across Africa, positioned as the next "big thing" to revolutionize the cash dominant economy of Africa. A recent survey revealed that there are 20 countries in which more than 10% of adults used mobile money at some point in 2011, of which 15 are in Africa. For example, in Sierra Leone, Liberia, Ghana, Sudan, Kenya, and Gabon, more than half of adults used mobile money (The Economist, 2012). From this survey, it is evident that mobile money has become one of the "must offer" services for telecom companies in Africa. For example the top ranked telecommunication companies in Sierra Leone – Orange and Africell all offer mobile money services to their clients and usage statistics are increasing daily.

Mobile money was initially made popular by Safaricom and Vodafone's M-Pesa ("M" for "mobile", "pesa" for "money" in Swahili) in Kenya, which started in 2007. The M-Pesa application is installed on the SIM cards of customers and works on all handset brands. It is free to register and the user does not need to have a bank account. Safaricom receives fees for withdrawals and transfers, but keeps deposits into the mobile wallets free. The transfer service was quickly picked up for use as an informal savings account system and electronic payment mechanism for bills, goods and services. With M-Pesa, Kenya is at the forefront of the mobile money revolution: the number of agents across the country increased by 40 percent in 2013. It is now estimated that 24.8 million subscribers use mobile money services, like M-Pesa, in Kenya (Communication Commission of Kenya, 2013). According to the Pew Research Center's 2013 survey report, the number of Kenyans using

mobile wallets to make or receive payments is higher than any of the other 24 countries surveyed: 50 percent of the Kenyan adult population uses mobile money services (Pew Research Center, 2013). Mobile money services have spread rapidly in many developing countries. However, only a handful of these initiatives have reached a sustainable scale, in particular GCASH and Smart Money in the Philippines; Wizzit, MTN Mobile Money and FNB in South Africa; MTN Mobile Money in Uganda; Vodacom M-PESA and Airtel in Tanzania; Celpay Holdings in Zambia and MTN Mobile Money, Orange Money in Côte d'Ivoire. The Philippines was one of the earliest adopters of mobile money services when SMART Communications launched SMART Money in 2001. The service, which uses SIM Tool-Kits, enables customers to buy airtime, send and receive money domestically and internationally via mobile, and pay for goods using a card. In 2004, Globe Telecom launched GCASH. This service provides a cashless method for facilitating money remittances, settle loans, disburse salaries or commissions and pay bills, products and services via text message. In South Africa, MTN Mobile Money was launched in 2005 as a joint venture between the country's second largest network operator MTN and a large commercial bank, Standard Bank. In Uganda, MTN was the first operator to launch mobile money services in 2009 and remains, by far, the market leader (Intermedia, 2012). By law, each mobile money provider has to partner with a bank. However, users do not need a bank account to use mobile money services. In Tanzania, Airtel was the first mobile network operator to introduce a phone-to-phone airtime credit transfer service, "Me2U," in 2005 (Intermedia, 2013). Airtel partners with Citigroup and Standard Chartered Bank to provide m-money services, including bill payments, payments for goods and services, phone-to-phone and phone-to-bank money transfers, and mobile wallets. In 2008, Vodacom Tanzania launched the second East African implementation of the Vodafone m-money transfer platform, M-Pesa.

Finally, in Côte d'Ivoire two mobile operators, Orange and MTN, are competing head to head in the mobile money market (CGAP, 2012). Orange Money was launched in 2008 by Orange in partnership with BICICI (BNP Paribas), and MTN Mobile Money was launched in 2009 by MTN in partnership with SGBCI (SociétéGénérale) (GSMA, 2014).

In Sierra Leone 21st June 2012, Airtel Money was launched, the service provides customers with convenient access to affordable and innovative financial services through their mobile phones. The platform allows customers to top up their phones with air time, send and receive money, pay their critical utility bills, and access their Bank accounts. Airtel also partnered with International Banks and Regional banks such as Guarantee Trust Bank, Eco Bank, Sierra Leone Commercial Bank Limited, United Bank for Africa, Access Bank and Zenith Bank to provide customers with access to deposit and withdraw cash, money transfers, banking services and pay bills.

II. Aim and Objectives of the Study

The aim of this research is to analyze the potential risk and fraud involved in mobile money transactions in Freetown, Sierra Leone.

a) Research Objectives

- To discuss the history of Mobile Money Transfer and the contribution of Orange and Africell the development of people in Freetown the capital city of Sierra Leone.
- To assess the Challenges and risk management in mobile money transfer and issues related to fraud.
- Mobile money security.
- To determine the potential of Orange and Africell Mobile Money in improving the lives of people in Freetown and on the Sierra Leone monetary policy.

III. Methodology

The research was carried out in Freetown, which is the capital and largest city of Sierra Leone. It is a major port city on the Atlantic Ocean and is located in the Western Area of the country. Freetown is Sierra Leone's major urban, economic, financial, cultural, educational and political centre, as it is the seat of the Government of Sierra Leone. The population of Freetown was 1,055,964 at the 2015 census.

The city's economy revolves largely around its harbour, which occupies a part of the estuary of the Sierra Leone River in one of the world's largest natural deep water harbours.

The population of Freetown is ethnically, culturally, and religiously diverse. The city is home to a significant population of all of Sierra Leone's ethnic groups, with no single ethnic group forming more than 27% of the city's population. As in virtually all parts of Sierra Leone, the Krio language is Freetown's primary language of communication and is by far the most widely spoken language in the city.

The city of Freetown was founded by abolitionist Lieutenant John Clarkson on March 11, 1792 as a settlement for freed African American, West Indian and Liberated African slaves. Their descendants are known as the Creole people. The local Temne and Loko people were living in villages in the land that became known as Freetown before the European arrival.

The study was conducted in two (2) mobile telecommunication companies in Sierra Leone. The population sample used was based on two mobile telecommunication companies in Sierra Leone Orange and Africell Mobile Telecommunications Companies. The sample selected one hundred people which include

staff, agents and subscribers. These one hundred people were chosen indiscriminately.

The information collected would be analysed using both quantitative and qualitative analysis. Tables and figures that would be used will be followed by interpretation and through discussion of the findings. The researcher will also embark on using pie chart on statistical packages for Social Science to be able to analyse the data.

IV. Results and Discussions

Data analysis and result presentation Questionnaires and interviews were used as the sources of collecting data for this research work. This chapter presents the findings of the data from the questionnaires and interviews conducted.

The researchers planned to use 120 questionnaires from the two mobile telecommunications companies, but after the disbursement of the questionnaires, 100 were retrieved in all, representing 83% of the total questionnaires administered. Data presented here mainly covers demographic information of respondents, duration of mobile money usage, fraud and actions susceptible to fraud, and mobile phone security and mobile money security. The following are the data collected from the questionnaires:

In all, 53% of the total respondents are male, while 47% are female. With regards to the age groups of respondents, 67% of the total respondents are between 18 and 29 years, 26% are also in the age range of 30 and 39 years, while 7% are between 40 and 49 years. None of the respondents fall within the 50 to 59 age group or above 60 years. Majority of the respondents, 34%, have Diploma level educational qualification, followed by 33% respondents with a bachelor's degree. Senior Secondary School (SSS) level education, those with no educational qualification and 2nd Degree holders represents 21%, 7% and 5% of total respondents respectively.

Table 4-1: Duration of using Mobile Money

Options	Frequency	Percentage
< 1 years	31	31 %
1-2 years	33	33 %
3-4 years	36	36 %
Total	**100**	**100 %**

The above Table 4-1 explains the duration of using mobile money. The table shows that 31 of the respondents have used mobile money for less than one year, and 33 of the respondents have also used mobile money for over two years, whilst 36 of the respondents used mobile money for over four years respectively.

Table 4-2: Preferred point of loading money on phone

Options	Frequency	Percentage
Service centres	73	73 %
Banks	12	12 %
Merchants	14	14 %
Peer-to-peer	01	01 %
Total	**100**	**100 %**

The above Table 4-2 identifies the preferred points of loading money on the mobile money wallet of the respondents. The table shows that 73 of the respondents prefer the service provider's service centre to the other sources available. 12, 14 and 1 of the respondents preferred Banks, Merchants and Peer-to-peer respectively.

Table 4-3: Preferred medium of transferring money

Options	Frequency	Percentage
Own phone (self)	51	51 %
Service centres	43	43 %
Merchants	06	6 %
Total	**100**	**100 %**

Table 4-3 above represents mobile money users' responses to the most convenient mode of transferring money. The available modes presented to the respondents are: performing the transfer on their own phone, using service centres, and visiting merchants to transfer money. Performing transfers on their own phones forms the majority of the responses: 51 out of 100. Using service centres for the transfer is another option available, and 43 of the respondents see this medium most convenient to them, and 6 of respondents preferred the merchants.

Table 4-4: Linkage between mobile phone access and risk of exploiting MM service

Option	Frequency	Percentage
Yes	22	22 %
No	78	78 %
Total	**100**	**100 %**

From the above Table 4-4, 22 of the respondents indicated that, yes, they will be bothered if anyone has access to their mobile money, since they believe the person can also have access to their mobile money by just having access to the mobile phone. The general trend that gives these respondents the cause to worry is that they store their PINs and password on their phones, and they believe technology is advanced such that people will have means of accessing their mobile money. On the other hand, 78% of the respondents do not think it is possible for anyone to access their mobile money wallet, if a person has access to their mobile phone. Some of the reasons given for this response are

that their mobile money PINs are secured, not easily guessed and known to the users alone. One respondent also gives the reason why he will not be bothered about unauthorized access to his phone:

"My password is not easy to guess and there is a threshold to the number of wrong password attempt one can make".

Table 4-5: Does secure phone make MM service secure?

Option	Frequency	Percentage
Yes	49	49 %
No	51	51 %
Total	100	100 %

This table (4-5) shows that 49 of the respondents agree that having a secure mobile phone definitely ensures the safety of their mobile money. However, 51% of the respondents do not think having a secure phone makes their mobile money secure in any way. The respondents in this class of thought believed that they would have to take precautions in order to protect their mobile money and not leave this to chance, because they have put in place factors to secure the phone.

V. Conclusions

This research has revealed that the major uses of mobile money service are for purchasing top ups and for local money transfer, as is generally believed to be the uses of mobile money in most African countries. The researchers are of the opinion that as more people have access to mobile phones as compared to bank accounts, and money transfer can be easily done on their mobile phones, this usage is very popular. More so, it is cumbersome for one to open a bank account, as several materials are required, such as government issued identity cards, references from an existing customer, as well as a form of confirmation of users' location.

Meanwhile, as compared to having a mobile money account, the process is not as complicated as opening a bank account. It can further be speculated that people are looking for easier and faster ways of sending and receiving money. It can also be argued that, as mobile money transfers are done mostly from the cities to the countryside, where most people do not have a bank account but a mobile phone is easily accessible, this could be a contributing factor for the major use of mobile money for transfer purposes.

As one of the major causes of consumer driven fraud is PIN sharing, it can be seen from this research that this is not a very common practice. However, the 9% that shared their PINs did so with their relations and sometimes with customer agents to help them in transacting one service or the other from their mobile money. It can be seen from this that, PIN sharing could be done based on trust, and if any fraud should be perpetuated through acquiring of the users' PIN, the person carrying out the fraud must first try to win the trust of the user, either by pretending to be a part of the service provider or a relative who is trying to offer a help. To avert this however, the researchers believe that the MNOs must alert users to first verify from them the authenticity of any suspected request before giving out any information that could make them vulnerable to fraud.

Despite users' awareness of their security measures they can take to prevent fraud, the service provider has a major task in securing the mobile money service, since as much as 13% believe the security of the service solely depends on the service provider. The researchers believe this category of users will invariably not put any blame on themselves if any fraud happens, since they believe total protection of the service depends on the service provider. It has also been found that even though there are several services available, such as pay bill and top up airtime, on the mobile money that users can take advantage of, the general usage of these other services are few. The researchers believe this could be as a result of the complex nature of using these services. The general perception that there is no direct linkage between mobile phone protection and mobile money protection could be attributed to the fact that users believe the service provider has put in place adequate measures to protect the mobile money service.

VI. Recommendations

Some of the recommendations made are as follows:

- As PIN sharing was identified as one of the major causes of consumer driven fraud, it is recommended that the service providers must set up password age parameters for the users to change their passwords every quarter. This must further be authenticated through answering personal identification questions.
- It is also suggested that service providers must enhance their awareness about the services available on the mobile money service.
- Service providers must also create awareness to mobile money users that the security of the mobile money service does not only depend on the MNOs, but the users also have a role to play.

References Références Referencias

1. Eric KodjoAfanu, Raymond SelormMamattah, 2013 Mobile Money Security, A Holistic Approach - Luleå University of Technology, Department of Computer Science, Electrical and Space Engineering.
2. JoseckLuminzuMudiri- Fraud in Mobile Financial Services, A MicroSave Publication.

3. María Paula Subia and Nicole Martinez- International Organization for Migration (IOM), ACP Observatory on Migration, 2014 Mobile money services: "A Bank in your pocket". Overview and opportunities.
4. Ismail, T. and K. Masinge, 2011 "Mobile Banking: Innovation for the Poor", UNU-MERIT, Working paper 2011-074. Available from: www.rrojasdata bank.info/mobilebanking15.pdf.
5. Godfried B. Adaba & Daniel Azerikatoa Ayoung, 2017 The development of a mobile money service: an exploratory actor-network study.
6. Andrew James Lake, November 2013 Risk management in Mobile Money: Observed Risks and Proposed Mitigants for Mobile Money Operators.
7. Adeyinkam Adedoyin, June 2018 Predicting fraud in mobile money transfer.
8. Lara Gilman and Michael Joyce Managing the Risk of Fraud in Mobile Money.
9. Odoyo Collins Otieno, Samuel Liyala, Benson Odongo, SilvanceAbeka – January 2016 Challenges facing the use and adoption of Mobile Phone Money Services.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 22 Issue 1 Version 1.0 Year 2022
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Comparative Analysis of Selected Filtered Feature Rankers Evaluators for Cyber Attacks Detection

By Olasehinde Olayemi

Abstract- An increase in global connectivity and rapid expansion of computer usage and computer networks has made the security of the computer system an important issue; with the industries and cyber communities being faced with new kinds of attacks daily. The high complexity of cyberattacks poses a great challenge to the protection of cyberinfrastructures, Confidentiality, Integrity, and availability of sensitive information stored on it. Intrusion detection systems monitors' network traffic for suspicious (Intrusive) activity and issues alert when such activity is detected. Building Intrusion detection system that is computationally efficient and effective requires the use of relevant features of the network traffics (packets) identified by feature selection algorithms. This paper implemented K-Nearest Neighbor and Naïve Bayes Intrusion detection models using relevant features of the UNSW-NB15 Intrusion detection dataset selected by Gain Ratio, Information Gain, Relief F and Correlation rankers feature selection techniques.

Keywords: features rankers, cyber-attacks, intrusion, classification, computer security, network packets.

GJCST-E Classification: K.4.4

Strictly as per the compliance and regulations of:

Comparative Analysis of Selected Filtered Feature Rankers Evaluators for Cyber Attacks Detection

Olasehinde Olayemi

Abstract- An increase in global connectivity and rapid expansion of computer usage and computer networks has made the security of the computer system an important issue; with the industries and cyber communities being faced with new kinds of attacks daily. The high complexity of cyberattacks poses a great challenge to the protection of cyberinfrastructures, Confidentiality, Integrity, and availability of sensitive information stored on it. Intrusion detection systems monitors' network traffic for suspicious (Intrusive) activity and issues alert when such activity is detected. Building Intrusion detection system that is computationally efficient and effective requires the use of relevant features of the network traffics (packets) identified by feature selection algorithms. This paper implemented K-Nearest Neighbor and Naïve Bayes Intrusion detection models using relevant features of the UNSW-NB15 Intrusion detection dataset selected by Gain Ratio, Information Gain, Relief F and Correlation rankers feature selection techniques. The results of the comparative analysis of the model's predictive performances shows that, among all the feature selection techniques used, the models of Relief F reduced features recorded the best cyber-attacks predictive performance. Models built with all the features of the dataset gives the least predictive performance. All the KNN models recorded better predictive performance than all Naïve Bayes models. The models' performance were measured in terms of classification/detection accuracy, precision and false alarm rate.

Keywords: features rankers, cyber-attacks, intrusion, classification, computer security, network packets.

I. Introduction

The increase in global connectivity and rapid expansion of computer usage and computer networks has made the security of the computer system an important issue; with the industries and cyber communities being faced with new kinds of attacks daily. The high complexity of intrusion poses a great challenge to the protection of cyberinfrastructure and the Confidentiality, integrity, and availability of sensitive information stored on them. The state of computer security is complicated, it is difficult to have a system that is completely free from attacks. The nature and the means of executing cyberattacks make it prevalent. Cyber-attacks are easy and cheap to execute, all that is require to stage a cyber-attacks are computer system and internet access, the nature of internet makes launching a cyber-attack is less risky than physical attacks, and not constrained by geographical distance. [1]. Network traffics contain different types of protocols and services which accounted for the multiple features in the network packet. Some of these features are redundant or irrelevant and does not contribute the classification of the network packets as either attack or normal network packets. The redundant features are the primary causes of increasing the false alarm rate (FAR) and decrease in detection accuracy. Feature Selection (FS) Techniques are the methods used to determine the relevant features of a dataset. It is an efficient way to reduce the dimensionality of a problem [2]. Different FS techniques existed in classification and clustering problems. They are i) Filter method ii) Wrapper Method and iii) Embedded method. The filter methods are used to select the features based on the scores in various statistical correlations. Wrapper method uses a greedy approach in feature selection. It evaluates all possible combination and produces the result for Machine learning. The embedded method combines the advantage of two models. Filtered Feature selection algorithms can be grouped into two categories from the point of view of a method's output: feature-ranking and feature-subset selection. Feature-subset selection focuses on selecting best subset of features that satisfies an evaluation criterion, feature-ranking on the other hand ranks features according to certain evaluation criterial, which measures the relevance of individual feature to the target class, and select the set of ranked features that gives the best evaluation performance, the drawback of this methods is that, a features that is not relevant to the target class on its own, can be very relevant when combined with others features.

The objectives of feature-ranking are three-folds: improving the prediction performance of the predictors, providing faster and more cost-effective predictors, and providing a better understanding of the underlying process that generated the dataset [3]. The FS also reduces the computational time to implement an online Network Intrusion Detection System (NIDS) [4]. The efficiency of the FS methods is measured by its accuracy at removing noisy and redundant features [5]. The quality of the network traffics /dataset does not only help to build effective NIDS but also shows its potential

Author: e-mail: olaolasehinde@fedpolel.edu.ng

efficiency during deployment in a real-life operating environment. NIDS analyze and monitor network traffic to detect suspicious activities and vulnerability in the system [6]. The effectiveness of NIDS is evaluated based on its ability to correctly identify network traffics as attacks traffic or benign traffics (normal) in a comprehensive dataset that contains normal and abnormal behaviors [7].

Feature-ranking techniques ranked features independently without involving any learning algorithm based on statistics, information theory, or some functions of classifier's outputs [8]. It consists of scoring each feature according to a particular evaluation criterion [9]. Several authors have proposed various features selection methods. In the work of Wang and Gombault [9], IG and Chi-squared were applied to extract nine most important features from the forty one features to build Bayesian Network and C 4.5 decision tree classifiers to detect DDoS attack in the network. Results obtained shows that the detection accuracy remains the same while the overall efficiency improved. Authors in [10] proposed a multi-filter feature selection techniques that combines the results four filter selections methods on NSL-KDD intrusion network dataset to achieve an optimum selection. C4.5 decision tree evaluation of the thirteen optimal selected features out of forty one features shows a high detection rate and classification accuracy when compared to the forty-one features and other classification techniques. [11] Proposed a feature selection method based on Decision Dependent Correlation (DDC). Mutual information of each feature and decision is calculated and top 20 important features {feature no.: 3, 5, 40, 24, 2, 10, 41, 36, 8, 13, 27, 28, 22, 11, 14, 17, 18, 7, 9 and 15} are selected and evaluated by SVM classifier. The classified result is 93.46% detection accuracy. [12] Applied Information Gain (IG), Correlation-based (CFS), Gain Ratio (GR) feature selection to reduce the dimensionality of NSL-KDD dataset, and built a decision tree classifiers of the three feature selection methods. The three classifier recorded an improved performance than the classifier built with the whole NSL-KDD dataset. [13] Proposed a feature selection method that combined three filter methods; Gain ratio, Chi-squared and Relief F (triple-filter) in a cluster-based heterogeneous Wireless sensor network (WSN) for attacks classification. 14 important features of the NSL-KDD intrusion detection benchmark dataset out of the 41 original features were extracted for intrusion detection classifier. Results obtained show that the proposed method can effectively reduce the number of features with a high classification accuracy and detection rate in comparison with other filter methods.

II. Methodology

The proposed architecture of the Comparative Analysis of Selected Filtered Feature Rankers Evaluators for Cyber Attacks Detection is depicted in Figure 1. The discretization of the UNSW-NB15 dataset was first carried out to make it suitable for machine learning. Four Filtered Feature Rankers Evaluators algorithms; (Information Gain, Relief F, Gain Ration, and Correlation) rankers were used to rank and select the optimal relevant features of training and testing UNSW-NB15 intrusion datasets. The training dataset with the all it feature and the reduced features of the training datasets were used to train the K Nearest Neighbors (KNN, and Naive Bayes' algorithms. The testing dataset with the all it features and the reduced features of the testing dataset were used to evaluate the two classifiers. The model's training is depicted in black arrow lines while the model's evaluation is depicted in red arrow lines in the figure. The results of the evaluation for each reduced dataset were analyzed.

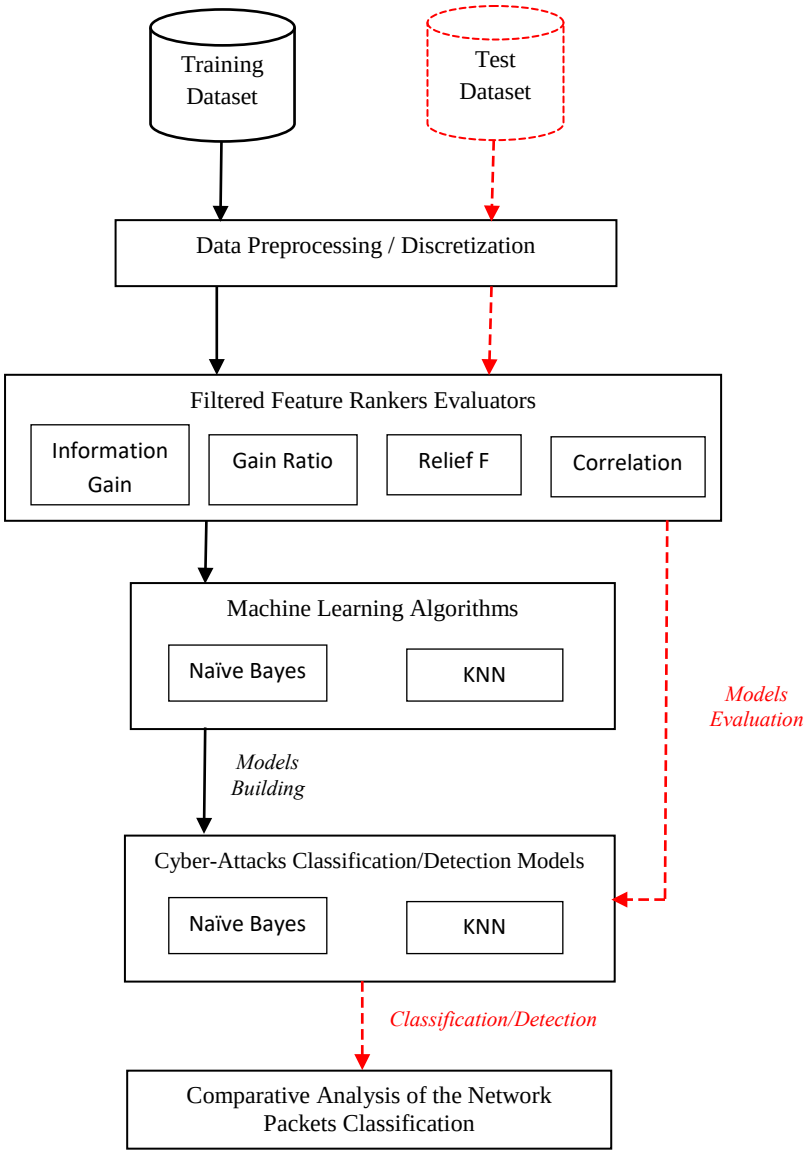


Figure 2: Architecture of the Selected Filtered Feature Rankers Evaluators for Cyber Attacks Detection

a) Description of UNSW-NB15 Dataset

The UNSW NB-15 dataset was developed using the IXIA Perfect Storm tool by the cybersecurity research group at the Australian Center for Cyber Security [14]. It is a fusion of normal network traffic packets, and synthetic modern-day network traffics attacks. The training and testing contain 82,332 and 174,341 records with 49 features each, respectively [14]. The dataset comprises nine attack categories and normal traffic, and it is suitable for the effective detection of existing and new attacks [14]. The details of both attack and normal traffic, coupled with the records in the training and testing categories, are presented in Table 1.

Table 1: Names and No of Attacks Categories in the UNSW-NB15 Dataset

Names of Attack	Training		Testing	
	No of Connection	Percentage Distribution	No of Connection	Percentage Distribution
Reconnaissance	3496	4.25	10491	5.98
Dos	4089	4.9	12264	6.99
Exploit	11132	13.52	33393	19.04
Shellcode	378	0.46	1133	0.65
Fuzzers	6062	7.36	18184	10.37
Backdoor	583	0.71	1746	1.00
Analysis	672	0.82	2000	1.14
Generic	18871	22.92	40000	22.81
Worms	44	0.05	130	0.07
Total No of Attacks	**45332**	**55.06**	**119341**	**68.06**
Normal	**37000**	**44.94**	**56000**	**31.94**
Total No of Connections	82332	100.00	175341	100.00

b) Data Munging and Analytic

This section outlines the Feature Rankers Evaluators and the machine learning techniques used for this study.

i. *Description of Attributes Selection Evaluators*

Attributes Selection Evaluator ranks features based on their relevant to the target class, ranking is a way of evaluating relevant features and selecting a minimal set of features based on given criteria in order to build simple models, that take less time to compute and become more understandable Feature ranking evaluation criterion compute the score *S(fi)* of feature *(fi)* of *the* training dataset. By convention a high score implies important (relevant) of the feature to the target class and select the *k* highest ranked features according to *S*. This is usually not optimal, but computationally efficient and often preferable to other, more complicated feature selection methods that involve searching through the entire search space. In this study, we use four feature-ranking techniques; Correlation Attribute Evaluator (CAE), Gain Ratio Attribute Evaluator (GAE), Information Gain attribute Evaluator (IGAE) and Relief F Attribute Evaluator (RFAE).

a. *Correlation Attribute Evaluator (CAE)*

Correlation Attribute Evaluator (CAE), evaluate Attribute using correlation analysis. The correlation between each attributes x and the target class Y, can be measured by finding correlation coefficient. A good feature is expected to have a higher correlation coefficient between it and target class. In correlation attribute evaluator method the attributes are considered based on their values where each value is treated as an indicator. CAE handles only nominal attributes input for evaluation and it uses Pearson's formula for computing correlation coefficient. for a candidate feature xi ∈ X and regression target Y the Pearson correlation coefficient is given by

$$\mathcal{R}(i) = \frac{cov(X_i, Y)}{\sqrt{var(X_i)var(Y)}} \quad (1)$$

where cov designates the covariance and var the variance.

b. *Information Gain attribute Evaluator (IGAE)*

Information gain (IG) measures the amount of information in bits about the class prediction, if the only information available is the presence of a feature and the corresponding class distribution. Concretely, it measures the expected reduction in entropy (uncertainty associated with a random feature) [15], it is given by equation 2.

Info Gain (Class, feature) = H (target class (Y)) – H (target class(Y) | feature (X))

$$IG = H(Y) - H(Y|X) \equiv H(X) - H(X|Y) \quad (2)$$

Where H(Y); the entropy of the target class H(Y) and $H(X \mid Y)$ is the entropy of target class given a certain attribute X.

The entropy of the target class *Y* is given by equation (3).

$$H(Y) = -\sum_{y \in Y} p(y) \log_2\big(p(y)\big) \quad (3)$$

Equation (4) gives the entropy of target class *Y* after observing feature *X*.

$$H(\boldsymbol{Y}|\boldsymbol{X}) = -\sum_{x \in X} p(x) \sum_{y \in Y} p(y|x) \log_2\big(p(y|x)\big) \quad (4)$$

c. *Gain Ratio Attribute Evaluator (GRAE)*

Gain ratio (GR) is a modification of the information gain that reduces its bias. It considered the number and size of branches in choosing an attribute. It assess the value of an attribute by measuring its gain ratio with respect to the target class [16]. the root attribute is the attribute of the UNSW-NB15 with the highest gain ratio, the gain ratio is the ratio of the

information gain and the split information for the attribute as presented in equation 5.

$$\text{Gain Ratio} = \frac{Information\ Gain(X)}{Split\ information(X)} \quad (5)$$

The information gain of attribute X is given by equation 2.

The Split information value of an attribute is chosen by taking the average of all the values in the domain of current attribute. It is given by equation 6.

$$Split(X) = -\sum_{x\epsilon X} \frac{|x|}{|n|} \cdot \log_2 \frac{|x|}{|n|} \quad (6)$$

Where n is the number of instances in the UNSW-NB15 training dataset.

d. *Relief Attribute Evaluator (RFAE)*

Relief Attribute Evaluator (RFAE) sample an instance recurrently using distance function taking into consideration the value of the given attribute for the nearest instance of the same and different class [13]. The original Relief algorithm, proposed by Kira and Rendell [8], is a two-class filtering algorithm for features normalized to [0, 1]. Each feature is initially assigned a zero weight. An A-dimensional training example R is chosen randomly and the Euclidean distance to all other instances calculated. Denote the nearest hit in the same class H, and the nearest miss in a different-class M. Since a good feature R[A] should be able to separate class values, it should have a small distance to H and a large distance to M. Hence W[A] is adjusted to reward good features and penalize poor ones. The final selection of features is made by selecting those large W[A], (that is . those that exceed a given threshold.)

ii. *Description of Machine learning techniques*

Two machine learning algorithms, namely; KNN and Naïve Bayes were used in this study to build the intrusion detection system.

a. *K-Nearest Neighbor*

Let p_i and qt represent the instance to be classified and the other instances in the dataset having the same number of features as P respectively, K-nearest neighbor Euclidean distance between p_i and q_t is defined in equation 7.

$$d(p_i, q_t) = \sqrt{\sum_{i=1}^{n} (p_i - q_i)^2} \quad (7)$$

From equation (3), a given instance will be classified as the attack categories having majority attacks among top k closest instance to the given instance.

b. *Naïve Bayes*

Given the UNSW-NB15 intrusion detection dataset that have X number *of* attributes called the predictors ($X = x_1, x_2,\ldots,x_n$) and another attribute y called the class label, with ten members $y_1,\ldots.y_{10}$, the Naive Bayes probability that a class y_j will be assigned to a given unlabelled instance X is given in equation 8.

$$p(y_j \mid x_1, \ldots., x_{43}) = \frac{p(y_j)p(x_i|y_j)}{p(x_i)} \qquad (\forall_j = 0,1, \ldots\ldots,9) \quad (8)$$

Maximum posterior probability for classifying a new instance attack categories is given in Equation 9.

$$y = \underset{y}{\arg max}\ py_j \prod_{j=0}^{9} p(y_j) p(x_1, x_2, \ldots x_{43} \mid y_j) \quad (9)$$

c) *Performance Evaluation Metrics*

Performance evaluation metrics play significant roles in assessing the predictive performance of the model and determining the model's fitness for the classification purpose. The confusion matrix, also known as the error matrix, is one of the most intuitive and easiest metrics used for finding the correctness and accuracy of the model. It has four possible outcomes, which are; True Positive (TP, Attack Network Packets detected as Attack Packets), True Negative (TN, Normal Network Packets Detected as Normal Packet), False Positive (FP, Attack Network Packets detected as Normal Packet), and False Negative (FN, Normal Network packets detected as Attack Packet). Detection accuracy, False alarm rate and precision are the three metrics used to evaluate the performances of the Intrusion detection classifiers of the four reduced dataset.

i. *Accuracy*

Accuracy (ACC) is the ratio of all correctly classified network packets to the total number of instances in the intrusion test dataset, it is given by equation.1. An accuracy of 1 implies error rate of 0 and an accuracy of 0 indicate error rate of 10.

$$ACC = \frac{TP + TN}{FN + FP + TN + TP} \quad (10)$$

ii. *False Positive Rate (FPR) or False Alarm Rate (FAR)*

False Positive Rate (FPR) or False Alarm Rate (FAR) is the proportion of actual network attacks cases

that were predicted as Normal packets by the model. FPR should be as low as possible to avoid unwanted false alarms. it is given by equation 11.

$$FPR = FAR = \frac{FP}{TN + FP} \quad (11)$$

iii. *Precision*

Precision is the ratio of correctly predicted positive observations to the total predicted positive observations. High precision relates to the low false positive rate. it is given by equation 12.

$$\text{Precision} = \frac{TP}{TP + FP} \quad (12)$$

III. Experimental Setup and Results Discussion

Four feature selection rankers were used to select the relevant features of the UNSW-NB15 intrusion dataset to build Intrusion Detection System. Two classification models (Naïve Bayes and KNN) were used to build the Intrusion detection system for the cyber-attacks detection and classification of Network traffic in a computer network. The relevant features of the UNSW-NB15 intrusion detection dataset selected by the four (4) filter features rankers are presented in Table 2. Relief F features ranker selected thirteen (13) features, Information Gain features ranker selected fourteen (15) features, Gain ration selected fifteen (14) features, while correlation ranker selected eleven (11) features. It was observed that Proto, Service and Ct_dst_sport_ltm were the only features that were commonly selected by the feature selection algorithms. Thus, they were the features observed to be the most relevant based on the four methods of evaluating the relevance and having the greatest importance in the detection and classification of attack packets in the network traffics.

Table 2: Features Selected by the Filtered Features Rankers

Relief F (13)	Gain Ratio (14)	Information Gain (15)	Correlation Ranker (11)
proto, service, state, smean, ct_dst_src_ltm Sttl, ct_state_ttl, ct_srv_src, ct_dst_sport_ltm, ct_srv_dst, dttl, ct_dst_ltm, ct_src_ltm	Proto, service, smean, ct_state_ttl, ct_dst_sport_ltm, ct_dst_dport_ltm, ct_srv_dst, Sbytes, dbytes, rate, dmean ,dpkts , dur, sload	proto, service, state, smean, swin, sttl, ct_state_ttl, dwin, ct_dst_sport_ltm, ct_src_dport_ltm, Sbytes, dttl, tcprtt, stcpb, dtcpb	proto, service, state, ct_srv_src, ct_dst_src_ltm, swin, sttl, Dwin, ct_dst_sport_ltm, ct_src_dport_ltm, ct_srv_dst

These reduced selected features with the complete features were used to build Intrusion detection systems of Naïve Bayes and KNN. The UNSW-NB15 testing dataset was used to evaluate all the classifiers. The confusion matrix and the performance of the KNN and Naïve Bayes classifiers with each of the selected features of the ranking feature technique is presented in Table 3 and 4 respectively. From tables 3 and 4, it shows that KNN and Naive Bayes intrusion detection models of Relief F selected features that identified thirteen (13) features recorded the best performance in terms of detection accuracy, classification precision and false alarm rate. The Intrusion detection models of KNN and Naïve Bayes of the fourteen (14) features identified by the Gain Ratio recorded the second best performance in terms of the selected performance metrics. Correlation and information Gain recorded the third and the fourth performances among the Rankers Features Selection Techniques respectively. Intrusion detection models of the two classifier with all of features of the UNSW-NB15 intrusion detection network dataset recorded the least and poorest performance, this result shows the importance and ability of the Rankers Features Selection Techniques to improve the performance of intrusion detection models.

The comparison analysis of the two classifiers shows that, KNN intrusion detection models recorded better detection accuracy, precision and false alarm rate than the Naïve Bayes model in the classification of UNSW-NB15 intrusion detection network dataset, it can be further deduced that the Relief F features selection method with KNN is the best-performing algorithm for the detection of network packets of UNSW-NB15 intrusion detection dataset. The comparison analysis of the selected Rankers Features Selection Techniques with each machine learning algorithms, based on the selected performance metrics is illustrated in Figure 2.

Table 3: Confusion Matrix and Performance of KNN Models with Each of the Rankers Features Selection Techniques

Rankers Features Selection Techniques	Number of selected Features	Confusion Matrix				Performance Metrics		
		TP	TN	FP	TP	Accuracy	Precision	FAR
Gain Ratio	14	106023	50900	13318	5100	89.50%	88.84%	20.74%
Information Gain	15	104572	49908	14769	6092	88.10%	87.62%	22.84%
Relief F	13	108503	51420	10838	4580	91.21%	90.92%	17.41%
Correlation	11	104572	50826	14769	5174	88.63%	87.62%	22.52%
All Attribute	49	90572	28026	28769	27974	67.64%	75.89%	50.65%

Table 4: Confusion Matrix and Performance of Naïve Bayes Models with Each of the Rankers Features Selection Techniques

Rankers Features Selection Techniques	Number of selected Features	Confusion Matrix				Performance Metrics		
		TP	TN	FP	TP	Accuracy	Precision	FAR
Gain Ratio	14	100629	47007	18712	8993	84.20%	84.32%	28.47%
Information Gain	15	89042	44576	30299	11424	76.20%	74.61%	40.47%
Relief F	13	102983	48937	16358	7063	86.64%	86.29%	25.05%
Correlation	11	93072	47186	26269	8814	79.99%	77.99%	35.76%
All Attribute	49	81272	29026	38069	26974	62.90%	68.10%	56.74%

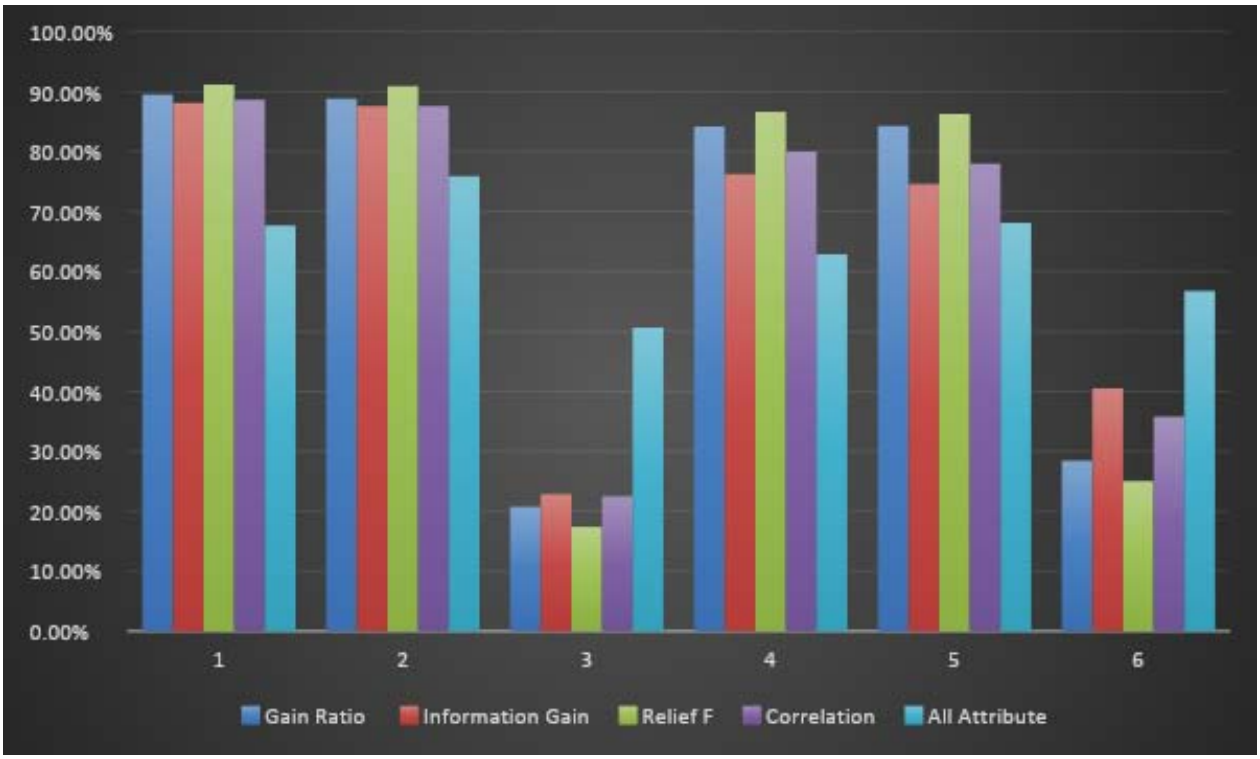


Figure 2: Comparison Analysis of the Selected Rankers Features Selection Methods with For Each Model

IV. Conclusions

In this research, Comparative Analysis of Selected Filtered Feature Rankers Evaluators for Cyber Attacks Detection was proposed using UNSW-NB15 intrusion detection network dataset. The dataset contained nine attacks and one normal traffic types with 49 features some of which were not suitable for the effective detection of existing and new attacks. Four selected Filtered Feature Rankers Evaluators ((Information Gain, Relief F, Gain Ratio, and Correlation) were applied to the dataset to select it suitable and

relevant features to model intrusion detection systems of KNN and Naïve Bayes machine learning algorithms. The Results of the features ranking shows that Relief F features ranker selected thirteen (13) features, Information Gain features ranker selected fourteen (15) features, Gain ration selected fifteen (14) features, while correlation ranker selected eleven (11) features. Features selected by Relief F recorded the best performance, Gain Ratio recorded the second best performance. Correlation and information Gain recorded the third and the fourth performances respectively, while the use of all the features recorded the least and poorest performance, this result shows the importance and ability of the Rankers Features Selection Techniques to improve the performance of intrusion detection models. All the KNN models recorded better performance than all Naïve Bayes models. The models' performance were measured in terms of Classification /detection accuracy, precision and false alarm rate. The results further shows models of KNN with the reduced features of Relief F features selection method recorded the best overall performance for the detection of network packets of UNSW-NB15 intrusion detection dataset.

a) Ethical Standard Funding

This research work is self-funded research undertaken by the authors at the Department of Computer Science, School of Applied sciences, Federal Polytechnics, Ile-Oluji, Nigeria.

Conflict of Interest

The corresponding author states that there is no conflict of interest.

References Références Referencias

1. Schreier F. (2015) On Cyberwarfare, DCAF Horizon 2015 working paper No. 7, Available at https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf (Accessed 2nd April, 2021).
2. Kavita P. and Pranjali D., "Survey on Data Mining Techniques for Intrusion Detection System", International Journal of Research Studies in Science, Engineering and Technology [IJRSSET] Volume 1, Issue 1, April 2014, PP 93-97.
3. Isabelle G. and Andre E. (2003): An Introduction to Variable and Feature Selection, Journal of Machine Learning Research 3: 1157-1182.
4. Olasehinde O.O., Williams K., Adegoke B. O. (2019) Reduced Features Intrusion Detection Systems Classification Accuracy Improvement. International Journal of Scientific & Engineering Research. 10(12) 181-186, 2019. http://dx.*doi*.org/10.1023/A:1006624031083.
5. Aldehim G., and Wang W. (2017) Determining appropriate approaches for using data in feature selection. Int. J. Mach. Learn. & Cyber. 8:915–928. 2017. https://doi.org/10.1007/s13042-015-0469-8.
6. Tariq, W., Arshad, M., Saqib, M., & Gul, N. (2012) Analysis of Security Techniques for Detecting Suspicious Activities and Intrusion Detection in Network Traffic. Semantic Scholar. 2012https://www.semanticscholar.org/paper/Analysis-of-Security-Techniques-for-Detecting-and-Tariq-Arshad/a993dab8bcd79ec8468c36489e2acabf957b71d0#citing-papers.
7. Gogoi P., Bhuyan M. H, Bhattacharyya D. K., and Kalita J. K. (2012) Packet and Flow Based Network Intrusion Dataset. Communications in Computer and Information Science, 322–334. 2012 https://doi.org/10.1007/978-3-642-32129-0_34.
8. Duch W, Winiarski T., Biesiada J., and. Kachel A, (2003) "Feature Ranking, Selection and Discretization," Int. Conf. on Artificial Neural Networks (ICANN) and Int. Conf. on Neural Information Processing (ICONIP), pp. 251–254, 2003.
9. Wang W., and Gombault S., Efficient detection of DDoS attacks with important attributes. In the 3rd IEEE International conference on Risks and Security of Internet and Systems (CRiSIS'08), Tozeur, Tunisia, 2008, pp. 61-67.
10. Opeyemi O., Kim-Kwang R. C., Ali D., Zheng X., and Mqhele. (2016) Ensemble-based Multi-Filter Feature Selection Method for DDoS Detection in Cloud Computing, journal of wireless communication and networking, doi: 10.1186/s13638-016-0623-3, 2016.
11. Qu G., Hariri S. and Yousif M., "A new dependency and correlation analysis for features," in *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, no. 9, pp. 1199-1207, Sept. 2005, doi: 10.1109/TKDE.2005.136.
12. Munson J. C. and Khoshgoftaar T. M.. The dimensionality of program complexity. In Proceedings of the 11th international conference on Software engineering, ICSE '89, pages 245–253. ACM, 1989.
13. Girish Chandrashekar and Ferat Sahin. "A survey on feature selection methods". In: Computers and Electrical Engineering 40.1 (2014), pp. 16–28. ISSN: 0045-7906.
14. Moustafa N. & Slay j. (2015). UNSW-NB15: A Comprehensive DataSet for Network Intrusion Detection Systems Military Communications and Information Systems Conference. (pp. 1-7).
15. Mitchell T. Machine Learning. McGraw-Hill, New York, 1997.
16. Sang-Hyun C. and Hee-Su C. (2014). Feature Selection using Attribute Ratio in NSL-KDD data. International Conference Data Mining, Civil and Mechanical Engineering (ICDMCME'2014), Feb 4-5, 2014 Bali (Indonesia).

Global Journals Guidelines Handbook 2022

www.GlobalJournals.org

Memberships

Fellows/Associates of Computer Science Research Council

FCSRC/ACSRC Memberships

Introduction

FCSRC/ACSRC is the most prestigious membership of Global Journals accredited by Open Association of Research Society, U.S.A (OARS). The credentials of Fellow and Associate designations signify that the researcher has gained the knowledge of the fundamental and high-level concepts, and is a subject matter expert, proficient in an expertise course covering the professional code of conduct, and follows recognized standards of practice. The credentials are designated only to the researchers, scientists, and professionals that have been selected by a rigorous process by our Editorial Board and Management Board.

Associates of FCSRC/ACSRC are scientists and researchers from around the world are working on projects/researches that have huge potentials. Members support Global Journals' mission to advance technology for humanity and the profession.

FCSRC

Fellow of Computer Science Research Council

FELLOW OF COMPUTER SCIENCE RESEARCH COUNCIL is the most prestigious membership of Global Journals. It is an award and membership granted to individuals that the Open Association of Research Society judges to have made a 'substantial contribution to the improvement of computer science, technology, and electronics engineering.

The primary objective is to recognize the leaders in research and scientific fields of the current era with a global perspective and to create a channel between them and other researchers for better exposure and knowledge sharing. Members are most eminent scientists, engineers, and technologists from all across the world. Fellows are elected for life through a peer review process on the basis of excellence in the respective domain. There is no limit on the number of new nominations made in any year. Each year, the Open Association of Research Society elect up to 12 new Fellow Members.

Benefit

To the institution

Get letter of appreciation

Global Journals sends a letter of appreciation of author to the Dean or CEO of the University or Company of which author is a part, signed by editor in chief or chief author.

Exclusive Network

Get access to a closed network

A FCSRC member gets access to a closed network of Tier 1 researchers and scientists with direct communication channel through our website. Fellows can reach out to other members or researchers directly.They should also be open to reaching out by other.

Career | Credibility | Exclusive | Reputation

Certificate

Certificate, LoR and Laser-Momento

Fellows receive a printed copy of a certificate signed by our Chief Author that may be used for academic purposes and a personal recommendation letter to the dean of member's university.

Career | Credibility | Exclusive | Reputation

Designation

Get honored title of membership

Fellows can use the honored title of membership. The “FCSRC” is an honored title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., FCSRC or William Walldroff, M.S., FCSRC.

Career | Credibility | Exclusive | Reputation

Recognition on the Platform

Better visibility and citation

All the Fellow members of FCSRC get a badge of "Leading Member of Global Journals" on the Research Community that distinguishes them from others. Additionally, the profile is also partially maintained by our team for better visibility and citation. All fellows get a dedicated page on the website with their biography.

Career | Credibility | Reputation

Future Work

Get discounts on the future publications

Fellows receive discounts on future publications with Global Journals up to 60%. Through our recommendation programs, members also receive discounts on publications made with OARS affiliated organizations.

Career | Financial

GJ Account

Unlimited forward of Emails

Fellows get secure and fast GJ work emails with unlimited forward of emails that they may use them as their primary email. For example, john [AT] globaljournals [DOT] org.

Career | Credibility | Reputation

Premium Tools

Access to all the premium tools

To take future researches to the zenith, fellows receive access to all the premium tools that Global Journals have to offer along with the partnership with some of the best marketing leading tools out there.

Financial

Conferences & Events

Organize seminar/conference

Fellows are authorized to organize symposium/seminar/conference on behalf of Global Journal Incorporation (USA). They can also participate in the same organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent. Additionally, they get free research conferences (and others) alerts.

Career | Credibility | Financial

Early Invitations

Early invitations to all the symposiums, seminars, conferences

All fellows receive the early invitations to all the symposiums, seminars, conferences and webinars hosted by Global Journals in their subject.

Exclusive

Publishing Articles & Books

Earn 60% of sales proceeds

Fellows can publish articles (limited) without any fees. Also, they can earn up to 70% of sales proceeds from the sale of reference/review books/literature/publishing of research paper. The FCSRC member can decide its price and we can help in making the right decision.

Exclusive | Financial

Reviewers

Get a remuneration of 15% of author fees

Fellow members are eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get a remuneration of 15% of author fees, taken from the author of a respective paper.

Financial

Access to Editorial Board

Become a member of the Editorial Board

Fellows may join as a member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. Additionally, Fellows get a chance to nominate other members for Editorial Board.

Career | Credibility | Exclusive | Reputation

And Much More

Get access to scientific museums and observatories across the globe

All members get access to 5 selected scientific museums and observatories across the globe. All researches published with Global Journals will be kept under deep archival facilities across regions for future protections and disaster recovery. They get 10 GB free secure cloud access for storing research files.

ASSOCIATE OF COMPUTER SCIENCE RESEARCH COUNCIL

ASSOCIATE OF COMPUTER SCIENCE RESEARCH COUNCIL is the membership of Global Journals awarded to individuals that the Open Association of Research Society judges to have made a 'substantial contribution to the improvement of computer science, technology, and electronics engineering.

The primary objective is to recognize the leaders in research and scientific fields of the current era with a global perspective and to create a channel between them and other researchers for better exposure and knowledge sharing. Members are most eminent scientists, engineers, and technologists from all across the world. Associate membership can later be promoted to Fellow Membership. Associates are elected for life through a peer review process on the basis of excellence in the respective domain. There is no limit on the number of new nominations made in any year. Each year, the Open Association of Research Society elect up to 12 new Associate Members.

Benefit

To the institution

Get letter of appreciation

Global Journals sends a letter of appreciation of author to the Dean or CEO of the University or Company of which author is a part, signed by editor in chief or chief author.

Exclusive Network

Get access to a closed network

A ACSRC member gets access to a closed network of Tier 2 researchers and scientists with direct communication channel through our website. Associates can reach out to other members or researchers directly.They should also be open to reaching out by other.

Career | Credibility | Exclusive | Reputation

Certificate

Certificate, LoR and Laser-Momento

Associates receive a printed copy of a certificate signed by our Chief Author that may be used for academic purposes and a personal recommendation letter to the dean of member's university.

Career | Credibility | Exclusive | Reputation

Designation

Get honored title of membership

Associates can use the honored title of membership. The “ACSRC” is an honored title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., ACSRC or William Walldroff, M.S., ACSRC.

Career | Credibility | Exclusive | Reputation

Recognition on the Platform

Better visibility and citation

All the Associate members of ACSRC get a badge of "Leading Member of Global Journals" on the Research Community that distinguishes them from others. Additionally, the profile is also partially maintained by our team for better visibility and citation.

Career | Credibility | Reputation

Future Work

Get discounts on the future publications

Associates receive discounts on future publications with Global Journals up to 30%. Through our recommendation programs, members also receive discounts on publications made with OARS affiliated organizations.

Career | Financial

GJ Account

Unlimited forward of Emails

Associates get secure and fast GJ work emails with 5GB forward of emails that they may use them as their primary email. For example, john [AT] globaljournals [DOT] org.

Career | Credibility | Reputation

Premium Tools

Access to all the premium tools

To take future researches to the zenith, associates receive access to all the premium tools that Global Journals have to offer along with the partnership with some of the best marketing leading tools out there.

Financial

Conferences & Events

Organize seminar/conference

Associates are authorized to organize symposium/seminar/conference on behalf of Global Journal Incorporation (USA). They can also participate in the same organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent. Additionally, they get free research conferences (and others) alerts.

Career | Credibility | Financial

Early Invitations

Early invitations to all the symposiums, seminars, conferences

All associates receive the early invitations to all the symposiums, seminars, conferences and webinars hosted by Global Journals in their subject.

Exclusive

Publishing Articles & Books

Earn 30-40% of sales proceeds

Associates can publish articles (limited) without any fees. Also, they can earn up to 30-40% of sales proceeds from the sale of reference/review books/literature/publishing of research paper.

Exclusive | Financial

Reviewers

Get a remuneration of 15% of author fees

Associate members are eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get a remuneration of 15% of author fees, taken from the author of a respective paper.

Financial

And Much More

Get access to scientific museums and observatories across the globe

All members get access to 2 selected scientific museums and observatories across the globe. All researches published with Global Journals will be kept under deep archival facilities across regions for future protections and disaster recovery. They get 5 GB free secure cloud access for storing research files.

Associate	Fellow	Research Group	Basic
$4800 **lifetime designation**	$6800 **lifetime designation**	$12500.00 **organizational**	APC **per article**
Certificate, LoR and Momento **2** discounted publishing/year **Gradation** of Research **10** research contacts/day **1 GB** Cloud Storage **GJ** Community Access	**Certificate,** LoR and Momento **Unlimited** discounted publishing/year **Gradation** of Research **Unlimited** research contacts/day **5 GB** Cloud Storage **Online Presense** Assistance **GJ** Community Access	**Certificates,** LoRs and Momentos **Unlimited** free publishing/year **Gradation** of Research **Unlimited** research contacts/day **Unlimited** Cloud Storage **Online Presense** Assistance **GJ** Community Access	**GJ** Community Access

Preferred Author Guidelines

We accept the manuscript submissions in any standard (generic) format.

We typeset manuscripts using advanced typesetting tools like Adobe In Design, CorelDraw, TeXnicCenter, and TeXStudio. We usually recommend authors submit their research using any standard format they are comfortable with, and let Global Journals do the rest.

Alternatively, you can download our basic template from https://globaljournals.org/Template.zip

Authors should submit their complete paper/article, including text illustrations, graphics, conclusions, artwork, and tables. Authors who are not able to submit manuscript using the form above can email the manuscript department at submit@globaljournals.org or get in touch with chiefeditor@globaljournals.org if they wish to send the abstract before submission.

Before and during Submission

Authors must ensure the information provided during the submission of a paper is authentic. Please go through the following checklist before submitting:

1. Authors must go through the complete author guideline and understand and *agree to Global Journals' ethics and code of conduct,* along with author responsibilities.
2. Authors must accept the privacy policy, terms, and conditions of Global Journals.
3. Ensure corresponding author's email address and postal address are accurate and reachable.
4. Manuscript to be submitted must include keywords, an abstract, a paper title, co-author(s') names and details (email address, name, phone number, and institution), figures and illustrations in vector format including appropriate captions, tables, including titles and footnotes, a conclusion, results, acknowledgments and references.
5. Authors should submit paper in a ZIP archive if any supplementary files are required along with the paper.
6. Proper permissions must be acquired for the use of any copyrighted material.
7. Manuscript submitted *must not have been submitted or published elsewhere* and all authors must be aware of the submission.

Declaration of Conflicts of Interest

It is required for authors to declare all financial, institutional, and personal relationships with other individuals and organizations that could influence (bias) their research.

Policy on Plagiarism

Plagiarism is not acceptable in Global Journals submissions at all.

Plagiarized content will not be considered for publication. We reserve the right to inform authors' institutions about plagiarism detected either before or after publication. If plagiarism is identified, we will follow COPE guidelines:

Authors are solely responsible for all the plagiarism that is found. The author must not fabricate, falsify or plagiarize existing research data. The following, if copied, will be considered plagiarism:

- Words (language)
- Ideas
- Findings
- Writings
- Diagrams
- Graphs
- Illustrations
- Lectures

- Printed material
- Graphic representations
- Computer programs
- Electronic material
- Any other original work

Authorship Policies

Global Journals follows the definition of authorship set up by the Open Association of Research Society, USA. According to its guidelines, authorship criteria must be based on:

1. Substantial contributions to the conception and acquisition of data, analysis, and interpretation of findings.
2. Drafting the paper and revising it critically regarding important academic content.
3. Final approval of the version of the paper to be published.

Changes in Authorship

The corresponding author should mention the name and complete details of all co-authors during submission and in manuscript. We support addition, rearrangement, manipulation, and deletions in authors list till the early view publication of the journal. We expect that corresponding author will notify all co-authors of submission. We follow COPE guidelines for changes in authorship.

Copyright

During submission of the manuscript, the author is confirming an exclusive license agreement with Global Journals which gives Global Journals the authority to reproduce, reuse, and republish authors' research. We also believe in flexible copyright terms where copyright may remain with authors/employers/institutions as well. Contact your editor after acceptance to choose your copyright policy. You may follow this form for copyright transfers.

Appealing Decisions

Unless specified in the notification, the Editorial Board's decision on publication of the paper is final and cannot be appealed before making the major change in the manuscript.

Acknowledgments

Contributors to the research other than authors credited should be mentioned in Acknowledgments. The source of funding for the research can be included. Suppliers of resources may be mentioned along with their addresses.

Declaration of funding sources

Global Journals is in partnership with various universities, laboratories, and other institutions worldwide in the research domain. Authors are requested to disclose their source of funding during every stage of their research, such as making analysis, performing laboratory operations, computing data, and using institutional resources, from writing an article to its submission. This will also help authors to get reimbursements by requesting an open access publication letter from Global Journals and submitting to the respective funding source.

Preparing your Manuscript

Authors can submit papers and articles in an acceptable file format: MS Word (doc, docx), LaTeX (.tex, .zip or .rar including all of your files), Adobe PDF (.pdf), rich text format (.rtf), simple text document (.txt), Open Document Text (.odt), and Apple Pages (.pages). Our professional layout editors will format the entire paper according to our official guidelines. This is one of the highlights of publishing with Global Journals—authors should not be concerned about the formatting of their paper. Global Journals accepts articles and manuscripts in every major language, be it Spanish, Chinese, Japanese, Portuguese, Russian, French, German, Dutch, Italian, Greek, or any other national language, but the title, subtitle, and abstract should be in English. This will facilitate indexing and the pre-peer review process.

The following is the official style and template developed for publication of a research paper. Authors are not required to follow this style during the submission of the paper. It is just for reference purposes.

Manuscript Style Instruction (Optional)

- Microsoft Word Document Setting Instructions.
- Font type of all text should be Swis721 Lt BT.
- Page size: 8.27" x 11'", left margin: 0.65, right margin: 0.65, bottom margin: 0.75.
- Paper title should be in one column of font size 24.
- Author name in font size of 11 in one column.
- Abstract: font size 9 with the word "Abstract" in bold italics.
- Main text: font size 10 with two justified columns.
- Two columns with equal column width of 3.38 and spacing of 0.2.
- First character must be three lines drop-capped.
- The paragraph before spacing of 1 pt and after of 0 pt.
- Line spacing of 1 pt.
- Large images must be in one column.
- The names of first main headings (Heading 1) must be in Roman font, capital letters, and font size of 10.
- The names of second main headings (Heading 2) must not include numbers and must be in italics with a font size of 10.

Structure and Format of Manuscript

The recommended size of an original research paper is under 15,000 words and review papers under 7,000 words. Research articles should be less than 10,000 words. Research papers are usually longer than review papers. Review papers are reports of significant research (typically less than 7,000 words, including tables, figures, and references)

A research paper must include:

a) A title which should be relevant to the theme of the paper.
b) A summary, known as an abstract (less than 150 words), containing the major results and conclusions.
c) Up to 10 keywords that precisely identify the paper's subject, purpose, and focus.
d) An introduction, giving fundamental background objectives.
e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition, sources of information must be given, and numerical methods must be specified by reference.
f) Results which should be presented concisely by well-designed tables and figures.
g) Suitable statistical data should also be given.
h) All data must have been gathered with attention to numerical detail in the planning stage.

Design has been recognized to be essential to experiments for a considerable time, and the editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned unrefereed.

i) Discussion should cover implications and consequences and not just recapitulate the results; conclusions should also be summarized.
j) There should be brief acknowledgments.
k) There ought to be references in the conventional format. Global Journals recommends APA format.

Authors should carefully consider the preparation of papers to ensure that they communicate effectively. Papers are much more likely to be accepted if they are carefully designed and laid out, contain few or no errors, are summarizing, and follow instructions. They will also be published with much fewer delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and suggestions to improve brevity.

Format Structure

It is necessary that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

All manuscripts submitted to Global Journals should include:

Title

The title page must carry an informative title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) where the work was carried out.

Author details

The full postal address of any related author(s) must be specified.

Abstract

The abstract is the foundation of the research paper. It should be clear and concise and must contain the objective of the paper and inferences drawn. It is advised to not include big mathematical equations or complicated jargon.

Many researchers searching for information online will use search engines such as Google, Yahoo or others. By optimizing your paper for search engines, you will amplify the chance of someone finding it. In turn, this will make it more likely to be viewed and cited in further works. Global Journals has compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Keywords

A major lynchpin of research work for the writing of research papers is the keyword search, which one will employ to find both library and internet resources. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining, and indexing.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy: planning of a list of possible keywords and phrases to try.

Choice of the main keywords is the first tool of writing a research paper. Research paper writing is an art. Keyword search should be as strategic as possible.

One should start brainstorming lists of potential keywords before even beginning searching. Think about the most important concepts related to research work. Ask, “What words would a source have to include to be truly valuable in a research paper?” Then consider synonyms for the important words.

It may take the discovery of only one important paper to steer in the right keyword direction because, in most databases, the keywords under which a research paper is abstracted are listed with the paper.

Numerical Methods

Numerical methods used should be transparent and, where appropriate, supported by references.

Abbreviations

Authors must list all the abbreviations used in the paper at the end of the paper or in a separate table before using them.

Formulas and equations

Authors are advised to submit any mathematical equation using either MathJax, KaTeX, or LaTeX, or in a very high-quality image.

Tables, Figures, and Figure Legends

Tables: Tables should be cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g., Table 4, a self-explanatory caption, and be on a separate sheet. Authors must submit tables in an editable format and not as images. References to these tables (if any) must be mentioned accurately.

Figures

Figures are supposed to be submitted as separate files. Always include a citation in the text for each figure using Arabic numbers, e.g., Fig. 4. Artwork must be submitted online in vector electronic form or by emailing it.

Preparation of Eletronic Figures for Publication

Although low-quality images are sufficient for review purposes, print publication requires high-quality images to prevent the final product being blurred or fuzzy. Submit (possibly by e-mail) EPS (line art) or TIFF (halftone/ photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Avoid using pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings). Please give the data for figures in black and white or submit a Color Work Agreement form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution at final image size ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs): >350 dpi; figures containing both halftone and line images: >650 dpi.

Color charges: Authors are advised to pay the full cost for the reproduction of their color artwork. Hence, please note that if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a Color Work Agreement form before your paper can be published. Also, you can email your editor to remove the color fee after acceptance of the paper.

Tips for writing a good quality Computer Science Research Paper

Techniques for writing a good quality computer science research paper:

1. Choosing the topic: In most cases, the topic is selected by the interests of the author, but it can also be suggested by the guides. You can have several topics, and then judge which you are most comfortable with. This may be done by asking several questions of yourself, like "Will I be able to carry out a search in this area? Will I find all necessary resources to accomplish the search? Will I be able to find all information in this field area?" If the answer to this type of question is "yes," then you ought to choose that topic. In most cases, you may have to conduct surveys and visit several places. Also, you might have to do a lot of work to find all the rises and falls of the various data on that subject. Sometimes, detailed information plays a vital role, instead of short information. Evaluators are human: The first thing to remember is that evaluators are also human beings. They are not only meant for rejecting a paper. They are here to evaluate your paper. So present your best aspect.

2. Think like evaluators: If you are in confusion or getting demotivated because your paper may not be accepted by the evaluators, then think, and try to evaluate your paper like an evaluator. Try to understand what an evaluator wants in your research paper, and you will automatically have your answer. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

3. Ask your guides: If you are having any difficulty with your research, then do not hesitate to share your difficulty with your guide (if you have one). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work, then ask your supervisor to help you with an alternative. He or she might also provide you with a list of essential readings.

4. Use of computer is recommended: As you are doing research in the field of computer science then this point is quite obvious. Use right software: Always use good quality software packages. If you are not capable of judging good software, then you can lose the quality of your paper unknowingly. There are various programs available to help you which you can get through the internet.

5. Use the internet for help: An excellent start for your paper is using Google. It is a wondrous search engine, where you can have your doubts resolved. You may also read some answers for the frequent question of how to write your research paper or find a model research paper. You can download books from the internet. If you have all the required books, place importance on reading, selecting, and analyzing the specified information. Then sketch out your research paper. Use big pictures: You may use encyclopedias like Wikipedia to get pictures with the best resolution. At Global Journals, you should strictly follow here.

6. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right? It is a good habit which helps to not lose your continuity. You should always use bookmarks while searching on the internet also, which will make your search easier.

7. Revise what you wrote: When you write anything, always read it, summarize it, and then finalize it.

8. Make every effort: Make every effort to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in the introduction—what is the need for a particular research paper. Polish your work with good writing skills and always give an evaluator what he wants. Make backups: When you are going to do any important thing like making a research paper, you should always have backup copies of it either on your computer or on paper. This protects you from losing any portion of your important data.

9. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several unnecessary diagrams will degrade the quality of your paper by creating a hodgepodge. So always try to include diagrams which were made by you to improve the readability of your paper. Use of direct quotes: When you do research relevant to literature, history, or current affairs, then use of quotes becomes essential, but if the study is relevant to science, use of quotes is not preferable.

10.Use proper verb tense: Use proper verb tenses in your paper. Use past tense to present those events that have happened. Use present tense to indicate events that are going on. Use future tense to indicate events that will happen in the future. Use of wrong tenses will confuse the evaluator. Avoid sentences that are incomplete.

11. Pick a good study spot: Always try to pick a spot for your research which is quiet. Not every spot is good for studying.

12. Know what you know: Always try to know what you know by making objectives, otherwise you will be confused and unable to achieve your target.

13. Use good grammar: Always use good grammar and words that will have a positive impact on the evaluator; use of good vocabulary does not mean using tough words which the evaluator has to find in a dictionary. Do not fragment sentences. Eliminate one-word sentences. Do not ever use a big word when a smaller one would suffice.

Verbs have to be in agreement with their subjects. In a research paper, do not start sentences with conjunctions or finish them with prepositions. When writing formally, it is advisable to never split an infinitive because someone will (wrongly) complain. Avoid clichés like a disease. Always shun irritating alliteration. Use language which is simple and straightforward. Put together a neat summary.

14. Arrangement of information: Each section of the main body should start with an opening sentence, and there should be a changeover at the end of the section. Give only valid and powerful arguments for your topic. You may also maintain your arguments with records.

15. Never start at the last minute: Always allow enough time for research work. Leaving everything to the last minute will degrade your paper and spoil your work.

16. Multitasking in research is not good: Doing several things at the same time is a bad habit in the case of research activity. Research is an area where everything has a particular time slot. Divide your research work into parts, and do a particular part in a particular time slot.

17. Never copy others' work: Never copy others' work and give it your name because if the evaluator has seen it anywhere, you will be in trouble. Take proper rest and food: No matter how many hours you spend on your research activity, if you are not taking care of your health, then all your efforts will have been in vain. For quality research, take proper rest and food.

18. Go to seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

19. Refresh your mind after intervals: Try to give your mind a rest by listening to soft music or sleeping in intervals. This will also improve your memory. Acquire colleagues: Always try to acquire colleagues. No matter how sharp you are, if you acquire colleagues, they can give you ideas which will be helpful to your research.

20. Think technically: Always think technically. If anything happens, search for its reasons, benefits, and demerits. Think and then print: When you go to print your paper, check that tables are not split, headings are not detached from their descriptions, and page sequence is maintained.

21. Adding unnecessary information: Do not add unnecessary information like "I have used MS Excel to draw graphs." Irrelevant and inappropriate material is superfluous. Foreign terminology and phrases are not apropos. One should never take a broad view. Analogy is like feathers on a snake. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Never oversimplify: When adding material to your research paper, never go for oversimplification; this will definitely irritate the evaluator. Be specific. Never use rhythmic redundancies. Contractions shouldn't be used in a research paper. Comparisons are as terrible as clichés. Give up ampersands, abbreviations, and so on. Remove commas that are not necessary. Parenthetical words should be between brackets or commas. Understatement is always the best way to put forward earth-shaking thoughts. Give a detailed literary review.

22. Report concluded results: Use concluded results. From raw data, filter the results, and then conclude your studies based on measurements and observations taken. An appropriate number of decimal places should be used. Parenthetical remarks are prohibited here. Proofread carefully at the final stage. At the end, give an outline to your arguments. Spot perspectives of further study of the subject. Justify your conclusion at the bottom sufficiently, which will probably include examples.

23. Upon conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print for the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects of your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form which is presented in the guidelines using the template.
- Please note the criteria peer reviewers will use for grading the final paper.

Final points:

One purpose of organizing a research paper is to let people interpret your efforts selectively. The journal requires the following sections, submitted in the order listed, with each section starting on a new page:

The introduction: This will be compiled from reference matter and reflect the design processes or outline of basis that directed you to make a study. As you carry out the process of study, the method and process section will be constructed like that. The results segment will show related statistics in nearly sequential order and direct reviewers to similar intellectual paths throughout the data that you gathered to carry out your study.

The discussion section:

This will provide understanding of the data and projections as to the implications of the results. The use of good quality references throughout the paper will give the effort trustworthiness by representing an alertness to prior workings.

Writing a research paper is not an easy job, no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record-keeping are the only means to make straightforward progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear: Adhere to recommended page limits.

Mistakes to avoid:

- Insertion of a title at the foot of a page with subsequent text on the next page.
- Separating a table, chart, or figure—confine each to a single page.
- Submitting a manuscript with pages out of sequence.
- In every section of your document, use standard writing style, including articles ("a" and "the").
- Keep paying attention to the topic of the paper.
- Use paragraphs to split each significant point (excluding the abstract).
- Align the primary line of each section.
- Present your points in sound order.
- Use present tense to report well-accepted matters.
- Use past tense to describe specific results.
- Do not use familiar wording; don't address the reviewer directly. Don't use slang or superlatives.
- Avoid use of extra pictures—include only those figures essential to presenting results.

Title page:

Choose a revealing title. It should be short and include the name(s) and address(es) of all authors. It should not have acronyms or abbreviations or exceed two printed lines.

Abstract: This summary should be two hundred words or less. It should clearly and briefly explain the key findings reported in the manuscript and must have precise statistics. It should not have acronyms or abbreviations. It should be logical in itself. Do not cite references at this point.

An abstract is a brief, distinct paragraph summary of finished work or work in development. In a minute or less, a reviewer can be taught the foundation behind the study, common approaches to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Use comprehensive sentences, and do not sacrifice readability for brevity; you can maintain it succinctly by phrasing sentences so that they provide more than a lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study with the subsequent elements in any summary. Try to limit the initial two items to no more than one line each.

Reason for writing the article—theory, overall issue, purpose.

- Fundamental goal.
- To-the-point depiction of the research.
- Consequences, including definite statistics—if the consequences are quantitative in nature, account for this; results of any numerical analysis should be reported. Significant conclusions or questions that emerge from the research.

Approach:

- Single section and succinct.
- An outline of the job done is always written in past tense.
- Concentrate on shortening results—limit background information to a verdict or two.
- Exact spelling, clarity of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else.

Introduction:

The introduction should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable of comprehending and calculating the purpose of your study without having to refer to other works. The basis for the study should be offered. Give the most important references, but avoid making a comprehensive appraisal of the topic. Describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will give no attention to your results. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here.

The following approach can create a valuable beginning:

- Explain the value (significance) of the study.
- Defend the model—why did you employ this particular system or method? What is its compensation? Remark upon its appropriateness from an abstract point of view as well as pointing out sensible reasons for using it.
- Present a justification. State your particular theory(-ies) or aim(s), and describe the logic that led you to choose them.
- Briefly explain the study's tentative purpose and how it meets the declared objectives.

Approach:

Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done. Sort out your thoughts; manufacture one key point for every section. If you make the four points listed above, you will need at least four paragraphs. Present surrounding information only when it is necessary to support a situation. The reviewer does not desire to read everything you know about a topic. Shape the theory specifically—do not take a broad view.

As always, give awareness to spelling, simplicity, and correctness of sentences and phrases.

Procedures (methods and materials):

This part is supposed to be the easiest to carve if you have good skills. A soundly written procedures segment allows a capable scientist to replicate your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order, but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt to give the least amount of information that would permit another capable scientist to replicate your outcome, but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section.

When a technique is used that has been well-described in another section, mention the specific item describing the way, but draw the basic principle while stating the situation. The purpose is to show all particular resources and broad procedures so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step-by-step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

Materials may be reported in part of a section or else they may be recognized along with your measures.

Methods:

- Report the method and not the particulars of each process that engaged the same methodology.
- Describe the method entirely.
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures.
- Simplify—detail how procedures were completed, not how they were performed on a particular day.
- If well-known procedures were used, account for the procedure by name, possibly with a reference, and that's all.

Approach:

It is embarrassing to use vigorous voice when documenting methods without using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result, when writing up the methods, most authors use third person passive voice.

Use standard style in this and every other part of the paper—avoid familiar lists, and use full sentences.

What to keep away from:

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings—save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part as entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Use statistics and tables, if suitable, to present consequences most efficiently.

You must clearly differentiate material which would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matters should not be submitted at all except if requested by the instructor.

Content:

- Sum up your conclusions in text and demonstrate them, if suitable, with figures and tables.
- In the manuscript, explain each of your consequences, and point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation of an exacting study.
- Explain results of control experiments and give remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or manuscript.

What to stay away from:

- Do not discuss or infer your outcome, report surrounding information, or try to explain anything.
- Do not include raw data or intermediate calculations in a research manuscript.
- Do not present similar data more than once.
- A manuscript should complement any figures or tables, not duplicate information.
- Never confuse figures with tables—there is a difference.

Approach:

As always, use past tense when you submit your results, and put the whole thing in a reasonable order.

Put figures and tables, appropriately numbered, in order at the end of the report.

If you desire, you may place your figures and tables properly within the text of your results section.

Figures and tables:

If you put figures and tables at the end of some details, make certain that they are visibly distinguished from any attached appendix materials, such as raw facts. Whatever the position, each table must be titled, numbered one after the other, and include a heading. All figures and tables must be divided from the text.

Discussion:

The discussion is expected to be the trickiest segment to write. A lot of papers submitted to the journal are discarded based on problems with the discussion. There is no rule for how long an argument should be.

Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implications of the study. The purpose here is to offer an understanding of your results and support all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of results should be fully described.

Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact, you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved the prospect, and let it drop at that. Make a decision as to whether each premise is supported or discarded or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."

Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work.

- You may propose future guidelines, such as how an experiment might be personalized to accomplish a new idea.
- Give details of all of your remarks as much as possible, focusing on mechanisms.
- Make a decision as to whether the tentative design sufficiently addressed the theory and whether or not it was correctly restricted. Try to present substitute explanations if they are sensible alternatives.
- One piece of research will not counter an overall question, so maintain the large picture in mind. Where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

When you refer to information, differentiate data generated by your own studies from other available information. Present work done by specific persons (including you) in past tense.

Describe generally acknowledged facts and main beliefs in present tense.

The Administration Rules

Administration Rules to Be Strictly Followed before Submitting Your Research Paper to Global Journals Inc.

Please read the following rules and regulations carefully before submitting your research paper to Global Journals Inc. to avoid rejection.

Segment draft and final research paper: You have to strictly follow the template of a research paper, failing which your paper may get rejected. You are expected to write each part of the paper wholly on your own. The peer reviewers need to identify your own perspective of the concepts in your own terms. Please do not extract straight from any other source, and do not rephrase someone else's analysis. Do not allow anyone else to proofread your manuscript.

Written material: You may discuss this with your guides and key sources. Do not copy anyone else's paper, even if this is only imitation, otherwise it will be rejected on the grounds of plagiarism, which is illegal. Various methods to avoid plagiarism are strictly applied by us to every paper, and, if found guilty, you may be blacklisted, which could affect your career adversely. To guard yourself and others from possible illegal use, please do not permit anyone to use or even read your paper and file.

Criterion for Grading a Research Paper (Compilation) by Global Journals Inc. (US)

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

Topics	Grades		
	A-B	**C-D**	**E-F**
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

INDEX

save our planet

Global Journal of Computer Science and Technology

Visit us on the Web at www.GlobalJournals.org | www.ComputerResearch.org
or email us at helpdesk@globaljournals.org

ISSN 9754350