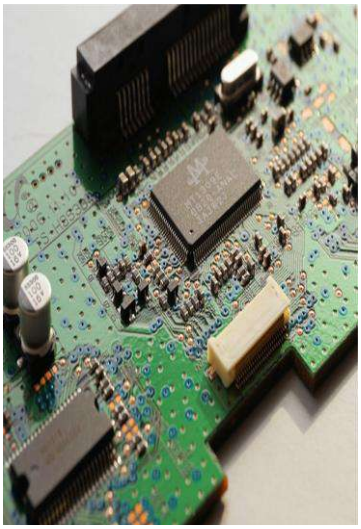
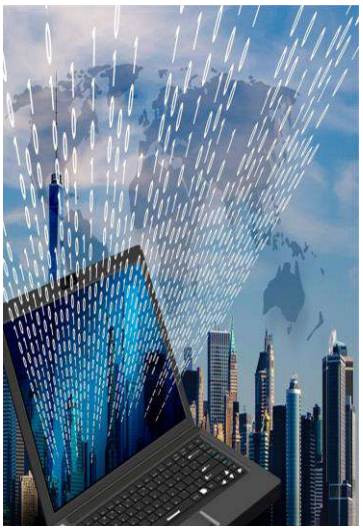
ISBN: 9780995707542

INTERNATIONAL JOURNAL of ENGINEERING AND APPLIED COMPUTER SCIENCE

EMPIRICAL RESEARCH PRESS

Volume: 04 | Issue: 02 | March | 2022



EMPIRICAL RESEARCH PRESS LTD.
London, United Kingdom

IJEACS

International Journal of

Engineering and Applied Computer Science

Empirical Research Press Ltd.

London, United Kingdom

Volume: 04, Issue: 02

ISBN: 9780995707542

www.ijeacs.com

Indexing, Hosting and Advertising

Message

International Journal of Engineering and Applied Computer Science (IJEACS) is open access, double-blind peer-reviewed international journal, monthly online publishing by Empirical Research Press Ltd. Empirical Research Press is a research publishing company with the name, trademark registered, incorporated in England and Wales, United Kingdom.

The scope of the International Journal of Engineering and Applied Computer Science is to publish high-quality research contributions, latest innovations, advanced development carried out in the field of Engineering, Computer Science, and Technology. The original research, review, case study, survey, new interpretation and implementation of concepts and theories, recent technological development, technical reports, empirical discussions are invited to submit for publication.

The major objectives of the International Journal of Engineering and Applied Computer Science are to maintain the high quality of publications and indexing with the world's highly accessed and cited research and academic databases. The scope of IJEACS publications also includes special and interdisciplinary research contributions. We offer best wishes to readers, reviewers, and contributors of IJEACS.

Board Members of IJEACS

Content

Empirical Research Press Ltd.
London, United Kingdom

International Journal of
Engineering and Applied Computer Science

Volume: 04, Issue: 02, March 2022 ISBN: 9780995707542

Mangrove Ecotourism Information System Based on Digital Book and Online Reservations

I Gede Sujana Eka Putra
Institute of Business and Technology Indonesia, Denpasar Bali, Indonesia

10.24032/IJEACS/0402/005

Mangrove Ecotourism Information System Based on Digital Book and Online Reservations

***Abstract*— Bali's tourism sector has faced serious challenges since the pandemic, with Bali's economic growth rate of -12.28% in the third quarter of 2020. Kampoeng Kepiting Mangrove Ecotourism located in Tuban, Kuta Badung district, Bali province is one of the tourism sectors which suffered a heavy impact. Before the pandemic, ecotourism visitors increased however during the pandemic, the number of visits decreased significantly. This study aims to develop a mangrove ecotourism information system, based on digital books and online reservations. The ecotourism digital book outlines the catalog of tour packages offered along with information on the mangrove tour packages for conservation and education. Based on the information from a digital book, potential visitors can use an online reservation application to make a reservation for tour packages and do payment by bank transfer. Once the payment process is done, visitors get digital vouchers to use the tour packages they have been reserved. The E-Voucher was used to visit the ecotourism of Kampoeng Kepiting. The development of a mangrove information system is expected to support the promotion of ecotourism in the recovery of ecotourism during the COVID-19 pandemic.**

Keywords- Kampoeng Kepiting, Ecotourism, Digital Book, Online Reservation

I. INTRODUCTION

The tourism sector in Bali is experiencing a fairly heavy impact due to the prolonged pandemic, which affects the economic level of the community. There has been a decline in Bali's economic growth rate of -12.28% since 2020 [1]. In the context of the economic recovery of the Bali tourism sector, a new strategy breakthrough is needed, tourists prioritize cleanliness, health, and practical ways, so a strategy is needed to develop ecotourism with digital-based modeling. One of the affected tourism sectors is the Kampoeng Kepiting mangrove ecotourism, which has been operating since 2008, managed by Wanasari fishermen in Tuban Village, Bali Indonesia.

Mangrove ecotourism areas themselves have several sub-activities, namely crab cultivation, mangrove education, mangrove processing, and marketing groups, community groups overseeing mangroves, cultural arts activities, water tourism, and culinary tourism [5]. Since before the pandemic until 2019, tourist visits have increased, but since the pandemic, until now mangrove ecotourism has stopped temporarily

The problems encountered are the absence of tourists and visitors who visit mangrove ecotourism, which is usually crowded with visitors, currently quiet/no visitors. This impacts the livelihoods of the Tuban Wanasari fisherman group, which partly depends on mangrove ecotourism for their economy. The current condition of mangrove ecotourism in its activities is still applying the manual method in tourism management. This study develops a mangrove ecotourism information system in the form of digital book applications and online reservations that support ecotourism promotion. Digital books are accessed online to describe the types and packages of mangrove tours. The online reservation application helps prospective visitors make their reservations on mangrove tour packages, after the payment process the system issues digital tour package vouchers. Ecotourism is the face of the future of tourism from the development of new lifestyles and awareness of the people who are increasingly caring about the natural environment. The industry 4.0 era affects various sectors, including the tourism sector. For example, now travelers simply rely on digital platforms to search, order, and even make payments. Tourism 4.0 is also known as Millennial Tourism. Currently, the growing traveler portfolio is the millennial generation where 50 percent of inbound travelers are millennials [7]. This is reinforced by data from Deloitte Consulting Southeast Asia 2019 which states that 40 percent of global tour and booking activity is done online [8]. This ecotourism can build the economy of fishermen, the availability of jobs, changes in livelihoods, mindset change, and ability development.

II. RESEARCH METHODS

A. *Stage of Research*

The research was conducted in mangrove ecotourism Kampoeng Kepiting Tuban, Badung Bali. The methods are carried out by digital books, and online reservations. Digital books could be accessed online which contains information and photos about tourism objects such as mangrove forest visits, mangrove nurseries, seed planting activities, mangrove forest conservation, culinary tours, and other activities. The digital online reservation is used by the visitor to reserve the ecotourism package by choosing the tour package provided. The stage of the research is shown in Figure 1.

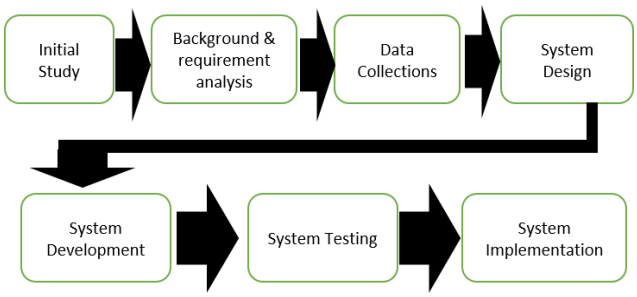


Figure 1. Stage of the Research

B. System Overview

A system overview is shown in Figure 2, starting with potential visitors wanting to know about ecotourism products and services through the digital promotion book application. Prospective visitors get a complete picture of the products and services provided by the tourism object to be visited. Prospective visitors can at the same time purchase by transfer of funds for the selected tour package. Visitors can first register personal data which then gets a Visitor ID. When a prospective visitor visits an ecotourism object, the visitor shows vouchers that have been purchased previously, in the form of a digital QR Code that can be used to pick up a tour package, by showing the voucher are then scanned by the officer, which indicates the visitor has taken the tour package.

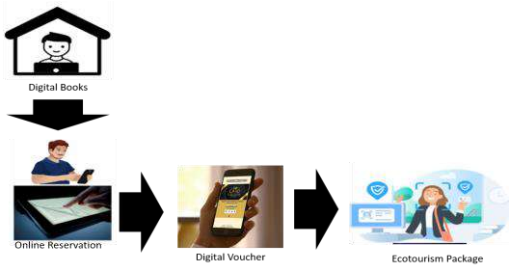


Figure 2. System Overview

The preliminary study activity aims to plan and coordinate activities to be carried out related to the Kampoeng Kepiting ecotourism digitalization model. The data collection activity by reviewing the research location and collecting data related to the latest ecotourism conditions as shown in Figure 3.

Figure 3. Preliminary Study and Interview

The system development method in this study uses the Prototyping development method, a systematic software development method, that has several stages including preliminary study, requirement analysis, software design, create prototyping, customer evaluation, software update, system development, software testing, and software implementation. The prototyping model is shown in Figure 4.

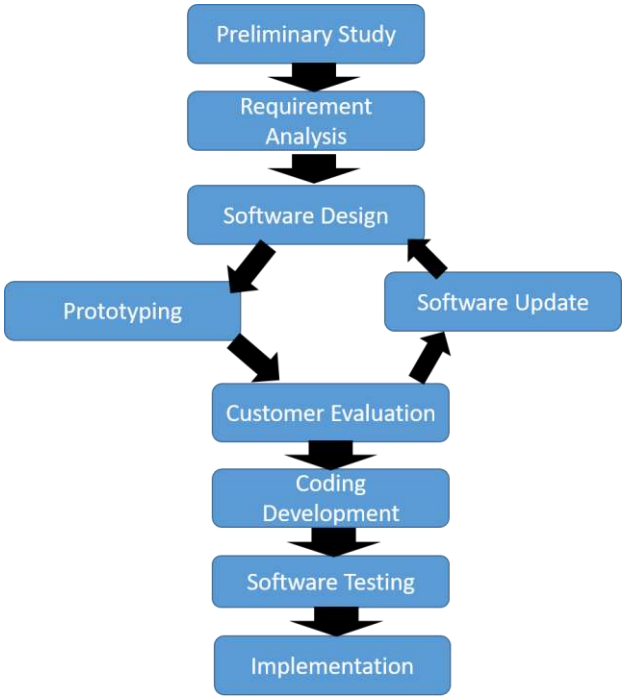


Figure 4. Prototyping Model Software Development

III. RESULTS AND DISCUSSIONS

The database design in the development of a relational-based ecotourism system in the form of a physical data model is shown in Figure 5.

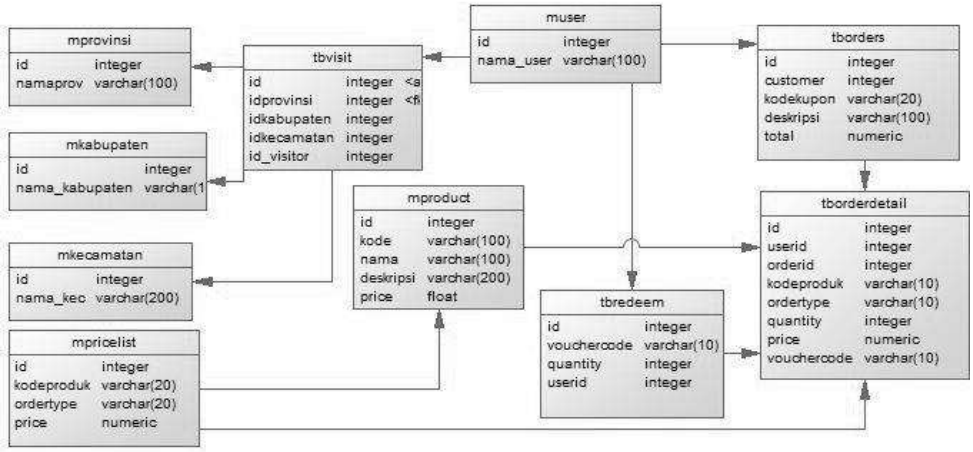


Figure 5. Physical Data Model Ecotourism Database

Visitor data and users are stored in the muser table, tour package product data is stored in the mproduct table, visitor reservation data is stored in the tborders and tborderdetail tables. Meanwhile, voucher usage data (redeem) is stored in the tbreedem table. Meanwhile, the price of the tour package is stored in the mpricelist table. All of these tables are related to each other as the basis for the concept of database normalization.

Data Flow Diagram is a diagram that describes the flow of data from a process that is often referred to as an information system. Data flow diagrams also provide information about the inputs and outputs of each entity and the process itself. Figure 6 shows a context diagram of a mangrove ecotourism information system

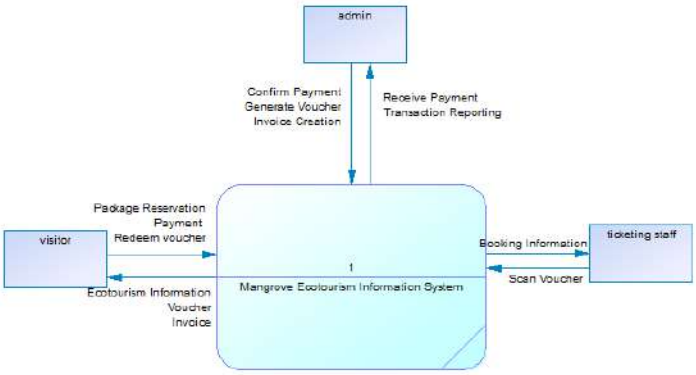


Figure 6. Context Diagram

The context diagram design is shown in Figure 6, which are 3 entities involved, the visitor entity, the admin entity, and the ticketing staff.

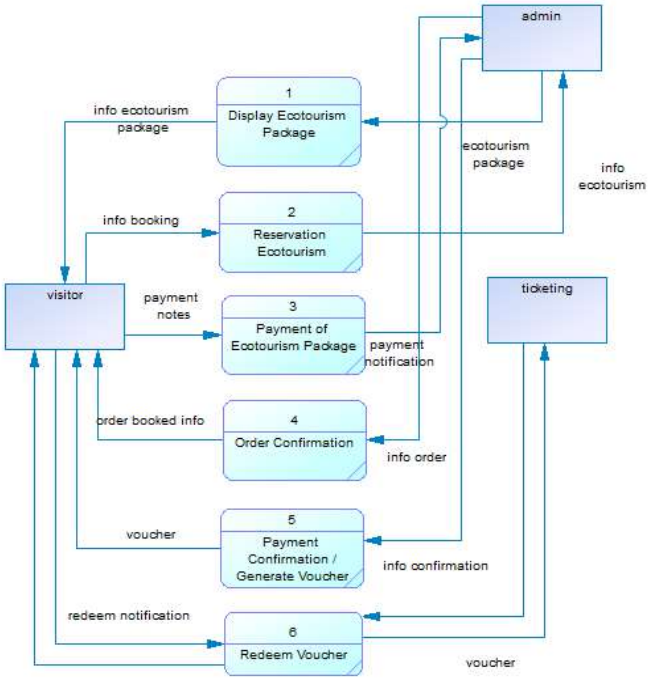


Figure 7. Design of Data Flow Diagram Level 1

The level 1 data flow diagram design is described in Figure 7, which is a description of the context diagram with a description of several processes in it, with the number of entities associated with the context diagram design.

The digital book application can help to promote Kampoeng Kepiting tour packages online. The application displays the available tour packages. The digital book could be seen in Figure 8.

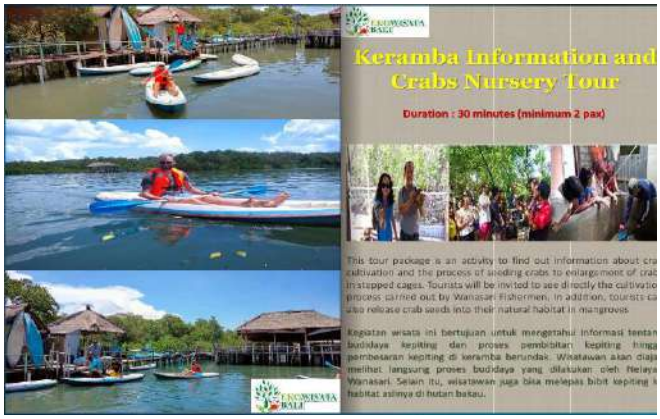


Figure 8. Digital Books for Crabs Nursery Tour

Crab Nursery Tour display crab nursery tour packages where tourists are invited to go around to see the crab cages in the location along with how to breed crabs.

Figure 9. Digital Books for Making Mangrove Seed Tour

Figure 9 shows the activity of making mangrove seed tours where tourists are invited to learn how to make mangrove seedlings and sow seeds in coastal water areas before planting. Making seeds, planting in polybags, and arranging them in the nursery until they are ready to be planted.

The online reservation application can be used by prospective visitors to make reservations and purchase tour package vouchers before visiting ecotourism locations. This application aims to implement digitalization in booking tour packages by using advance payments and implementing a voucher system, thereby reducing direct contact with visitors and ecotourism organizers in the payment process. The

appearance of the tour package reservation application begins with the user logging in or creating a new account to be able to login into the application as shown in Figure 10.

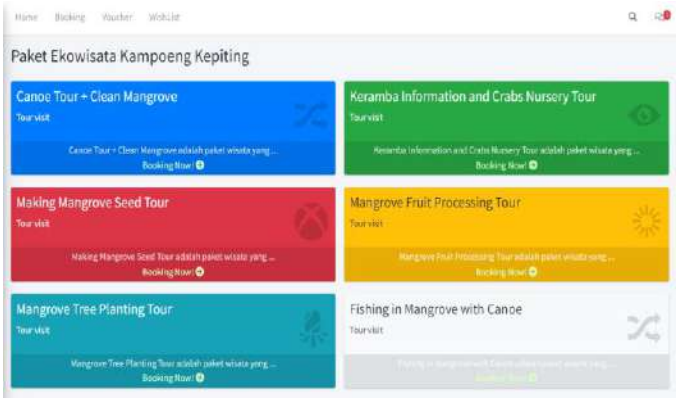


Figure 10. Online Reservation Ecotourism Packages

The online reservation below displays the tour packages offered in Kampoeng Kepiting. There are booking menus, voucher menus, wish list menus, price list menus that can be used by tourists as a reference for making tour package reservations, as shown in Figure 10.

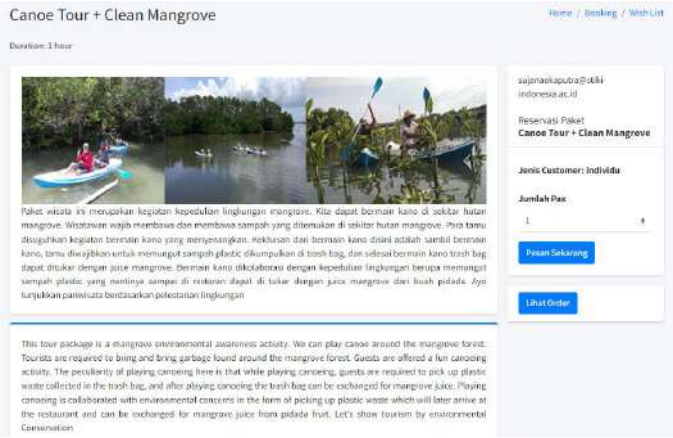
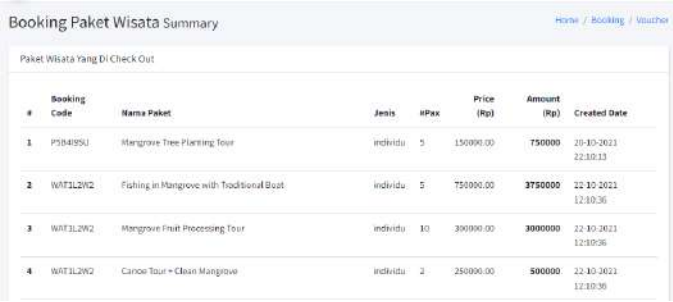


Figure 11. Canoe Tour and Clean Mangrove Packages

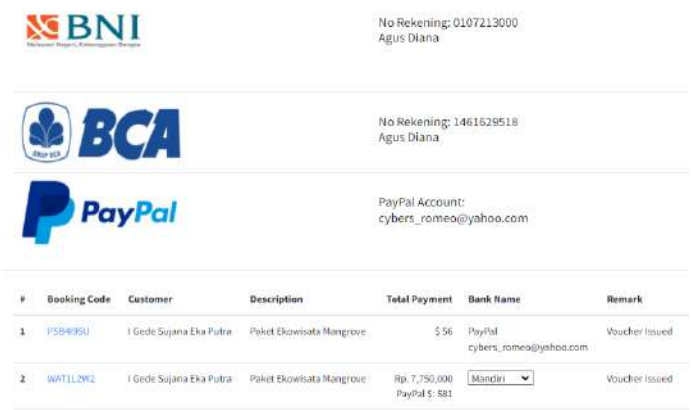
Figure 11 describe canoe tour and clean mangrove packages. This is a mangrove environmental awareness activity, while visitors play canoe around the mangrove forest and are required to bring garbage found around the mangrove forest, and once landing the visitor is served fresh mangrove juice.



#	Booking Code	Nama Paket	Jenis	#Pax	Price (Rp)	Amount (Rp)	Created Date
1	P5B49SU	Mangrove Tree Planting Tour	individu	5	150000.00	750000	20-10-2021 22:10:13
2	WAT1L2W2	Fishing in Mangrove with Traditional Boat	individu	5	750000.00	3750000	22-10-2021 12:10:36
3	WAT1L2W2	Mangrove Fruit Processing Tour	individu	10	300000.00	3000000	22-10-2021 12:10:36
4	WAT1L2W2	Canoe Tour + Clean Mangrove	individu	2	250000.00	500000	22-10-2021 12:10:36

Figure 12. Booking List Ecotourism Package

Figure 12 describes the booking list of the package consisting of package name, visitor type, total pax, and package price. The bottom displays the total cost of the booking order. The tour package that has been ordered can then be selected for booking confirmation by pressing the "Check Out" button. Once Check-Out, the system automatically generates a booking code, then displays the summary of the booking order.



#	Booking Code	Customer	Description	Total Payment	Bank Name	Remark
1	P5B49SU	I Gede Sujana Eka Putra	Paket Ekowisata Mangrove	$ 56	PayPal cybers_romeo@yahoo.com	Voucher Issued
2	WAT1L2W2	I Gede Sujana Eka Putra	Paket Ekowisata Mangrove	Rp. 7,750,000 PayPal $: 581	Mandiri	Voucher Issued

Figure 13. Payment Methods Package Booked

Figure 13 shows the payment method for the packages booked, where this module contains information about the bank account for payment or use PayPal account. Each package consists of a booking code, description, and total payment. Furthermore, if the payment has been made, the tour package manager can check and confirm the payment that has been made to create a voucher.

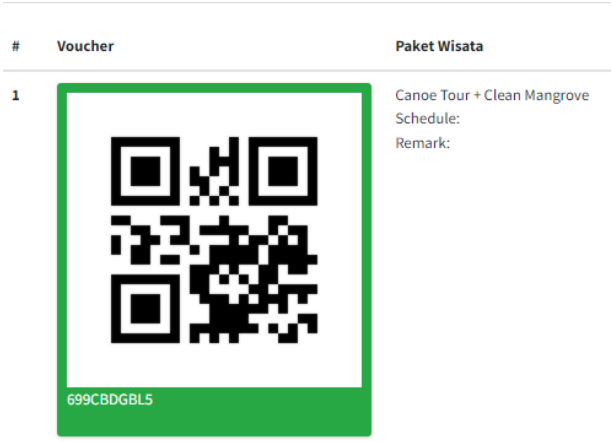


Figure 14. Ecotourism Voucher Package

Figure 14 shows the ecotourism voucher package created by the system automatically after the payment is confirmed by the admin. Furthermore, visitors can use the voucher to enjoy the ecotourism package.

System testing is done by using black-box testing. Black box testing is one of the software testing methods that focuses on the functionality side, especially on application input and output (whether it is in accordance with what is expected or not). The results of testing the digital book application are shown in Table I.

TABLE I. DIGITAL BOOKS APPLICATION TESTING

No	Module Name	Remark
1	Digital Books application	The application describes tour package information properly for each page without errors being found. The website can be accessed on the page: www.kampoengkepiting.com

TABLE II. ONLINE RESERVATION MANGROVE ECOTOURISM

No	Module Name	Remark
1	Login and register account	The application can validate logins and passwords. The application has successfully logged into the online reservation application with the registered email password
2	Dashboard application	The application can display the details of the tour package after the dashboard is clicked.
3	Booked Now	the application can record the number of pax ordered according to the selected tour package
4	List of Booking Package	the application can display tour packages that have been booked
5	Check out booking	the application can check out orders that have been booked, and enter the payment menu
6	Payment Confirmation	the application can confirm payment, make tour package vouchers, and display tour package vouchers

The implementation model of the mangrove ecotourism system is broadly shown in Table III.

TABLE III. OVERVIEW OF THE SYSTEM IMPLEMENTATION MODEL

No	Module Name	Remark
1	Digital Books	Prospective visitors can view ecotourism tour packages online
2	Ecotourism Package	Prospective visitors register and then view tour packages on the website
3	Reservation Menu	Visitors can make a reservation of tour packages and then the system creates summary orders and provides payment information. Prospective visitors make payments via bank transfer (national) or via PayPal account (international)
4	Payment Confirmation	Admin checks payments and confirms payments. If the payment is done, the payment is confirmed and the system issues a tour package voucher for visitors (QR Code)

IV. SUMMARY

The conclusions from this research are as follows:

A. The digital ecotourism model implemented is in the form of digital book media applications, online reservations / digital vouchers.

B. Digital book applications and online reservations provide complete information on tour packages and make it easier to book the packages that can be accessed anywhere and anytime.

C. The system test results show the system runs according to its function and is error-free.

REFERENCES

[1] Badan Pusat Statistik Provinsi D.I Yogyakarta, "Berita Resmi Statistik," Bps.Go.Id, no. 27, pp. 1–8, 2019, [Online]. Available: https://papua.bps.go.id/pressrelease/2018/05/07/336/indeks-pembangunan-manusia-provinsi-papua-tahun-2017.html.

[2] kompas, "Sanur, Ubud, dan Nusa Dua Disiapkan sebagai "Green Zone" di Bali," 2021.

[3] www.cnnindonesia.com/, "Sandiaga Bakal 'Buka Pintu' Bali Bagi Turis Asing Pada Juni," https://www.cnnindonesia.com/, 2021.

[4] I. G. M. I. S. Wardani and I. P. Anom, "Dampak Sosial Ekonomi Pengelolaan Ekowisata Mangrove Kampoeng Kepiting Terhadap Nelayan Desa Tuban Kabupaten Badung pengorganisasian , pengendalian , penempatan , pengambilan keputusan yang dilakukan oleh setiap organisasi dengan tujuan untuk mengkoordina," J. Destin. Pariwisata, vol. 5, no. 1, pp. 72–77, 2017.

[5] N. W. N. S. Wardani and I. G. A. Wesnawa, "Potensi Ekowisata Kampoeng Kepiting Di Desa Tuban, Kecamatan Kuta, Kabupaten Badung," J. Pendidik. Geogr. Undiksha, vol. 6, no. 1, pp. 1–12, 2018, doi: 10.23887/jjpg.v6i1.20678.

[6] E. H. dan R. Mardiana, "Pengaruh Ekowisata Berbasis Masyarakat Terhadap Perubahan Kondisi Ekologi, Sosial Dan Ekonomi Di Kampung Batusuhunan, Sukabumi," J. Sosiol. Pedesaan, vol. 2, no. 3, pp. 146–159, 2014.

[7] Indonesiainside.id, "50 Persen Wisatawan Indonesia Adalah Kelompok Milenial," 2019.

[8] B. Rhama, "Peluang Ekowisata Dalam Industri 4.0 di Indonesia," J. Ilmu Sos. Polit. dan Pemerintah., vol. 8, no. 2, pp. 37–49, 2019, [Online]. Available: https://e-journal.upr.ac.id/index.php/JISPAR/article/view/1036.

[9] Jogiyanto H M, Analisis dan desain: sistem informasi pendekatan terstruktur teori dan praktek aplikasi bisnis. Yogyakarta: Andi Offset, 2005.

[10] M. Bulman, "SDLC - Waterfall Model," Indep., 2017.

AUTHOR PROFILE

Mr. I Gede Sujana Eka Putra is studying in doctoral program at Udayana University, Bali Indonesia. He graduated with a bachelor's degree in multimedia telecommunications at the Sepuluh Nopember Institute of Technology, Surabaya, and a master's degree in Management of Computer Information Systems at Udayana University. He has more than 18 years of experience working in the field of information technology and he has developed a traceability information system for the fish processing industry and the application called “TraceTales”. Sujana is committed to continuing to play an active role in developing and implementing technology to support sustainable fisheries. Currently, he is active in conducting research about developing an information system of fisheries traceability system from upstream (catch), processing into downstream (end customer). His research interest includes the Internet of Things (IoT), Biometrics, Machine Learning, Artificial Neural Network. He has attended 3 national conferences, presented 3 papers, published 4 papers in International Journals and 9 papers in National Journals indexed.

Empirical Research Press Ltd.
London, United Kingdom

International Journal of
Engineering and Applied Computer Science

Volume: 04, Issue: 02, March 2022 ISBN: 9780995707542

Analysis of Most Common Encryption Algorithms

Attique Ahmed[1], *Muhammad Naeem*[2]

[1,2] Department of Computer Science, Abbottabad University of Science and Technology, Pakistan

10.24032/IJEACS/0402/003

Volume: 04, Issue: 02, ISBN: 9780995707542, March 2022

Analysis of Most Common Encryption Algorithms

***Abstract*—As the things are settled down after the emergence of technology, and this is the decade of professionalism as far as technology is concerned, security of data is the major hurdle in this race. This is the era in which data is one click away from the users, so data needs to be more secured so that it can be avoided unauthorized access. For this purpose, different data security fields have also emerged to ensure data security and confidentiality. In this survey paper we will look up all the techniques used for data encryption and after that, we compare those techniques to provide the best algorithm to ensure that data is secured. We go categorically, as in most of the cases, symmetric encryption technique is applicable and, in a few cases, asymmetric is recommended. Firstly, in our study, we compare both the techniques with each other and then compare all the algorithms working under the above-mentioned categories concerning their time, efficiency, memory usage, latency, key size, and several rounds which will result in showing the best algorithm according to input data.**

Keywords- Encryption, Cryptography, Symmetric, Asymmetric, data security, algorithm.

I. INTRODUCTION

The settlement of technology and software programs used these days has facilitated malicious customers to intercept information at some stage in data transmission [2]. As a result, it's far extraordinarily crucial for any corporation or person to guard their touchy and treasured records. Security frequently looks up retaining the information secure from unauthorized access to maintain the quality line of defense [9]. Encryption is a method to save data so that the information stays unchanged and guarded at some stage in the information transmission from the sender to the meant recipient [26]. Encryption is described as the procedure of concealing records from intruders or unauthorized persons [14]. Conversely, decryption is the procedure of changing records again into the record's regular layout [14].

People and organizations are being subjected to protection incidents including breaches of privacy and identity theft. As a result, people's monetary facts were stolen, online debts were given illegally accessed, and to a degree person names and passwords were given posted to the public. In 2021, there were 1291 protection incidents and forty-four million data were compromised amongst exceptional businesses. The hike of security breaches was up to 17% as compared to the year 2020 [28]. Moreover, those affected businesses incur large quantities of losses in phrases of stolen budgets and different costs in the aftermath of the incidents [20].

To mitigate the security threats as far as data is concerned; encryption techniques and algorithms were designed right from the emergence of new technology. There are two types of Encryption algorithms which are named Symmetric and Asymmetric algorithms which have their pros and cons respectively. An in-depth study reveals that it varies from case to case in selecting the optimal encryption algorithm [18].

II. FUNDAMENTALS OF STUDY

Data Security has become a crucial factor nowadays, mainly with current exchange networks, which have drawbacks that might be leveraged to devastating effects. In our study, we afford a few dialogues on famous encryption algorithms that may be used to tighten data protection in Symmetric/ Asymmetric Encryption. The best manner to start this debate is to begin from the fundamentals first. Thus, we study definitions of algorithms and basic cryptographic standards after which dive into the center part of the dialogue in which we give an evaluation of two techniques [3][16].

A. Algorithm

The algorithm is a set of rules, a method, or a system for fixing a problem. An encrypted set of rules is a fixed mathematical method for acting encryption on facts. Through using such a set of rules, data is made inside cipher textual content and calls for using a key to remodeling facts into their unique shape [15]. This brings us to the idea of cryptography that has been lengthy and has been utilized in data protection in data communication.

B. Cryptography

Cryptography is a way of the use of superior mathematical concepts in storing and transmitting data in a specific shape so that is understood by the ones whom it's supposed can examine and the method it. Encryption is key idea in cryptography [13][17]. It is the method in which a message is encoded in a layout that can't be examined or understood without the aid of using a key. A simple content from a person may be encrypted to ciphertext, and then processed through a data exchange channel so no one can intrude with obvious textual content. When it hits the receiver end, the ciphertext is decrypted to the original simple content [22].

C. Encryption

It is the method of locking up data with the use of cryptography. The data that has been protected in this manner is encrypted [1].

D. Decryption

The method of opening the encrypted data by using cryptographic methods [1].

E. Key

A piece of hidden information like a password is used to encrypt and decrypt data. There are some distinct kinds of keys utilized in cryptography [4].

F. Steganography

It is truly the technological know-how of hiding data from hackers and unknown people that could harm you. The distinction between steganography and encryption is that the snoopers won't have the ability to comprehend there are any hidden data in the picture, text, or any other media [26].

G. Symmetric Encryption

This is the most effective type of encryption that provides one hidden key to cipher and decrypt data [22]. Symmetric encryption is an ancient and well-known method. In this method, the mystery key is used which may be a number, a phrase, or a string of arbitrary letters. It is mixed with the obvious textual data or a message to enclose the content material in a specific manner. The sender and recipient must know the name of the key which is used to encrypt and decrypt all of the messages. Blowfish, Twofish, AES, DES, 3DES, and RCG are examples of symmetric encryption. The broadly used symmetric set of rules is AES-128, AES-256, and blowfish. See Figure 1.

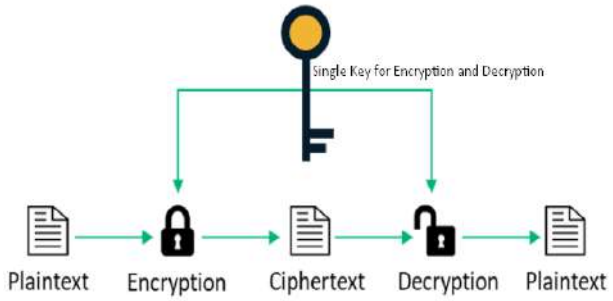


Figure 1. Symmetric Key Encryption

H. Asymmetric Encryption

Asymmetric encryption can also be named public-key encryption which is comparatively a new method, as compared to symmetric encryption. Asymmetric encryption makes use of two keys to encrypt simple textual content namely a public key and a private key [29]. Secret keys are then exchanged over the Internet or a massive network. It guarantees that hackers/snoopers cannot misuse the keys. It is critical to observe that absolutely anyone with this key can decrypt the message and that is why such encryption makes use of associated keys to enhance protection [2]. A public key is made generously had to absolutely everyone who would possibly need to send or receive a message.

A message encrypted with the use of a public key can best be decrypted using a private key; a message encrypted by the use of a personal key may be decrypted by the use of a public key. Security of general public key is not always required because it's far from publicly to be had and may be surpassed over the internet [38].

Asymmetric encryption is typically utilized in everyday communication channels, mainly over the Internet. The most popular asymmetric encryption algorithms are EIgamal, RSA, DSA, elliptic curve technique and hyperelliptic curve techniques, etc. See Figure 2.

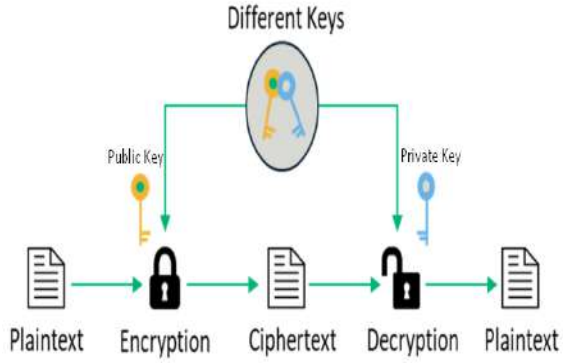


Figure 2. Asymmetric Key Encryption

Upon detailed investigation, we found differences between symmetric and asymmetric encryption techniques. All of them are given in the table below:

TABLE I. DIFFERENCE BETWEEN SYMMETRIC AND ASYMMETRIC TECHNIQUES

No	Symmetric Encryption	Asymmetric Encryption
1.	A single key is used to both encrypt and decrypt data.	Alternate keys are used to encrypt and decrypt data. The public key for encryption and the private key for decryption.
2.	The size of ciphertext is comparatively the same or smaller than the size of the original content.	The size of ciphertext is comparatively the same or larger than the size of the original content.
3.	The process of encryption is faster than asymmetric.	The process of encryption is slower than symmetric.
4.	Used when a large amount of data is required to be transferred.	Used when data is small.
5.	Largely used for confidentiality.	Used for confidentiality, authenticity, and non-repudiation.
6.	Resource utilization is low.	Resource utilization is high.

III. ANALYSIS OF POPULAR ALGORITHMS

In this section, we compare different algorithm techniques. Firstly, we consider symmetric algorithms, and then we compare asymmetric algorithms. At the end of the study, we compare both symmetric and asymmetric algorithms in order to suggest the best algorithm which can compensate for all types of encryption tasks with great reliability.

A. *Symmetric Algorithms Comparison*

After complete analysis, it is clear that blowfish and AES are the best among all other algorithms [4]. As these are invented after DES and 3DES so all the complications and drawbacks present in the aforementioned algorithms were mitigated in AES and blowfish techniques [23]. By comparing the key size of all the algorithms, it is observed that the AES and blowfish have bigger key sizes as compared to other techniques.

Blowfish is based on a Feistel network [11]. Feistel network uses a series of consecutive ciphers on a block of given data and is designed for a block of ciphers that encrypt a large amount of data [3]. A Feistel network works on a division basis, by splitting the block of data into 2 equal pieces and then applying encryption in multiple rounds [12].

TABLE II. SYMMETRIC ALGORITHMS COMPARISON

Parameters for Comparison	DES	3DES	AES	Blowfish	Twofish
Developers	IBM	IBM	NIST	Bruce Schneire	Bruce Schneire
Emerging Year	1974	1978	2001	1993	1972
Size of Key	56 bits	192 bits	128, 192, 256 bits	Up to 448 bits	Up to 256 bits
Size of Block	64 bits	64 bits	64 bits	64 bits	128 bits
No. of Rounds	16	48	10, 12, 14	16	16
Algorithm Type	Feistel N/W	Feistel N/W	Substitution & Permutation Network	Feistel N/W	Feistel N/W
Encryption Time (ms) (25kb file size)	0.89	1.391	0.48,0.67, 0.95	0.59	0.99

AES is based on substitution and permutation networks [15]. The substitution and permutation network works on mathematical calculation and formulae to substitute and flip flop the date from one place to another [11]. In this way, the data can be made non-understandable by a common person until it is decrypted by the person who knows the key for decryption [22].

B. *Asymmetric Algorithms Comparison*

By comparing the data fetched from Table III, it can be examined that RSA and ECC are in the race [5]. To filter one out of two, we need to understand the basic working and specifications of both algorithms thoroughly.

The key size in RSA can proceed up to a thousand bits, but the problem is that, if we use the larger key, greater will be the time of encryption and decryption, which is not our desire from this technique [27].

TABLE III. ASYMMETRIC ALGORITHMS COMPARISON

Parameters for Comparison	Elliptic Curve	Elgamal	RSA
Developers	Neal Koblitz, Victor S. Miller	Taher Elgamal	Rivest, Shamir, and Adleman
Emerging Year	1985	1985	1977
Size of Key	Up to 512 bits	521 bits	Up to 15360 bits
Algorithm Type	Algebraic Structure of elliptic curve over a finite field	Diffie Hellman key exchange	Exponentiation is a finite field over integers including prime numbers
Encryption Time (ms)	390	297	531

On the other hand, ECC can do the specific task of encryption with the least bits of the key [9]. This can be shown in Table IV.

TABLE IV. RSA VS ECC (BORROWED FROM [13])

Bits Level	RSA	ECC
80 bits	1024	160
112 bits	2048	224
128 bits	3072	256
192 bits	7680	386
256 bits	15360	512

ECC is a very promising asymmetric cryptography technique that was presented by Miller and his fellow Koblitz during the late 1980s [1]. This kind of algorithm is suitable for devices using memory constraints such as Palmtop computers, Smartphones, Smartcards, etc [16]. As compared to RSA and ECC requires few parameters to encrypt and decrypt the desired data or content, keeping the security level equivalent to all other sibling algorithms [13].

RSA uses the technique of exponentiation over finite fields including prime numbers [17]. On the other hand, ECC uses algebraic expressions which can also be used to encrypt and decrypt data more conveniently. ECC shows great results in respect of performance so this can be recommended as far as asymmetric techniques are concerned [13].

IV. DISCUSSION

To conclude the discussion, we have a specific kind of distribution as shown in Figure 3.

We can easily comprehend the fact from the figure that if the input size is less than 512 bits then we go for symmetric algorithms. The reason behind this observation is that symmetric key encryption seems faster than asymmetric

encryption concerning processing time. Another reason for using symmetric key encryption is that resource utilization is very low in this technique so it is best suited to content with lesser size.

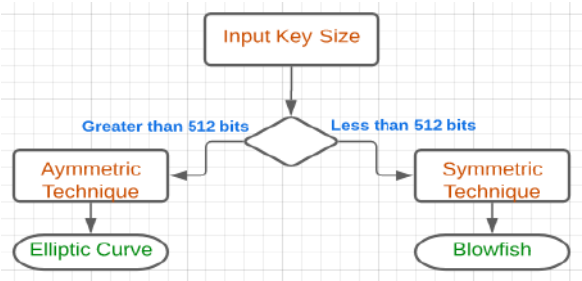


Figure 3. Suggested Best Encryption Technique

If in such cases where input data is greater than 512 bits then as a drawback of symmetric algorithm it can't handle large size of input data. So, in this case, we use the asymmetric technique.

By Deep looking at asymmetric encryption techniques, we also recommended that the ECC algorithm is the best among all older techniques and has criteria of factorization which has diverse variations to solve complex issues.

In the case of the symmetric approach, we conclude that blowfish is the best available amongst all. The reason behind this fact is that AES is also in the race, but as far as brute force attacks are concerned, AES can't handle these attacks. On the other hand, blowfish have the ability to mitigate and almost resist brute force attacks. So, in the case of security and performance, our study shows that blowfish is the best among all symmetric techniques.

V. Conclusion and Future Work

This analysis and study did not only help us to find the best algorithm among the cluster of techniques being used in the world, but also provides us with the future aspects in which we can also work on the techniques which are free of symmetric and asymmetric approaches. Those techniques may be named hybrid encryption techniques. Hybrid techniques are also present in the market. But the problem is that these are at the initial stage and have various limitations and deficiencies which are yet to be removed.

References

[1] Mota, Aquino Valentim, et al. "Comparative analysis of different techniques of encryption for secured data transmission." 2017 IEEE International Conference on Power, Control, Signals & Instrumentation Engineering (ICPCSI). IEEE, 2017.

[2] Sharma, Apoorva, and Gitika Kushwaha. "Comparative Analysis of Different Encryption Techniques in Mobile Ad-Hoc Networks (MANETs)." IITM Journal of Management & IT 10.1 (2019): 55-64.

[3] Bhanot, Rajdeep, and Rahul Hans. "A review and comparative analysis of various encryption algorithms." International Journal of Security & Its Applications 9.4 (2015): 289-306.

[4] Jeeva, A. L., Dr V. Palanisamy, and K. Kanagaram. "Comparative analysis of performance efficiency and security measures of some encryption algorithms." International Journal of Engineering Research & Applications (IJERA) 2.3 (2012): 3033-3037.

[5] Prajapati, Priteshkumar, et al. "Comparative analysis of DES, AES, RSA encryption algorithms." International Journal of Engineering & Management Research (IJEMR) 4.1 (2014): 132-134.

[6] Smekal, David, Jan Hajny, and Zdenek Martinasek. "Comparative analysis of different implementations of encryption algorithms on FPGA network cards." IFAC-PapersOnLine 51.6 (2018): 312-317.

[7] Riman, Chadi, and Pierre E. Abi-Char. "Comparative analysis of block cipher-based encryption algorithms: A survey." Information Security and Computer Fraud 3.1 (2015): 1-7.

[8] Marwaha, Mohit, et al. "Comparative analysis of cryptographic algorithms." Int. J. Adv. Eng. Tech/IV/III/July-Sept 16 (2013): 18.

[9] Maqsood, Faiqa, et al. "Cryptography: a comparative analysis for modern techniques." International Journal of Advanced Computer Science & Applications 8.6 (2017): 442-448.

[10] Hercigonja, Zoran. "Comparative analysis of cryptographic algorithms." International Journal of Digital Technology & Economy 1.2 (2016): 127-134.

[11] Long, Sihan. "A Comparative Analysis of the Application of Hashing Encryption Algorithms for MD5, SHA-1, and SHA-512." Journal of Physics: Conference Series. Vol. 1314. No. 1. IOP Publishing, 2019.

[12] Panda, Madhumita. "Performance analysis of encryption algorithms for security." 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES). IEEE, 2016.

[13] Farah, Shahzadi, et al. "An experimental study on performance evaluation of asymmetric encryption algorithms." Recent Advances in Information Science, Proceeding of the 3rd European Conf. of Computer Science,(EECS-12). 2012.

[14] Singh, Gurpreet. "A study of encryption algorithms (RSA, DES, 3DES, and AES) for information security." International Journal of Computer Applications 67.19 (2013).

[15] Yegireddi, Ramesh, and R. Kiran Kumar. "A survey on conventional encryption algorithms of Cryptography." 2016 International Conference on ICT in Business Industry & Government (ICTBIG). IEEE, 2016.

[16] Mushtaq, Muhammad Faheem, et al. "A survey on the cryptographic encryption algorithms." International Journal of Advanced Computer Science and Applications 8.11 (2017): 333-344.

[17] Jaryal, Shikha, and Chetan Marwaha. "Comparative analysis of various image encryption techniques." International Journal of Computational Intelligence Research 13.2 (2017): 273-284.

[18] Dakate, Deepak Kumar, and Pawan Dubey. "Performance comparison of symmetric data encryption techniques." IDEA 128 (2012): 58.

[19] Ebrahim, Mansoor, Shujaat Khan, and Umer Bin Khalid. "Symmetric algorithm survey: a comparative analysis." arXiv preprint arXiv: 1405.0398 (2014).

[20] Jang, Shin Woo. "Comparative analysis of AES, Blowfish, Twofish and Threefish encryption algorithms." Anal. Appl. Math. 10 (2017): 5.

[21] Liu, Fuwen, and Hartmut Koenig. "A survey of video encryption algorithms." computers & security 29.1 (2010): 3-15.

[22] Kumar, Anuj, Sapna Sinha, and Rahul Chaudhary. "A comparative analysis of encryption algorithms for better utilization." International Journal of Computer Applications 71.14 (2013).

[23] Hamouda, Baha Eldin Hamouda Hassan. "Comparative study of different cryptographic algorithms." Journal of Information Security 11.3 (2020): 138-148.

[24] Innokentievich, Tutubalin Pavel, and Mokshin Vladimir Vasilevich. "The Evaluation of the cryptographic strength of asymmetric encryption algorithms." 2017 Second Russia and Pacific Conference on Computer Technology and Applications (RPC). IEEE, 2017.

[25] Saleh, Mohammed A., et al. "An analysis and comparison for popular video encryption algorithms." 2015 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE). IEEE, 2015.

[26] Mahajan, Prerna, and Abhishek Sachdeva. "A study of encryption algorithms AES, DES and RSA for security." Global Journal of Computer Science and Technology (2013).

[27] Afolabi, A. O., and O. G. Atanda. "Comparative analysis of some selected cryptographic algorithms." Computing, Information Systems, Development Informatics & Allied Research Journal 7.2 (2016): 41-52.

[28] https://www.securitymagazine.com/articles/96667-the-top-data-breaches-of-2021

AUTHORS PROFILE

Mr. Attique Ahmed has completed his BS degree in Computer Science from Hazara University, Mansehra, Pakistan. Presently, He is pursuing M.Phil. degree in Computer Science from Abbottabad University of Science and Technology, Abbottabad, Pakistan.

Dr. Muhammad Naeem is an Associate Professor and Head of the Department of Computer Science at Abbottabad University of Science and Technology, Abbottabad, Pakistan. He has completed his Ph.D. from Leicester University, United Kingdom.

Empirical Research Press Ltd.
London, United Kingdom

International Journal of
Engineering and Applied Computer Science

Volume: 04, Issue: 02, March 2022 ISBN: 9780995707542

A Secured Text Encryption with Near Field Communication (NFC) using Huffman Compression

Adeniji Oluwashola David[1], *Akinola Olaniyan Eliais*[2]

[1, 2] Department of Computer Science, University of Ibadan, Nigeria

10.24032/IJEACS/0402/002

Volume: 04, Issue: 02, ISBN: 9780995707542, March 2022

A Secured Text Encryption with Near Field Communication (NFC) using Huffman Compression

***Abstract*—There are a lot of Challenges raised over the security of information written to the Mifare classic 1k a Radio Frequency Identification card due to the vulnerability status of this card. The card's information can be traced to another card or an electronic device. These issues allow for unauthorized access to the data on the Mifare classic 1k-enabled device data which are transmitted between the device and reader. The information produced by a Mifare classic 1k enabled credential system for a stated status is also a concern. The focus of the study is to develop an algorithm to secure information written to the Near Field Communication tag. The performance of the system shows that when n=50, with elapse time of 1.2ms the unique character was 64, likewise at optimal when n=200, the elapse time was 1ms with the unique character of 62. This result shows a decline of the symbol-by-symbol restriction with elapses time which can secure the information of the unique character.**

Keywords- RFID, Compression, Encryption, Huffman, Security.

I. INTRODUCTION

Radio Frequency Identification systems operate in three modes which are low frequency (LF), high frequency (HF), and ultra-high frequency (UHF) bands. The frequencies band are opposite to each other due to the advantages and disadvantages related to the frequency band. The operation of a low frequency creates a laggard read rate with an enlarged capacity for reading neighboring, metallic, or liquid regions. The procedure of implementation of a higher frequency will result in quicker data transfer rates with longer ranges. The LF band frequency is between 30kHz-300 kHz with lengthy wavelengths of around 2,400 meters. LF RFID systems are simply allowed to use the small range between 125kHz –134 kHz. The High-Frequency scheme operates within the 3 MHz to 30 MHz limit and renders reading distances of 10 cm - 1 m.

Higher frequency, equal to low frequency, utilizes magnetic coupling to intercommunicate between the tags and RFID reader/antenna. HF motion can pass directly in most materials excluding water and compact metals. Compressed metals, like aluminum, can still be labeled with HF tags and perform normally. HF labels trust magnetic connection for power source, so they endeavor to improve the lifespan of the application unless damaged by wear and tear of the tag end. Within the higher frequency set of the RF range, near-field connection, or NFC, is a communication code of behavior licensed by the International Organization of Standardization. The ultra-higher frequency (UHF) set inside the RF range ranges from 300 MHz to 3 GHz; however, most UHF RFID systems operate between the 860 – 960 MHz bands.

The essential exceptions are RFID arrangements that operate at 433 MHz and 2.45 GHz. In real-world applications, the type of RFID to be used depends on the use case, cost, maintainability, regulations, environmental factor, and other requirements. This has made the world of RFID-based identification systems a little bit complicated. A typical RFID system consists of tags, a reader, an information system, and materials. The information system consists of data storage, infrastructure, software applications, and middleware. RFID system usually requires a form of middleware application that handles the translation of the RFID data to an intelligible form that the information system can understand. This is important because, rarely is an information system built from scratch based on RFID, usually; RFID is introduced to augment the current identification system which usually has been built already. The ease of integration to an existing system usually makes an RFID system a go-to for RFID-based identification systems. This also means that a new system can be built without incorporating the essence of RFID into the core of the system.

II. LITERATURE REVIEW

The application of RFID in human tracking and identification has many branches, as seen in the work of [1] who proposed the use of RFID based system in the identification of patients and staff. The review in [2] also works on RFID based attendance capturing system. A work by [3] implemented RFID Based Security and Access Control System which works with other information systems. Some research has shown that an RFID system does not always require a full-fledged infrastructure. The study in [4] built an RFID system based on the Arduino microcontroller, which does not require putting network infrastructure or a central database in place. Some privacy developers see RFID's distribution and un-restricted deployment as a kind of crack of doom scenario in which corporate and government involution can pervasively monitor individuals, paving the way for a techno-totalitarian state. Also, each person's movements, associates, and casual acquaintances are cautiously monitored and recorded in futuristic data centers [5]. The security Method will defend it from any sign of vulnerabilities associated with the network such as distributed denial of service (DDoS) attacks [6]. Some systems may even lack a full network-based information system together employing a microcontroller to serve as the logic or decision unit of the information system. The research in [7] on design guidelines and best practices, divides the RFID system into three subsystems; RF Subsystem, Enterprise Subsystem, and inter-enterprise subsystem. The performance analysis of the Huffman code was discussed in [8]. Symmetric Key Block Cipher Algorithms was developed thereby describing the analysis of the cipher algorithm. The significant roles of encryption algorithms are numerous and essential in information security by [9] in Comparative Study of

Symmetric Cryptography Mechanism. Therefore, this strategy attempts to detect only known attacks based on predefined attack characteristics in [10]. It is of very low standard and quality, has little or no integrity, very easy to forge in [11]. The tradeoff between the two protocols can provide a significant impact on the networks.in [12]. AdaBoost Algorithm selects the best set of Haar features and implements it in cascade to decrease the detection time [13].

III. METHODOLOGY

There are three procedures during the implementation with independent solutions which can be extracted and implemented in different devices. The language of implementation was C# which simulates the first stage in the developed model. The first stage is the development of the Information System. The Information System handles HTTP requests, handles database communication, authorization and authentication. The module consists of the Core, infrastructure, and WebAPIs.The core configures the entities and the business rules by ensuring that, the data is securely accessed. Accessing the database, calling an external endpoint, and sending emails were handled by the infrastructure layer whileWebAPIs interface provided the secured information access to the Core through HTTP requests. The card Interactor layer is the second stage which deals with the hardware, it implements and exposes the API to communicate with the card through the interfaces using dependency injection.

The third stage is the Middleware which consists of Logic Base. This handles the Middleware logic, implements the basic checks, and has its logic without having to contact the information system. Southbound. deals with the hardware interface directly through the Card Interactor. Every read and writes operation is handled here while the Northbound deals with communications with the information system. Figure1 below shows the solution map of the developed model.

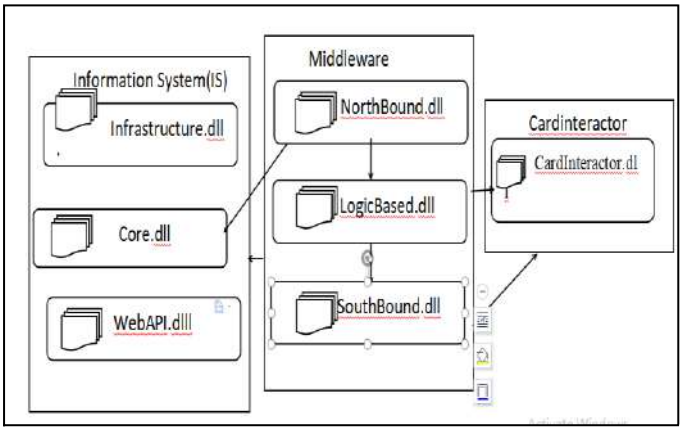


Figure 1. Model Solution Map 1

The Huffman coded information during the simulation using hexadecimal was encrypted before being written to the card. The symmetric encryption key of 6 character long alphanumeric character-set was coded using equation 1 below.

$$C = \{a-z\} \cup \{A-Z\} \cup \{0-9\} \quad \ldots\ldots\ldots\ldots(1) \quad \text{And} \quad K \subseteq C \quad \text{Where}$$

K is the Key and C is the characterset

The key was calculated with the entropy of the password. Password entropy predicts how difficult a given password would be to crack through brute force or guessing. Figure 2 shows the developed simulation model on visual studio IDE.

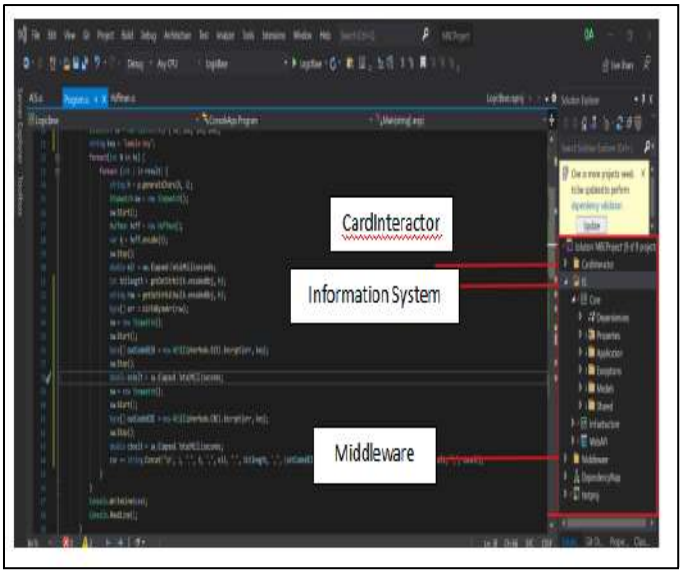


Figure 2. Simulation in Visual Studio IDE

The simulation was tested to detect Mifare standard 1k with active protocol as shown in Figure 3 below.

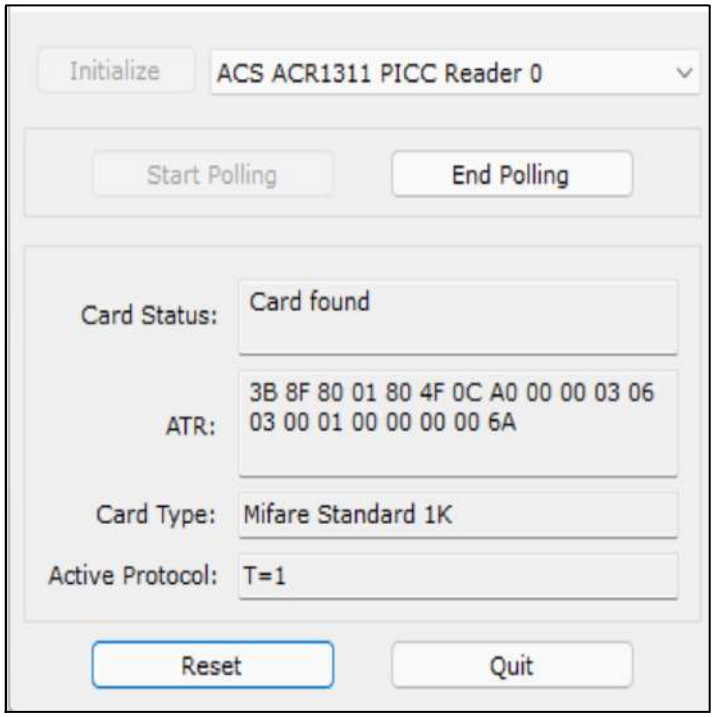


Figure 3. Interface Showing Card interactor window (card detected)

IV. RESULT AND DISCUSSION

The results from the model consist Huffman Time function which was used to identify if symbols are not independent and identically distributed because Huffman is based on the desired approach to get the optimal compression, so the study uses the shared complexity of symbol-by-symbol coding. For a given message of byte N, where n is the total number of unique characters, there is less compression achieved as n increases. The maximum compression ratio is achieved when n = 1 for the same value of N. There is a clear correlation between the number of unique characters n and how deep the tree is, which in turn affects time performance during the simulation as shown in Figure 4.1, 4.2, 4.3 and 4.4 below.

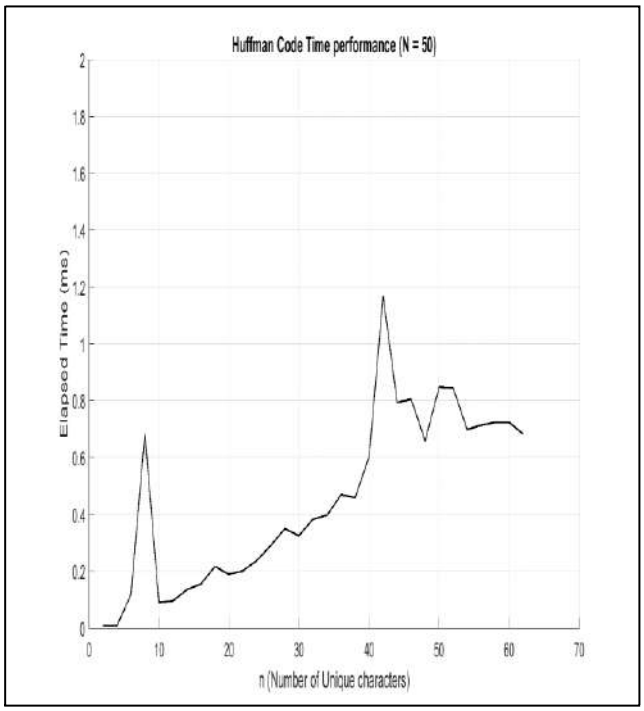


Figure 4.1. Graph of Time performance when N=50

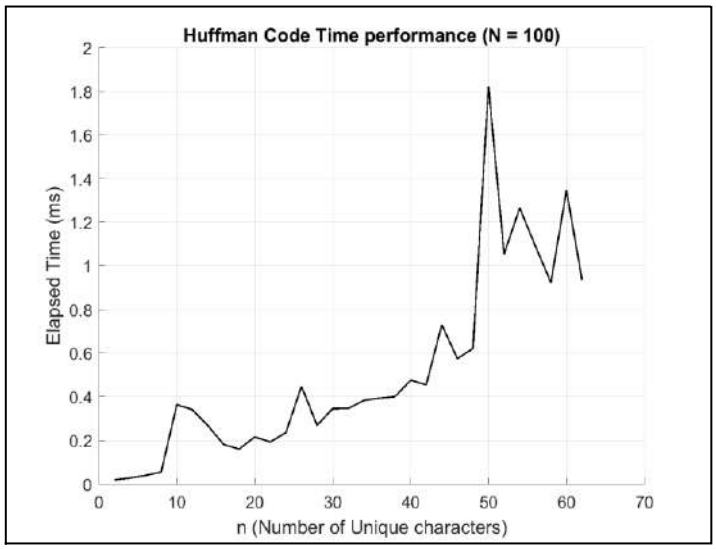


Figure 4.2. Graph of Time performance when N=100

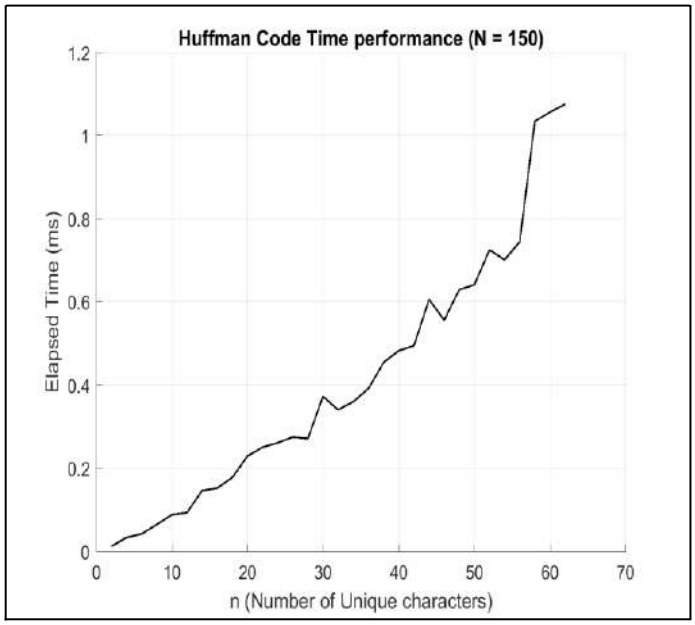


Figure 4.3. Graph of Time performance when N=150

The results of Huffman code time performance during the simulation when n=50, n=100, n=150, and n= 200 are depitched to confirm that the result of the graph presents the elapsed time against the number of unique characters. These results present the desired approach to get the optimal compression when n=50 with elapse time of 1.2ms when the unique character was 64 in Figure 4.1.

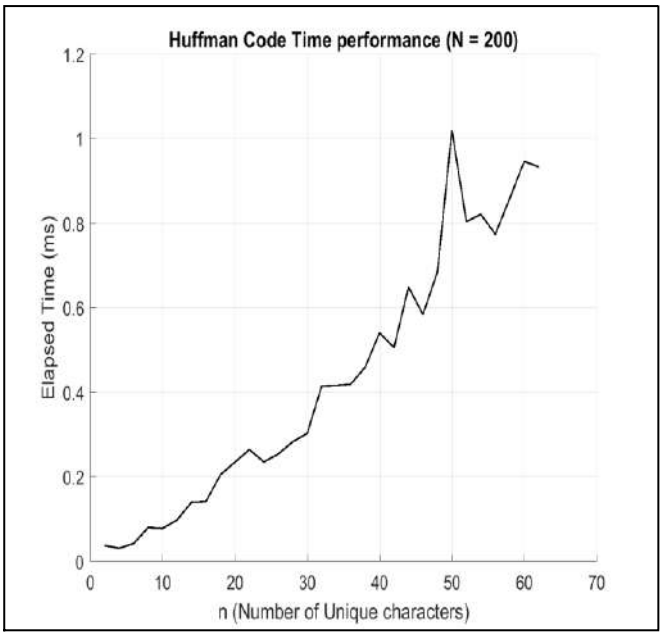


Figure 4.4. Graph of Time performance when N=200

In a related result when n=100 the elapse time for the Huffman performance was 1.8ms with the unique character of 64 as shown in Figure 4.2. Also, when n=150 the elapse time from the graph was 1.03ms with 64 unique characters, and when n=200 the elapse time was 1ms with the unique character

of 62 as shown in the graph of Figure 4.3 and Figure 4.4 respectively.

The evaluation of the Huffman time performance during the simulation is presented in the graph in Figure 4.5 below.

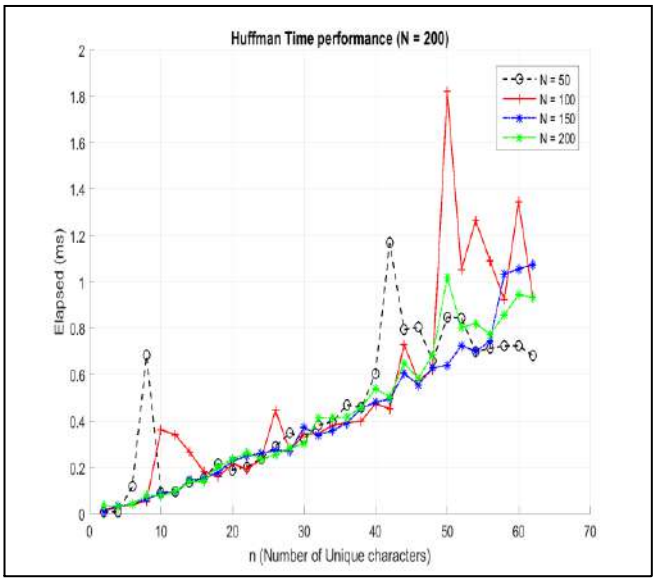


Figure 4.5. Graph of Time performance and compression

This result shows a decline in the symbol-by-symbol restriction which can secure the information of the unique character. The clear correlation between the number of unique characters is a reflection of how deep the tree is, which in turn affects time performance during the simulation.

V. CONCLUSION

The information system and the RFID system will be linked together by the means of integration. This essentially ensures that both systems can be built and extended independently without having to redesign the other part of the system. A file database is chosen for this research, this ensures that reliance on the network is obviated reducing the overhead cost of the server and network latency. The developed model in the research due to declination of the symbol-by-symbol restriction will ensure that a brute-force attempt outside this model when guaranteed by a hacker will fail because the system will revert to anti-brute-force to mitigate against guessing the 6-character long key.

ACKNOWLEDGEMENT

The research was conducted at the Department of Computer Science, University of Ibadan, Nigeria. The authors thank the department for their support in this research work.

REFERENCES

[1] Cerlinca, T. I., Turcu, C., Turcu, C., & Cerlinca, M. RFID-based Information System for Patients and Medical Staff Identification and Tracking. InTech.2010

[2] Rjeib, H. D., Salih Ali, N., Al Farawn, A., Al-Sadawi, B., & Alsharqi, H. Attendance and Information System using RFID and Web-Based Application for Academic Sector. IJACSA) International Journal of Advanced Computer Science and Applications, 2018. 9(1).

[3] Umar Farooq, Mahmood ul Hasan, Muhammad Amar, Athar Hanif, & Muhammad Usman Asad. "RFID Based Security and Access Control System". 2014. IACSIT International Journal of Engineering and Technology, 6.

[4] Adak, D., Kumar Pain, M., & Dey, U. K. . RFID BASED SECURITY SYSTEM USING ARDUINO MODULE. International Journal of Scientific & Engineering Research, 2017,8(3).

[5] Ashimi, O. Q., Adeniji, O. D. "Detection and Mitigation of Flood Attacks in IPv6 Enabled Software Defined Networks. *Advances in Research Journal*, 2020, Vol. 21. No. 8. 1-9.

[6] Williams, G. Radio frequency identification. In *Technology for Facility Managers: The Impact of Cutting-Edge Technology on Facility Management* pp. 2018, 75–83.

[7] Konstantinides, J. M., & Andreadis, I. Performance analysis for canonical Huffman coding with fixed window size. Electronics Letters, 2016, 52(7), 525–527.

[8] Mankotia, S., & Sood, M. A Critical Analysis of Some Symmetric Key Block Cipher Algorithms. International Journal of Computer Science and Information Technologies, 2015, .6(1), 495–499.

[9] Logunleko K.B., Adeniji. O.D., Logunleko A.M." A Comparative Study of Symmetric Cryptography Mechanism on DES, AES, and EB64 for Information Security". International Journal of Scientific Research in Computer Science and Engineering.2020, Vol.8, Issue.1, .45-51.

[10] Adeniji O.d., Olatunji O.O. "Zero Day Attack Prediction with Parameter Setting Using Bi Direction Recurrent Neural Network in Cyber Security".International Journal of Computer Science and Information Security (IJCSIS), 2020, Vol. 18, No. 3,111-118.

[11] Eze Chika Victor, Adeniji Oluwashola David,.Character Proximity For RFID Smart Certificate System: A Revolutionary Security Measure To Curb Forgery Menace. International Journal of Scientific &Technology, 2014, Vol 3 No 10: 66-70.

[12] Adeniji O. D, Osofisan Adenike Route Optimization in MIPv6 Experimental Testbed for Network Mobility: Tradeoff Analysis and Evaluation. International Journal of Computer Science and Information Security (IJCSIS), Vol. 18, No. 5, pp 2020, 19-28.

[13] Ayorinde Henry Omopintemi, Promise Irebami Ayansola Kehinde Gbemisola Ogundijo Device Synchronization Using a Computerize Face Detection and Recognition System for Cyber security. International Journal of Computer (IJC),2022.ISSN 2307-4523.

Empirical Research Press Ltd.
London, United Kingdom

International Journal of
Engineering and Applied Computer Science

Volume: 04, Issue: 02, March 2022 ISBN: 9780995707542

A Novel Framework for Selecting Elicitation Technique based on Attribute Mapping

Attique Ahmed[1], Muhammad Naeem[2]

[1,2] Department of Computer Science, Abbottabad University of Science and Technology, Pakistan

10.24032/IJEACS/0402/001

Volume: 04, Issue: 02, ISBN: 9780995707542, March 2022

A Novel Framework for Selecting Elicitation Technique based on Attribute Mapping

***Abstract*—The software development process is completely based on the requirements of stakeholders. If the requirements of stakeholders are being integrated into the proposed system, then it can be assumed that the end product is going to be optimal and successful. To achieve a successful product, different Requirement Elicitation Techniques (RET) are being practiced. The selection of a suitable RET is based on the nature of the product being developed. So, a single RET doesn't fit all products. In this paper, we differentiate all RETs from each other which makes it easier for an analyst to choose suitable RET from the available ones. We further designed a novel mapping framework that extracts the best suited RET to any software based on its attributes. We have further implemented the proposed framework by using an online vehicle booking system as a running example.**

Keywords- Requirement Elicitation Techniques (RETs), Requirement Gathering, RETs in Software Development, Mapping of characteristics.

I. INTRODUCTION

In the software development process, the number of Requirement elicitation techniques is being incremented over time because every developer thinks of having the best technique to overcome the hurdles both in development as well as in the end product when the user uses the product. On the other hand, this idea has created a big problem for the industry which technique is the best among all? [1] And can be implemented to get a reliable and user-acceptable product [1].

By going through the literature, it can easily be judged that above 50% of the software projects get failed and the end users/stack holders don't accept the product [14]. The reason for failure can be due to one of the following aspects [2].

i. Requirements Elicitation.
ii. Requirements Analysis.
iii. Requirements Implementation.
iv. Requirements Documentation.
v. Requirements Validation.

Among all the above-mentioned phases of Requirement engineering, the most crucial and challenging phase is Requirement elicitation. This is the only stage through which the data and all other aspects of the product to be made can be extracted from stakeholders. So, if this phase goes wrong or is ambiguous, this will surely result in rejected end product [19].

In this paper comparison of almost all the RE techniques concerning different scenarios is being discussed which will surely be helpful for developers to choose the best technique and to gather maximum input from the stakeholders. The comparison comprises three phases. In the first phase, the pros and cons of all the RE techniques are discussed to have a birds-eye view of the techniques being implemented. The second phase is related to the characteristics of all techniques through which developers can decide to go or not to go with any specific technique. In the third and the last phase, a requirement elicitation framework is provided through which a developer can easily find out the best RE technique among the cluster. An example is also provided in which a suitable requirement elicitation technique is selected according to the proposed framework.

II. ADVANTAGES AND DISADVANTAGES OF DIFFERENT REQUIREMENT ELICITATION TECHNIQUES

Firstly, all the advantages and limitations of every single RE technique are discussed in Table I below to get a basic idea that what are the key strengths and limitations present in every RE technique [3][14].

The benefits of all techniques are mentioned in Table I to sort out the basic utilities and positive aspects present in them [13]. All the techniques are divided into four main categories namely Traditional, Cognitive, Collaborative, and Observational requirement elicitation techniques [1, 2] [13, 17]. The first group of techniques are very basic and are being used since the emergence of the said field. The reliability of these techniques is also very good and the techniques are well-reputed as well. But with time there emerged the need for some other techniques because the existing techniques were leaving some vacant spaces which directly challenge the success of the end product.

The Cognitive Techniques are also very reliable and are used mostly in gathering information regarding system development. The Collaborative and Observational techniques are also well in the industry and are being implemented by analysts and developers to develop the demanded and reliable end product. The benefits and limitations of every requirement elicitation technique are discussed below which enroots towards characteristics analysis and finally, the optimized techniques are sorted out to provide feasibility to the developer and stakeholders as well [1-3].

TABLE I. COMPARISON OF REQUIREMENT ELICITATION TECHNIQUES

Category	Elicitation Techniques	Merits	Demerits
Traditional R.E. Techniques	Interviews	The proposed system is discussed in detail. Data is informative and useful.	The amount of data is very large and hard to summarize.
	Surveys	Many users can be involved by using this very cheap method to get large information.	A system as a whole can't be analyzed, which is the actual demand of elicitation.
	Questionnaire	A basic approach in which every aspect is asked remotely from stakeholders.	Only for basic and quick knowledge. Further ideas can't be generated.
	Task Analysis	It directs the user to the system interface.	Time-consuming because details are needed for a small product.
	Domain Analysis	It derives its strength from existing system documentation and manuals.	It becomes more than a task, converted to a case study.
	Introspection	The smart and useful technique has almost no cost.	Comprehensive knowledge of business areas is demanded.
Cognitive R.E. Techniques	Card Sorting	Differentiation between different requirements. Customer knowledge is analyzed.	Work in collaboration is more realistic and useful compared to this technique.
	Class Responsibility Collaboration (CRC)	Provides fundamentals to make UML diagrams.	It suits only the designer, not the software engineer
	Laddering	Hierarchy-based requirements arrangements.	Not suitable for large projects because addition and deletion are difficult.
	Repertory Grid	Identification of characteristics is easy.	Identification becomes hard in complex systems.
Collaborative R.E. Techniques	Focus Group	Every condition defined by stakeholders can be evaluated and useful data can be collected from them.	In the case of multiple stakeholders, it results in a conflict.
	Brainstorming	New ideas are generated by this technique. Decision-making is easy.	Does not suit to Busy and Crowded environment
	Joint Application Development (JAD)	Customer-Developer collaboration is easy to create, change or delete any aspect of the system.	Expert Knowledge at both ends lacks.
	Requirement Workshop	Large and complex data can be extracted by the detailed workshop.	It has a huge cost and does not align with small tasks.
	Protocol Analysis	All the stakeholders and users are required to participate to get a suitable system.	Deadlock can occur due to multiple thoughts.
	Prototyping	Developing a new system becomes easy due to the involvement of stakeholders, especially in making GUI.	Time and cost both are utilized at a high rate.
Observational R.E. Techniques	Ethnography	Social behaviors are brought into context to get quality attributes.	Multiple Communities can create a hurdle in using this technique.
	Observation	This technique is helpful in requirement analysis and validation phases for analysts.	Observation can be partial or leftover due to travel expenses.
	Apprenticing	Facilitates both analyst and stakeholder to work in cooperation.	The willingness of stakeholders is optional.

III. Characteristics Based Analysis of Different Requirement Elicitation Techniques

The characteristics of every elicitation technique are different from each other in various aspects which are discussed in Table II. Every technique has different characteristics concerning the location of analysts and stakeholders, the role of the analyst, mode of conduction, type of data, size of data, and the number of stakeholders [2, 14].

TABLE II. Characteristics Based Analysis of Requirement Elicitation Techniques

Category	Elicitation Techniques	Location Analyst/Clients	Role of Analyst	Mode of Conduction	Type of Data	Size of Data	Stakeholders
Traditional R.E. Techniques	Interviews	Same	To Lead	Direct	Qualitative & Quantitative	Large	One/Many
	Surveys	Different	Facilitate	Indirect	Qualitative & Quantitative	Large	Many
	Questionnaire	Same	To Lead	Indirect	Quantitative	Medium	Many
	Task Analysis	Same	Facilitate	Indirect	Quantitative	Medium	N/A
	Domain Analysis	Same	Facilitate	Indirect	Quantitative	Medium	N/A
	Introspection	N/A	Passive	Direct	Quantitative	Small	N/A
Cognitive R.E. Techniques	Card Sorting	Same	Facilitate	Indirect	Quantitative	Medium	Many
	Laddering	Same/Different	Facilitate	Indirect	Qualitative & Quantitative	Small to Medium	One
	Repository Grid	N/A	Facilitate	Indirect	Qualitative & Quantitative	Small	Many
Collaborative R.E. Techniques	Focus Group	Same	To Lead	Indirect	Qualitative	Small	Many
	Brainstorming	Same	To Lead	Direct	Qualitative	Small	Many
	Joint Application Development (JAD)	Same	To Lead	Direct	Qualitative	Medium	Many
	Requirement Workshop	Same	To Lead	Direct	Qualitative	Small	Many
	Protocol Analysis	N/A	Passive	Direct	Qualitative	Medium	Many
	Prototyping	N/A	Passive	Direct	Qualitative	Small	More than 1, not many
Observational R.E. Techniques	Ethnography	Same	Passive	Direct	Qualitative	Medium	Many
	Observation	Same	Passive	Direct	Qualitative	Medium	Many
	Apprenticing	Same	Passive	Direct	Qualitative	Small	One

In location, it is distinguished whether the location of analysts and stakeholders is the same or not? If the location is the same then the 'same' value is entered otherwise if the location is different, then the value 'different' is entered in the field. Likewise, if the role of the analyst is to facilitate the stakeholders, then 'facilitate' value is entered. If the role is to lead the system, the 'to lead' value is entered into the field. In some cases where the analyst is not directly involved and is not currently on the active side, then 'passive' value is entered in the field.

In the column 'mode of conduction,' it is decided that if the elicitation technique is designed for direct elicitation purpose, then the value 'direct' is entered, and if the elicitation technique is performing some other functions as well, then 'indirect' is entered in the required field. 'Size of data' plays a huge role in the elicitation process because if the data provided at the output is small, then there might be a lack of complete data according to the situation, but if it is large, then there is the probability of vague and irrelevant data. But in both cases, the values to be entered in the required field would be 'small' and 'large' as the case may be [17].

Lastly, the numbers of stakeholders are also discussed to analyze the people involved in every elicitation technique. This is because involving the stakeholders every time is time consuming and difficult task which leads to delays in finalizing the end product. In Table II the values 'One' or 'Many' can be entered according to the suitable case.

IV. Framework for Selecting Suitable Technique

After a complete analysis of the system, a complete framework is hereby proposed (Figure. 1) which can be used to find out the best requirement elicitation technique according to the proposed system's attributes, characteristics of all the above-mentioned techniques, situation based/ on-ground analysis by the analyst.

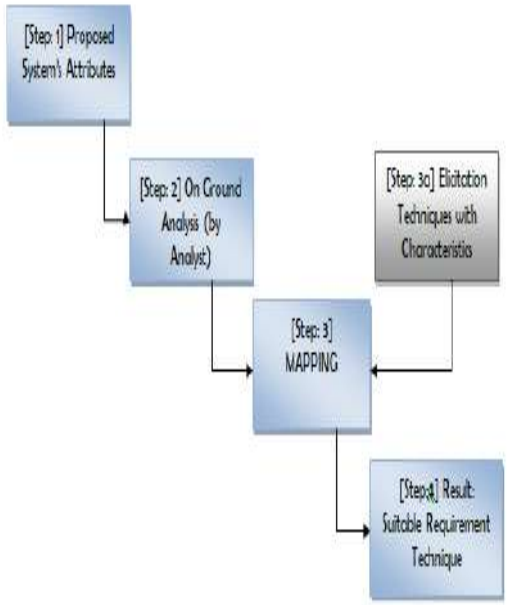


Figure 1. Characteristics Based Analysis Of Requirement Elicitation Techniques

The proposed system attributes are defined by the stakeholders in whom they define the system as well as their requirements in the final product. The number of stakeholders is also defined in this step to facilitate the analyst/developer.

All the elicitation techniques are also defined in the framework, which is essential to mention here to map them with the system which is to be created. The characteristics are comprehensively discussed earlier in this study and are well versed to map them with the system which is to be created. The characteristics are comprehensively discussed earlier in this study and are well versed to implement in any upcoming system.

On-ground analysis are also given as input to the framework, which is done by the analyst because the observation is compulsory before requirement engineering. In requirement engineering, one of the basic things is to identify the social environment in which the proposed system will be used and grow. The criteria are changed as the situation gets changed and the elicitation technique is also changed according to realities.

All three inputs are applied to a mapping function that takes the inputs from three sides and maps them with each other to provide outcomes with the resultant techniques which are most suitable to the system attributes given by the stakeholders, characteristics provided by this analysis, and situations mentioned by the analyst.

Lastly in our framework, results are mentioned, in which the analyst finds the result of all the processes and finds the best technique for elicitation of requirements which is more likely to produce a successful product at the end of the process of software development life cycle.

V. Implementation of Framework

A complete study of different elicitation techniques concerning various parameters is conducted, and then at last a framework is proposed in which all the parameters are mapped together and a suitable solution in the form of any elicitation technique is provided.

To express the above-mentioned framework in a better way, a real-world project is defined here, on which said framework is implemented and a resultant elicitation technique is provided at the end which is suitable to the given project.

VI. Running Example

The online vehicle booking system is an online web-based project which is intended to provide the customer's facilities to communicate with the organization and to book a vehicle by performing some well-defined functions on the web portal. The stakeholders then validate the data and after completing all the preliminary proceedings send the vehicle to the customers at their venue as mentioned while filling out the online form. The payment method is also integrated into the web portal or app to give ease to the customers for paying the requisite amount after consulting with the organization.

It works on different modules like the customer module and administrator module. Customers can browse for the demanded vehicles from the store and can apply for the vehicle as well. The administrator can look into the matter of vehicle booking and other relevant tasks regarding the platform.

The actual company also has employees who are responsible to provide end-to-end delivery of any designated task. So, in all, we have three modules which are client, agent, and employees. The said project has some on-ground realities/ situations which are expressed below.

A. *Step 1:* In the above online web project; there are numerous stakeholders like administrators, employees, and end-users/ customers. The administrator and employees are always available for requirement elicitation, but clients/ customers are not present at the time of the startup of the said web portal. So, in this on-ground analysis, the analyst has to perform some functions to collect the customer needs from the portal, which is mandatory.

B. *Step 2:* If we talk about the scope of the project, we have various users on the platform. So, we have to go for those Characteristics which ensure that multiple users can access the system without any difficulty.

C. *Step 3:* As the number of customers accessing the system is very large. All the customers have different intellectual regarding the use of the internet and web app. So, situational measures are also to be performed so that all customers can use the web system reliably.

D. *Step 4:* In this project, the characteristics which are demanded, are also present in the projects previously made. This project is not of a new sort, so use cases can also be implemented to evaluate the elicitation technique.

The elicitation techniques based on the situation can be more than one because in one scenario one technique is useful and for other scenarios, other techniques can be implemented. But the best technique is based on the percentage that how much a technique is suited to any specific domain. In an online vehicle booking system, all the employees and stakeholders can be brought onto a single table e.g., for Interviews.

Brainstorming is a technique that can also be used in this scenario because it includes customers who are not always available, especially at the time of development. The document Analysis technique can also be used to understand the previous work on the same type of project.

The last conversation is in between the selected techniques because a single technique must be chosen to ensure reliability in the development process. As far as the current situation is concerned, Interviews for sake of getting information from organizational stakeholders and Document Analysis for sake of getting information on the customers'/end-user's demands are the best techniques to be implemented.

VII. Conclusion and Future Work

In this paper, we completely focused on different requirement elicitation techniques. A three-dimensional analysis of all the techniques is brought out. The first dimension was related to an in-depth analysis of different requirement elicitation techniques. In the second aspect, an efficient approach was applied to all techniques which were characteristic-based analysis. At the end of the research, a mapping framework is presented which is practically applied to a running example as well.

As we have provided a complete implementable framework to select suitable RE techniques but in the future, many aspects can also be considered. Time complexity can be a huge factor that can be given priority based on complete research. Likewise, many industries have their pre-implemented techniques which can be either successful or unsuccessful

depending on case to case. So, the characteristics-based techniques can also be implemented on the sample taken from any specific region or industry type as well.

REFERENCES

[1] S. Tiwari, S. S. Rathore, & A. Gupta, (2012, September). Selecting requirement elicitation techniques for software projects. In 2012 CSI Sixth International Conference on Software Engineering (CONSEG) (pp. 1-10). IEEE.

[2] M. A. Abbasi, J. Jabeen, Y. Hafeez, D. Batool, & N. Fareen, (2015). Assessment of requirement elicitation tools and techniques by various parameters. Software Engineering, 3(2), 7-11.

[3] M. Tariq, S. Farhan, H. Tauseef, & M. A. Fahiem, (2015). A comparative analysis of elicitation techniques for the design of smart requirements using situational characteristics. International Journal of Multidisciplinary Sciences and Engineering, 6(8), 30-38.

[4] H. Dar, M. I. Lali, H. Ashraf, M. Ramzan, T. Amjad, & B. Shahzad, (2018). A systematic study on software requirements elicitation techniques and their challenges in mobile application development. IEEE Access, 6, 63859-63867.

[5] A. Nawaz, A. U. Rehman, & W. H. Butt, (2020). A Survey of Requirement Engineering Process in Android Application Development. arXiv preprint arXiv:2008.13113.

[6] G. C. Sampada, T. I. Sake, & M. Chhabra, (2020, November). A Review on Advanced Techniques of Requirement Elicitation and Specification in Software Development Stages. In 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC) (pp. 215-220). IEEE.

[7] B. Zachariah, & O. F. Nonyelum, (2020). A Comparative Analysis of Requirement Gathering Techniques. IUP Journal of Computer Sciences, 14(2), 7-32.

[8] S. W. Kamal, M. Yaseen, A. U. Rahman, M. Bacha, & I. Kazim, (2020). Practices for Implementing Collaborative Tools and Modern Technologies during Requirement Elicitation in Global Software Development. i-Manager's Journal on Software Engineering, 14(4), 20.

[9] I. Udousoro, (2020). Effective requirement engineering process model in software engineering. Software Engineering, 8(1), 1.

[10] Z. Sofyan,(2020, March). User requirements elicitation in web-based Participatory Geographic Information System interface design. In IOP Conference Series: Materials Science and Engineering (Vol. 796, No. 1, p. 012028). IOP Publishing.

[11] A. H. Zahid, A. Liaqat, M. S. Farooq, & S. Naseer, (2020). Requirement Elicitation issues and Challenges in Pakistan Software Industry. VFAST Transactions on Software Engineering, 8(1), 28-36.

[12] A. Jarzębowicz, & K. Poniatowska, (2020). Exploring Impact of Requirements Engineering on Other IT Project Areas–Case Study. Computer Science, 21(3).

[13] I. H. Hussein, J. Din, S. Baharom, & M. B. Jasser, (2021). An Approach for Selecting the Suitable Requirement Elicitation Technique. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(3), 2083-2087.

[14] S. Hunzai, & I. A. Shah, (2021). Impact of Elicitation Techniques on Requirement Validation in Software Industry in Pakistan. International Journal of Computer Science and Information Security (IJCSIS), 19(3).

[15] D. Gobov, & I. Huchenko, (2021, January). Influence of the Software Development Project Context on the Requirements Elicitation Techniques Selection. In International Conference on Computer Science, Engineering and Education Applications (pp. 208-218). Springer, Cham.

[16] M. A. Iqbal, & A. Shah, (2021). Stakeholder's Evaluation Process for GSD Based Requirements Elicitation Frameworks. Pakistan Journal of Engineering and Technology, 4(01), 175-183.

[17] V. Singh, D. Pandey, K. Sahu, & M. W. Khan, Optimizing the Impact of Security Attributes in Requirement Elicitation Techniques using FAHP. communications, 14, 15.

[18] K. L. Hobbs, A. R. Collins, & E. M. Feron, (2021). Risk-based formal requirement elicitation for automatic spacecraft maneuvering. In AIAA Scitech 2021 Forum (p. 1122).

[19] D. Gobov, & I. Huchenko, (2021). Software Requirements Elicitation Techniques Selection Method for the Project Scope Management. In ITPM (pp. 1-10).

[20] N. C. Alflen, L. C. Santos, E. P. Prado, & A. Grotta, (2021). Using Combined Techniques for Requirements Elicitation: A Brazilian Case Study.

[21] D. A. P. Sari, A. Y. Putri, M. Hanggareni, A. Anjani, M. L. O. Siswondo, & I. K. Raharjana, (2021, February). Crowdsourcing as a tool to elicit software requirements. In AIP Conference Proceedings (Vol. 2329, No. 1, p. 050001). AIP Publishing LLC.

AUTHORS PROFILE

Mr. Attique Ahmed has completed his BS degree in Computer Science from Hazara University, Mansehra, Pakistan. Presently, He is pursuing M.Phil. degree in Computer Science from Abbottabad University of Science and Technology, Abbottabad, Pakistan.

Dr. Muhammad Naeem is an Associate Professor and Head of the Department of Computer Science at Abbottabad University of Science and Technology, Abbottabad, Pakistan. He has completed his Ph.D. from Leicester University, United Kingdom.

Empirical Research Press Ltd.
London, United Kingdom

International Journal of
Engineering and Applied Computer Science

Volume: 04, Issue: 02, March 2022 ISBN: 9780995707542

Performance Analysis of the Bus Topology Network for Effectual Data Distribution

Ojo Jayeola Adaramola[1], Jamiu Rotimi Olasina[2]

[1,2] Department of Computer Engineering, Federal Polytechnic Ilaro, Nigeria

10.24032/IJEACS/0402/007

Volume: 04, Issue: 02, ISBN: 9780995707542, March 2022

Performance Analysis of the Bus Topology Network for Effectual Data Distribution

Abstract- **Stability, reliability, efficiency, and dependability necessitate a higher performance feature-based system in Ethernet LAN to meet the prevalent emergent technology of 5G and beyond 5G in the domain of networking. LAN technology has experienced the most progression since it came to reality. Despite its ability to achieve promising performance, the technology still keeps some topology characteristics that have a greater influence on its performance. This paper, therefore, addresses the high packet loss experienced in bus topology by investigating the performance of bus topology in four practical scenarios consisting of 10, 20, 30, and 40 nodes. In some applications, traffic was cautiously selected and configured in the application configuration to generate traffic for the modeling. These include HTTP, FTP, email, and databases before they were finally defined in the profile configuration. Substantial global and object statistics such as delay (sec), traffic-sent (bits/sec), traffic-received (bits/sec) for global, and throughput (bits/sec) for global were considered as network metrics for simulation in the OPNET environment. The results obtained proved that as the number of nodes increased, more traffic (bits/sec) were sent and received, more messages were delivered (bits/sec), the delay (sec) was lowered, but greater bit errors per packet were experienced in the network, thus making the bus topology not very suitable for a larger network.**

Keywords- Bus Topology, Global Statistics, LAN, OPNET, Packet Loss.

I. INTRODUCTION

In our present-day communication, networks play an imperative role in effective data distribution as it is applied to every sphere of life, ranging from education to banking, commerce, industry, and entertainment. The use of Local Area Networks (LANs) in propagating appreciable information to people is necessary, especially in an academic setting where the use of modern networking technology is required [1]. The LAN is classified into topology, architecture/design, and protocols [2]. The work aims to achieve the best topology using the most suitable links and several nodes, so that, the network can experience better data-flow-rate in terms of speed [3]. Various types of topologies are available in computer networking. These include star topology, which requires a central host for node connection, bus topology, which requires a common medium for transmission, ring topology, which requires point-to-point connection of the nodes to form a closed path, and mesh topology, which also requires connection of each node to every other node in the network [2, 4].

Several simulation tools like packet tracer, OMNet++, NS-2, NS-3, OPNET, Netsim, and Glomosim are available to properly model and analyze topology in a network environment to lower the cost of evaluation and deployment [5]. The OPNET simulator was preferred because of its flexibility, ease of use, user-friendliness, availability in a Graphic User Interface (GUI), excellent documentation, fastest simulation, and the greatest scalability, freely and commercially available. OPNET also allows the investigation of bit errors, packet losses, data message flows, and link failures [6].

Several performance metrics are available in the OPNET environment to serve as performance pointers and to determine the behavior of network topology. The following performance metrics were considered for maximum efficiency: The delay (sec), which is regarded as the time taken for data to travel from source to destination (the lesser the delay, the higher the performance); throughput (bits/sec), is the average message successfully delivered over a transmission link (the higher the throughput, the higher the performance) [7]. Also, traffic sent (bits/sec) from the source to all available nodes, traffic received (bits/sec) sinks to all available nodes [8], and bit error per packet.

The aim of this work is based on investigating the performance of bus topology to tackle high packet loss for effectual data distribution using simulation approaches. In this paper, four scenarios were modeled by considering different sizes of nodes to cater to network applications: FTP, HTTP, email, and database. The simulation metrics in this paper include: delay (sec), traffic sent (bits/sec), traffic received (bits/sec), throughput (bits/sec), and bit errors per packet. The metrics were implemented and a comparison of each of these metrics was considered for various sizes of LAN networks to achieve optimum performance.

The remaining part of this work is structured as follows: Section I, explained the introductory part of the research work. Section II reviewed the work of different researchers. Section III discussed the techniques used to implement the research work. Section IV discussed and presented the results obtained from the bus topology implementation. Section V serves as the concluding part of the research work.

II. RELATED WORK

This phase of the research briefly discussed various ideas presented by different researchers on network topology and the best techniques deployed to achieve their desired goal. [9], according to this paper, computer networks and the recent developments in the field of computer networks were explicitly examined. Accordingly, keystream network topology configurations were discussed; the basic advantages and disadvantages of nearly eight configurations were also presented in their work. Based on their investigation, different architectural characteristics were studied to assist in developing innovative networks that are in practice. According to their findings, an innovative idea will help engineers advance the

subsequent generation of the network. In [10], analytical research on different existing topologies to have a fleeting knowledge of each topology and its characteristics was carried out. In their work, both the advantages and disadvantages of each topology were presented. They, however, observed that two or more of these topologies with their characteristics can be combined to form a hybrid topology. This topology proved to be more effective, reliable, flexible, and scalable as advantages, but it required expensive infrastructure and design complexity. Researchers in [11], also carried out the analytical investigation on different categories of network topologies that were based on their advantages, disadvantages, and other differentiating factors that segregate them. A comparison table was prepared to determine how data flow in the topologies. They presented their work as a great tool for dealing with any problem related to network topology. In [12], a topology for improving performance for their campus, called hybrid topology was proposed. This required the comparison of the output performance of the existing topology with the output performance of the hybrid topology. They concluded that this method produced better and required advancement in network performance for their campus after properly implementing their proposed approach in a simulation environment.

This was based on the fact that there was no packet loss; their work was faced with a smaller delay time and had a lower hop count. They stressed that this network can be extended to handle increasing user numbers. According to the work in [8], performance evaluations on bus topologies using a simulation approach were carried out. Their method was based on various network parameters such as delay in (sec), throughput in (bits/sec), traffic-sent in (bits/sec), traffic- received in (bits/sec) for 10 Ethcoax stations. An OPNET software was considered the simulation of choice for the implementation and thus simulated for 1 hour.

They concluded that using the simulation approach is far easier than the real-time execution strategy. And they further stressed that as the number of nodes increases, the network performance decreases and thus experiences little differences in delay (bits/sec), but there was not much difference in end-to-end delay. [13], considered three main topologies to include bus, ring, and star for various numbers of workstations using software methods. Four different scenarios were examined for each topology, and each scenario consisted of 5, 10, 15, and 20 workstations. They based their analysis on four different parameters, which include the number of collisions experienced on one server, delay in (sec) for global statistics, load in (bits/sec), and traffic received in (bits/sec) on object statistics. Each topology was compared distinctly and also compared for an equal number of linked devices. They came to the conclusion that as the number of linked workstations grows, the network's performance declines, and that the bus topology outperforms the other two topologies.

In this research work, bus topology was investigated with different sizes of four modeling scenarios: 10 nodes, 20 number nodes, 30 number nodes, and 40 numbers nodes. This method was used to examine how the bus topology behaved in the presence of high packet loss when the number of nodes in the network grew. The metrics used to generate network traffic were HTTP, FTP, email, and databases, which were compared in the OPNET simulation environment to achieve a reasonable result.

III. METHODOLOGY AND PROCEDURES

This aspect describes the method and procedure deployed to appreciate the performance of well-organized network topology (Bus Topology) for maximum data communication. The process was designed and implemented in an OPNET simulation environment where different scenarios were modeled. The simulation approach was considered to ease the cost of execution and, thus, demonstrated the expected outcome in the real-life exploitation.

The office scale (100 x 100 meters) was designed using the startup wizard, and the ethcoax model family was selected. Different sizes of bus topologies (10, 20, 30, and 40) were generated in the rapid configuration of the OPNET, where ethcoax_station was chosen as the node model, eth_coax as the link model, and eth_tap as the tap model, and other attributes remained in their default position. The bus attributes were adjusted with the name changed as eth_coax_adv, the data rate of 500,000bps was fixed and the delay of 0.05 seconds was considered. Application configuration, profile configuration, and nodes were configured with (HTTP, FTP, email, and the database) to generate traffic. The simulation was set up, and the global statistics (Delay in (sec), traffic-received in (bits/sec), and traffic-sent in (bits/sec)), and also object statistics (Throughput in (bits/sec), Bits Error per Packet), were obtained.

Application configuration (default), profile configuration (configured with four (4) selected network parameters), and a server configured to provide required services such as HTTP server, FTP server, email server, and database server to ten nodes connected to the eth_coax backbone are shown in Figure 1. The model was simulated for 1 hour (60 min) for optimal results.

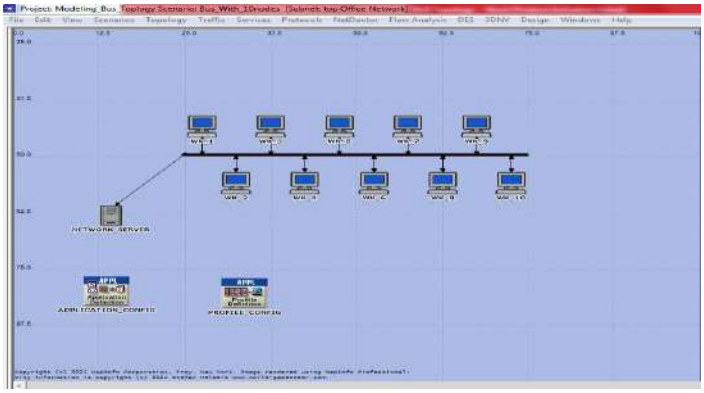


Figure 1. Bus Topology Modelled with 10 Nodes

Figure 2 shows a server configured to provide the required services which are HTTP Server, FTP Server, Email Server, and Database Server to the 20 nodes connected to the eth_coax backbone. The model was simulated for 1 hour (60 min) for optimal results.

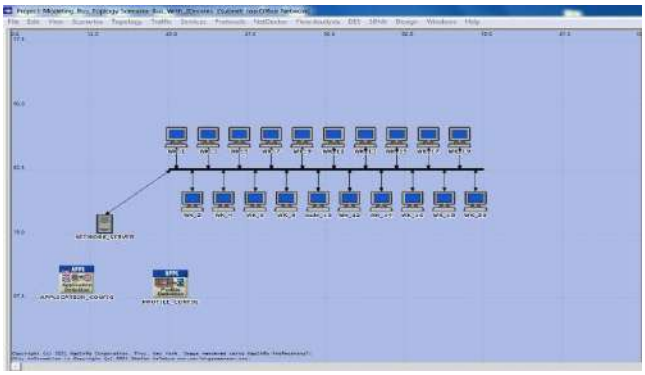


Figure 2. Bus Topology Modelled with 20 Nodes

Application configuration (default), profile configuration (configured with four (4) selected network parameters), and a server configured to provide required services such as HTTP server, FTP server, email server, and database server to 30 nodes connected to the eth_coax backbone are all shown in Figure 3. The model was simulated for 1 hour (60 min) for optimal results.

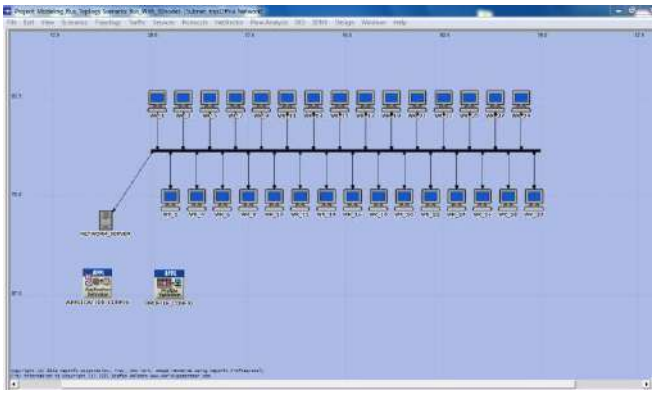


Figure 3. Bus Topology Modelled with 30 Nodes

Figure 4 shows a server configured to provide required services such as HTTP server, FTP server, email server, and database server to 40 nodes connected to the eth_coax backbone, as well as profile configuration (configured with four (4) selected network parameters). The model was simulated for 1 hour (60 min) for optimal results.

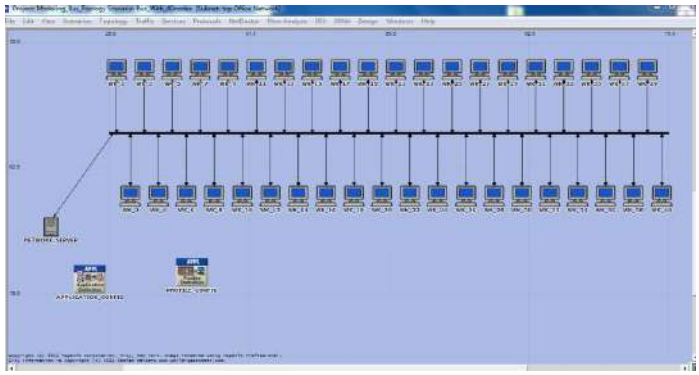


Figure 4. Bus Topology Modelled with 40 Nodes

Figure 5 depicts the bus topology modeling of the discrete encryption system (DES) execution manager for four scenarios, each of which was simulated for one hour.

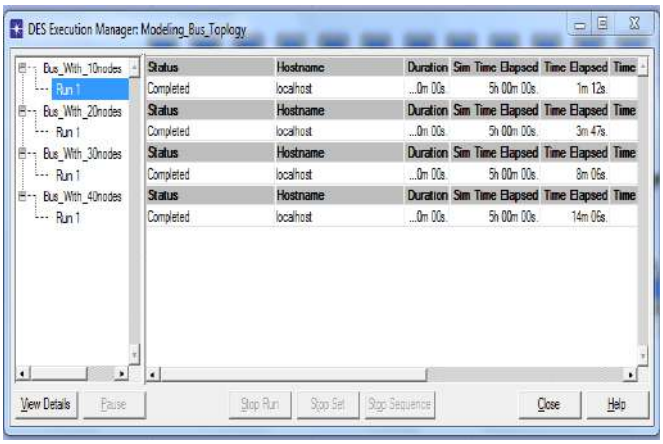


Figure 5. DES Execution Manager Modelling for Bus Topology

Some of the parameters selected for modeling the bus topology in a simulation environment are registered in Table I.

TABLE I. PARAMETERS USED

S/N	Parameters	Values
1	Application Traffic	HTTP, Ftp, Email, Database
2	Network Parameters	Delay, Traffic Sent, Traffic Received, Bits Error per Packet
3	Number of Nodes	10, 20, 30, 40
4	Link Model	Eth_Coax
5	Node Model	Ethcoax_Station
7	Tap Model	Eth_Tap
8	Data Rate	500,000bps
9	Delay	0.05 Second

IV. RESULTS AND DISCUSSION

The simulated results were presented for various scenarios. The results for a bus topology modeled with 10 nodes are shown in Table II.

TABLE II. BUS TOPOLOGY WITH 10 NODES

Time in (sec)	Delay in (sec)	Traffic Received in (bits/sec)	Traffic Sent in (bits/sec)	Through put in (bits/sec)	Bits Error Per Packet
0	0.2889	68,039.11	76,231.11	77,233.33	25.30
10	0.2872	73,201.03	82,122.27	83,598.15	38.55
20	0.2886	72,804.78	82,050.03	83,413.33	50.34
30	0.2884	72,874.67	82,055.66	83,290.85	55.61
40	0.2912	73,302.00	82,753.25	84,027.45	56.36
50	0.2912	73,350.53	82,843.61	84,140.00	56.00
60	0.2921	73,425.35	82,880.28	84,168.00	56.07

The network parameters of consideration were delay in (sec), traffic-sent in (bits/sec), traffic-received in (bits/sec) for global statistics, throughput in (bits/sec), and Bits Error per

Packet for object statistics. The results were obtained and presented in tabular form as shown in Table II after simulating for one hour. From Table II, the lower delay was observed between 0-30Secs, more traffic received between 40-60secs, greater traffic sent, and higher throughput experienced from 10-30sec, and error increases as simulation time increase.

Table III represents the results obtained for a bus topology modeled with 20 nodes. The network parameters of consideration were delay in (sec), traffic received in (bits/sec), and traffic sent in (bits/sec) considering global statistics, throughput in (bits/sec), and Bits Error per Packet for object statistics. After one hour of simulation, the results were obtained and presented in tabular form as shown below. From Table III, the higher delay was observed at 0 sec and decreased with time, greater traffic was received at 10 sec and then, from 40–60 sec, higher traffic was sent at 10 sec, higher throughput was experienced at 110 sec, and errors increased on the network as simulation time linearly increased.

TABLE III. BUS TOPOLOGY WITH 20 NODES

Time in (sec)	Delay in (sec)	Traffic Received in (bits/sec)	Traffic Sent in (bits/sec)	Throughput in (bits/sec)	Bits Error Per Packet
0	0.2748	135,623.11	151,779.56	152,366.67	88.69
10	0.2731	152,737.68	166,229.33	166,959.65	116.83
20	0.2723	151,961.60	165,114.31	165,653.33	125.71
30	0.2722	151,788.48	164,846.50	165,357.05	128.83
40	0.2715	152,161.05	164,954.35	165,416.18	129.86
50	0.2721	152,470.25	165,333.84	165,853.33	128.76
60	0.2721	152,023.04	164,998.26	165,358.67	133.05

Table IV represents the results obtained for a bus topology consists 30 number nodes. The network parameters of consideration were delay in (sec), traffic received in (bits/sec), and traffic sent in (bits/sec) based on global statistics, throughput in (bits/sec), and Bits Error for object statistics.

TABLE IV. BUS TOPOLOGY WITH 30 NODES

Time in (sec)	Delay in (sec)	Traffic Received in (bits/sec)	Traffic Sent in (bits/sec)	Throughput in (bits/sec)	Bits Error Per Packet
0	0.2650	198,428.44	222,549.33	512,600.00	260.33
10	0.2670	228,609.50	249,221.24	246,215.79	218.12
20	0.2673	227,999,66	247,905.52	245,100.00	208.76
30	0.2673	228, 540.17	248,678.07	245,547.44	214.35
40	0.2672	228,813.80	248,684.76	245,720.59	213.27
50	0.2670	228,805.77	248,656.65	245,661.57	213.08
60	0.2670	228,859.42	248,715.95	245,765.33	213.03

After one hour of simulation, the results were obtained and presented in tabular form as shown in Table IV. From this Table, the higher delay was observed from 20 sec to 30 sec and decreased with time, greater traffic was received from 40 sec to 60 sec, greater traffic was sent at 10 sec, higher throughput was experienced at 10 sec, and more errors per packet were observed at 0 sec and decreased on the network as simulation time increased.

Table V represents the results obtained for a bus topology modeled with 40 nodes. The network parameters of consideration were delay in (sec), traffic received in (bits/sec), traffic sent in (bits/sec) for global statistics, throughput in (bits/sec), and Bits Error for object statistics.

TABLE V. BUS TOPOLOGY WITH 40 NODES

Time in (sec)	Delay in (sec)	Traffic Received in (bits/sec)	Traffic Sent in (bits/sec)	Throughput in (bits/sec)	Bits Error Per Packet
0	0.2677	259,640.89	295,367.11	284,666.66	306.28
10	0.2635	303,834.57	332,458.67	325,229.83	265.19
20	0.2647	303,286.04	331,561.45	324,360.00	269.67
30	0.2639	303,016.47	331,039.79	323,674.51	272.20
40	0.2635	303,492.18	331,665.57	324,158.33	274.79
50	0.2641	303,272.66	331,310.18	323,968.24	272.71
60	0.2638	302,785.42	330,870.33	323,456.00	273.76

The results were obtained and presented in tabular form as shown above after being simulated for one hour. Table V shows that the higher delay was observed at 0 sec and varied time, that more traffic was received at 10 sec, that greater traffic was sent at 10 sec, that higher throughput was observed at 10 sec and varied time, and that more errors per packet were observed and varied time as the simulation time increased.

The delay (sec) for each scenario is listed in Table VI, and the graphical representation of this Table is shown in Figure 6.

TABLE VI. DELAY IN SECS FOR ALL SCENARIOS

Time in (sec)	Delay (sec) in for 10 Nodes	Delay (sec) in for 20 Nodes	Delay (sec) in for 30 Nodes	Delay (sec) in for 40 Nodes
0	0.2889	0.2748	0.2650	0.2677
10	0.2872	0.2731	0.2670	0.2635
20	0.2886	0.2723	0.2673	0.2647
30	0.2884	0.2722	0.2673	0.2639
40	0.2912	0.2715	0.2672	0.2635
50	0.2912	0.2721	0.2670	0.2641
60	0.2921	0.2721	0.2670	0.2638

A comparative analysis of various scenarios in tabular form was carried out based on the given network parameters to obtain the effective performance of this topology. Figures 6–10 show the graphical representation of the findings.

Figure 6 shows the graph for all of the delays (sec) considered for different nodes. During the data transmission process, it was clear that a bus topology with 10 nodes had the highest delay (sec), while a topology with 40 nodes had the lowest delay (sec).

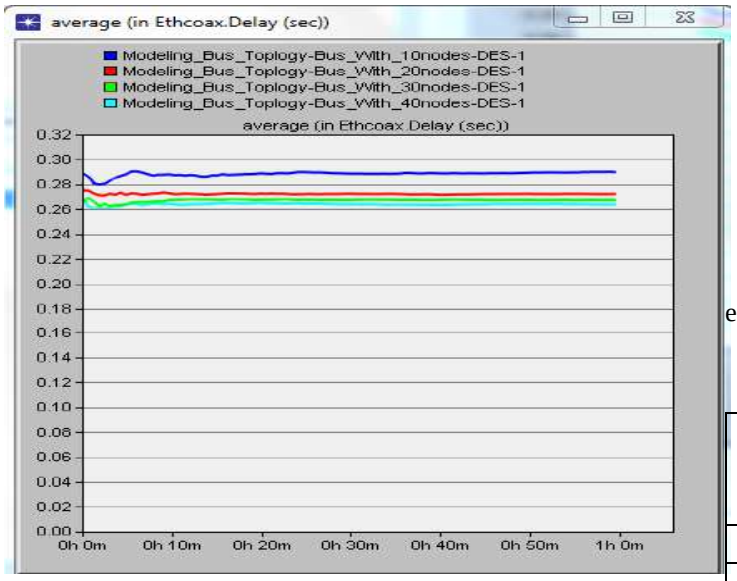


Figure 6. Delay in sec for all Scenarios

The traffic received in (bits/sec) for all scenarios is listed in Table VII, and a graphical representation of this Table is shown in Figure 7.

TABLE VII. TRAFFIC RECEIVED IN BITS/SEC FOR ALL SCENARIOS

Time in (sec)	Traffic Received for 10 Nodes in (bits/sec)	Traffic Received for 20 Nodes in (bits/sec)	Traffic Received for 30 Nodes in (bits/sec)	Traffic Received for 40 Nodes in (bits/sec)
0	68,039.11	135,623.11	198,428.44	259,640.89
10	73,201.03	152,737.68	228,609.50	303,834.57
20	72,804.78	151,961.60	227,999,66	303,286.04
30	72,874.67	151,788.48	228, 540.17	303,016.47
40	73,302.00	152,161.05	228,813.80	303,492.18
50	73,350.53	152,470.25	228,805.77	303,272.66
60	73,425.35	152,023.04	228,859.42	302,785.42

The graph for all the traffic received (bits/sec) is presented in Figure 7. It is crystal clear that a bus topology with 40 nodes received the most traffic (bits/sec), while a topology with 10 nodes experienced the lowest traffic (bits/sec) during the data transmission process.

Figure 7. Traffic Received in Bits/Sec for all Scenarios

Table VIII, which shows the traffic sent in (bits/sec) for each scenario, is represented graphically in Figure 8.

TABLE VIII. TRAFFIC SENT IN BITS/SEC FOR ALL SCENARIOS

Time in (sec)	Traffic Sent for 10 Nodes in (bits/sec)	Traffic Sent for 20 Nodes in (bits/sec)	Traffic Sent for 30 Nodes in (bits/sec)	Traffic Sent for 40 Nodes in (bits/sec)
0	76,231.11	151,779.56	222,549.33	295,367.11
10	82,122.27	166,229.33	249,221.24	332,458.67
20	82,050.03	165,114.31	247,905.52	331,561.45
30	82,055.66	164,846.50	248,678.07	331,039.79
40	82,753.25	164,954.35	248,684.76	331,665.57
50	82,843.61	165,333.84	248,656.65	331,310.18
60	82,880.28	164,998.26	248,715.95	330,870.33

Figure 8 shows that during the data transmission process, a bus topology with 40 nodes sent the most traffic (bits/sec), while a topology with 10 nodes experienced the least traffic (bits/sec).

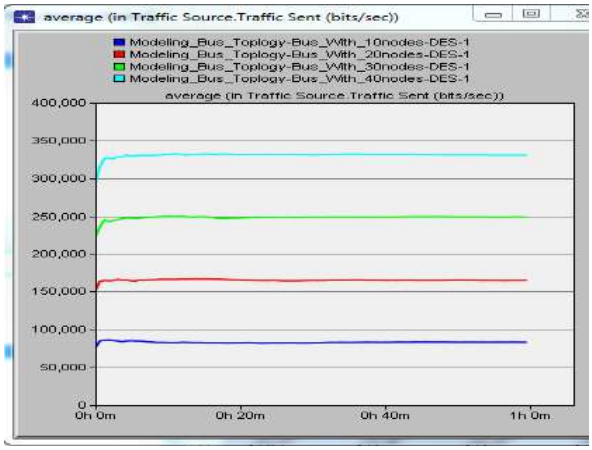


Figure 8. Traffic Sent in Bits/Sec for all Scenarios

Table IX shows the throughput (bits/sec) for all of the scenarios, and Figure 9 shows the graphical representation of this Table.

TABLE IX. THROUGHPUT IN BITS/SEC FOR ALL SCENARIOS

Time in (sec)	Throughput for 10 Nodes in (bits/sec)	Throughput for 20 Nodes in (bits/sec)	Throughput for 30 Nodes in (bits/sec)	Throughput for 40 Nodes in (bits/sec)
0	77,233.33	152,366.67	512,600.00	284,666.66
10	83,598.15	166,959.65	246,215.79	325,229.83
20	83,413.33	165,653.33	245,100.00	324,360.00
30	83,290.85	165,357.05	245,547.44	323,674.51
40	84,027.45	165,416.18	245,720.59	324,158.33
50	84,140.00	165,853.33	245,661.57	323,968.24
60	84,168.00	165,358.67	245,765.33	323,456.00

Figure 9 shows that during the data transmission process, a bus topology with 40 nodes experienced higher throughput (bits/sec), while a topology with 10 nodes experienced the lowest throughput (bits/sec).

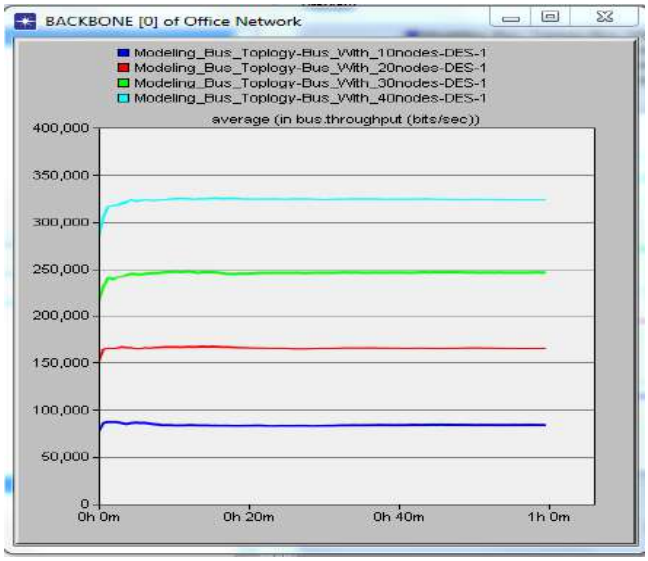


Figure 9. Throughput in Bits/Sec for all Scenarios

The Bits Error per Packet for all of the scenarios is presented in Table X below, with a graphical representation in Figure 10.

TABLE X. BITS ERROR PER PACKET FOR ALL SCENARIOS

Time in (sec)	Bits Error Per Packet for 10 Nodes	Bits Error Per Packet for 20 Nodes	Bits Error Per Packet for 30 Nodes	Bits Error Per Packet for 40 Nodes
0	25.30	88.69	260.33	306.28
10	38.55	116.83	218.12	265.19
20	50.34	125.71	208.76	269.67
30	55.61	128.83	214.35	272.20
40	56.36	129.86	213.27	274.79
50	56.00	128.76	213.08	272.71
60	56.07	133.05	213.03	273.76

Figure 10 shows that a bus topology with 40 nodes had higher bit errors per packet during the data transmission process than a topology with 10 nodes, which had the lowest bit errors per packet.

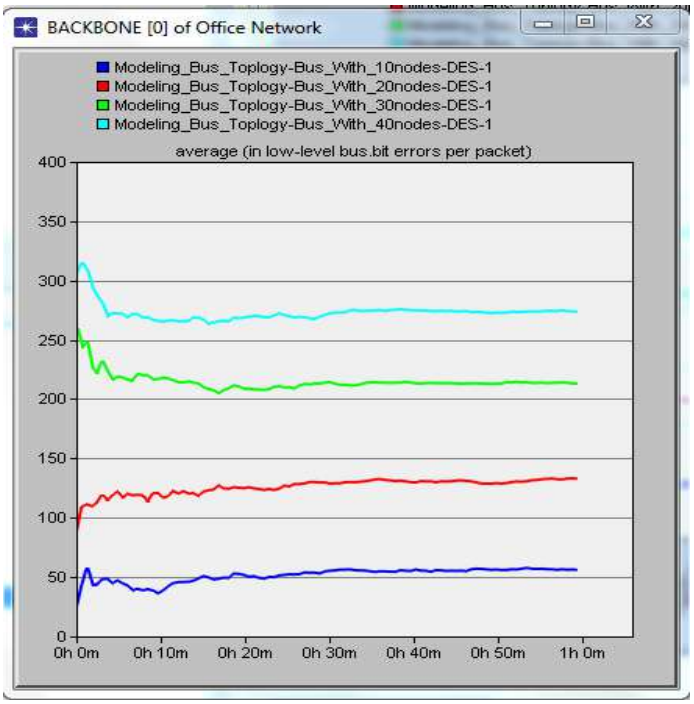


Figure 10. Bits Error per Packet for all Scenarios

V. CONCLUSION

Considering the vital and prevalent concern of distributed computers with the ability to provide great performance at a moderate cost, different computers were linked to provide effective data distribution. However, based on the results obtained from the simulation environment, it is crystal clear that delays were higher in scenarios with lower nodes. But this result was contrary to the presumption that scenarios with fewer nodes would experience little or no delay. Furthermore, the scenario with higher nodes sent and received more traffic than those with lower scenarios. The scenario with a larger number of nodes experienced higher throughput as a result of the longer backbone (eth_coax) and also encountered the problem of higher bit errors per packet because of the high collision rate experienced in the network with larger nodes. In the nearest future, more research into the performance of this topology could be done by taking into account, a variety of other network parameters to learn more about the bus topology performance.

REFERENCES

[1] C. G. Maranan, J. B. Enriquez, & B. T. Tanguilig.Optimized Network Topology for e-Learning Zone. International Journal of Engineering and Technical Research (IJETR) Vol. 3, Issue 8, pp. 71-77, 2015.

[2] A. Jain, & Verma, S. Simulation and Performance Comparison of Different Expansions of Star Network Using Opnet. International Journal of Advanced Research in Computer Science, Vol 4, Issue 10, Pp. 194-200, 2013.

[3] S. Kaur, & M. Gothwal. Simulation and Performance Comparison of different Expansions of Star Network using Opnet. International Journal of Advanced Technology in Engineering and Science, Vol 2, Issue 1, Pp. 41-47, 2014.

[4] A. A. Atayero, A. S. Alatishe, & J. O. Iruemi, Modeling and Simulation of a University LAN in OPNET Modeller Environment. International Journal of Emerging Technology and Advanced Engineering, 2012.

[5] O. J. Adaramola, & J. R. Olasina. Network Model Analysis in Opnet Simulation. International Journal of Engineering Applied Sciences and Technology, Vol 5, Issue 1, Pp. 47-51, 2020.

[6] M. Hammoshi, & R. Al-Ani. Using OPNET to Teach Students Computer Networking Subject. Tikrit Journal of Pure Science, Vol 15, Issue 1, Pp. 1-12, 2010.

[7] M. Doheir, B. Hussin, & A. S. Basari. An Enhancement of Performance for Network Configuration at FTMK Using OPNET. International Journal on Communications Antenna and Propagation (I.Re.C.A.P.), Vol 4, Issue 5, Pp. 157-161, 2014.

[8] R. Shelat, & M. Bhatt. Analysis and Implementation of Bus Topology in OPNET Simulator Environment. International Journal of Latest Trends in Engineering and Technology Vol 7, Issue 3, Pp. 479-484, 2017.

[9] Q. Liu, & Q. Liu. A Study on Topology in Computer Network. 2014 7th International Conference on Intelligent Computation Technology and Automation, 2014

[10] N. Bisht, & S. Singh. Analytical Study of Different Network Topologies. International Research Journal of Engineering and Technology (IRJET), Vol 2, Issue 1, Pp. 88-90, 2015.

[11] M. S. Deshmukh, & P. V. Dudhe. A Succinct Study of different Computer Network Topologies. International Journal of Innovative and Emerging Research in Engineering. Vol 3, Issue 1, Pp. 63-66, 2016.

[12] D. K. Aristarkus, S. Palaniappan, & T. Purnshatman. Hybrid Topology Design for Improving Network Performance. Global Journal of Computer Science and Technology: E Network, Web & Security, Vol 17, Issue 3, Pp. 24-30, 2017.

[13] N. N. Qaqos, S. R. M. Zeebaree, & B. K. Hussan. Opnet Based Performance Analysis and Comparison among Different Physical Network Topologies. Academic Journal of Nawroz University (AJNU). 7(3), Pp. 48- 54, 2018.

AUTHORS PROFILE

Mr. Adaramola Ojo Jayeola has completed his M.Sc. degree in Computer Systems and Network Engineering from the University of Greenwich, London, United Kingdom in 2016, and his M.Sc. in Electronics and computers engineering from Lagos State University, Nigeria in 2018. He is currently working as Chief Technologist in the Department of Computer Engineering at the Federal Polytechnic Ilaro, Ogun State, Nigeria. Adaramola is a member of the engineering professional body in Nigeria (Council for the Regulation of Engineering in Nigeria) and many societies and associations including The Nigerian Institution of Professional Engineers and Scientists (NIPES), The Nigerian Society of Engineering Technicians (NIST), The Society of Digital Information and Wireless Communication (SDIWC), the International Association of Engineers (IAENG), and the International Computer Science and Engineering Society (ICSES). He has published articles in prestigious journals and has attended both local and international conferences. His areas of interest are computer hardware and networking, wireless communication, routing protocols, vehicular ad-hoc networks, and ZigBee technology.

Mr. Olasina, Jamiu Rotimi completed his M.Eng in Electrical and Information Engineering(Computer Engineering) from Covenant University, Ota, Nigeria. He Obtained B.Eng in Electrical and Computer Engineering, from the Federal University of Technology, Minna, Nigeria. He also obtained a National Diploma in Computer Engineering, from the Federal Polytechnic Ilaro, Nigeria. Engr. Olasina, J. R is a lecturer, in the Department of Computer Engineering, Federal Polytechnic Ilaro, Nigeria., and he also researches in the domain of software-defined radio, radio communication, cognitive radios, 5G technology, Data communication and networking, AI and Machine Learning, etc. He is conversant with the use of many tools like Matlab, Python, Linux, C and C++ programming, GNU-Radio companion, Arduino sketch, etc. He is a registered computer engineer with the Council for the Regulation of Engineering in Nigeria (Coren), The Nigerian Institution of Professional Engineers and Scientists (NIPES), The Society of Digital Information and Wireless Communication (SDIWC), and the International Association of Engineers (IAENG).

Call for Papers

International Journal of Engineering and Applied Computer Science (IJEACS) invites authors to submit their manuscripts for categories like research papers, review articles, survey papers, technical reports, reports of unsuccessful research projects, case studies, tutorials, book reviews, short communications, and cross talk, extended version of conference papers for publication in our monthly issue.

IJEACS reviews manuscripts through a double-blind peer-review process. Authors can submit their original, unpublished manuscript which is not under consideration for publication in any journal or conference through email. IJEACS publishes papers in major streams of Engineering and Computer Science including the following but not limited to.

Computer Science

- Software Design and Modeling
- Service-Oriented Architecture
- Open-Source Software
- Software Testing and Maintenance
- Software Measurement and Reliability
- Knowledge-based Systems
- Image Processing and Computer Graphics
- Extreme Programming and Formal Methods
- Artificial Intelligence, Image Recognition, and Biometrics.
- Machine Learning and Computer Vision
- Algorithm Analysis and Design
- Computational Mathematics
- Data Structures and Graph Theory
- Video Coding and Data Compression
- Database Systems and Big Data Analytics
- Internet of Things, Architecture and Computing
- Parallel and Distributed Computing
- Cloud Computing, Agent-Oriented System
- Communication Network and Systems

- Embedded Systems and Applications
- Cryptography and Information Assurance
- Computational Biology and Bioinformatics
- Human-Computer Interaction
- Natural Language Processing

Engineering

- Micro Processor Architecture and Design
- VLSI/IC Microelectronics and Computer Design
- Parallel Processing and Digital Systems
- Wireless Transmission and Mobile Communication
- Antenna and Wave Propagation
- Semiconductors, Circuits, and Signal System
- Material Science and Metallurgy
- Machine and System Design
- Robotics and Automated Control
- Manufacturing Processes and CAD/CAM
- Quality Control and Assurance
- Digital Signal Processing
- Photonics, Fiber Optics, and Optical Communication
- Biosensors, Electrical-based Interactions
- Nanoelectronics Devices and Silicon Micro/Nano Electronics Applications
- Distributed monitoring systems and Smart Systems
- Fluid Dynamics and Implementations
- Mechanics and Vibration
- Heat Transfer
- Combustion Engines and Automobiles
- Health Instrumentations and Technologies
- Thermal Engineering
- Solar Power Systems
- Ergonomics

Submit your manuscript to:

ijeacs@gmail.com or submit@ijeacs.com or ed.manager@ijeacs.com

Innovations continue to serve the humanity

Issue Highlights

9 780995 707542

International Journal of Engineering and Applied Computer Science

Volume: 04, Issue: 02, March 2022

ISBN: 9780995707542