ACADEMIC YEAR(2022-2023)						
S.No	**Name of the course**	**Course Code**	**Programme Offering**	**Project work**	**Internip training**	**Number of students**
1	Project Work	MC5414	MASTER OF COMPUTER APPLICATIONS	✓		3
2	Python Programming	MC5107	MASTER OF COMPUTER APPLICATIONS	✓		1
3	Advanced Database Technology	MC5105	MASTER OF COMPUTER APPLICATIONS		✓	3
4	Artificial Intelligence and Machine Learning	MC5208	MASTER OF COMPUTER APPLICATIONS	✓		1
5	Data Science	MC5306	MASTER OF COMPUTER APPLICATIONS		✓	1
6	Internet Programming	MC5206	MASTER OF COMPUTER APPLICATIONS	✓		3
7	Cloud Computing Technologies	MC5207	MASTER OF COMPUTER APPLICATIONS	✓		2

PRINCIPAL
JKK MUNIRAJAH COLLEGE
OF TECHNOLOGY
T.N. PALAYAM (Po)-638 506.
GOBI (Tk), ERODE (Dt).

J.K.K. MUNIRAJAH COLLEGE OF TECHNOLOGY

Approved by AICTE, New Delhi And Affiliated to Anna University, Chennai.

Accredited by NAAC with "A" grade

T.N. Palayam (Po), Gobi (Tk), Erode (Dt) – 638 506

MASTER OF COMPUTER APPLICATIONS

2022-2023

S.NO	REG.NO	STUDENT NAME	PROJECT	INTERNSHIP
1	731221622005	MONISHA.S		✓
2	731221622007	PERINBARAJ.S		✓
3	731221622008	PRADEESHKUMAR.N		✓
4	731221622009	SOWMIYA.R		✓

PRINCIPAL
JKK MUNIRAJAH COLLEGE
OF TECHNOLOGY
T.N. PALAYAM (Po)-638 506.
GOBI (Tk), ERODE (Dt).

J.K.K.MUNIRAJAHCOLLEGEOFTECHNOLOGY

Approved by AICTE, NewDelhi And Affiliated to Anna University,Chennai.

T.N.Palayam(Po),Gobi(Tk),Erode(Dt)–638506

MASTER OF COMPUTER APPLICATIONS

S.No	Name of the Course that include experiential learning through Project Work/Internship/Field Visit
1	Project Work
2	Python Programming
3	Advanced Database Technology
4	Artificial Intelligence and Machine Learning
5	Data Science
6	Internet Programming
7	Cloud Computing Technologies

PRINCIPAL
JKK MUNIRAJAH COLLEGE
OF TECHNOLOGY
T.N. PALAYAM (Po)-638 506.
GOBI (Tk), ERODE (Dt).

PROJECT

DEFECT TRACKING SYSTEM

A PROJECT REPORT

Submitted by

L N NAVANEETHARAN (731220622001)

in partial fulfillment for the award of the degree

of

MASTER OF COMPUTER APPLICATIONS

J.K.K.MUNIRAJAH COLLEGE OF TECHNOLOGY

T.N.PALAYAM, GOBI-638 512

ANNA UNIVERSITY: CHENNAI 600 025

SEPTEMBER 2022

PRINCIPAL
JKK MUNIRAJAH COLLEGE
OF TECHNOLOGY
T.N. PALAYAM (Po)-638 506.
GOBI (Tk), ERODE (Dt).

ANNA UNIVERSITY:CHENNAI 600 025

BONAFIDE CERTIFICATE

Certified that this project report on **"DEFECT TRACKING SYSTEM"** is the bonafide work of **"L.N.NAVANEETHARAN (731220622001)"** who carried out the project work under my supervision.

SIGNATURE

Dr.N.SATHYABALAJI.M.E,M.I.S.T.E.,Ph.D.,
HEAD OF THE DEPARTMENT
Associate Professor
Dept. of Computer Applications
J.K.K. Munirajah College of Technology
T.N. Palayam

5.9.22 M.Senthilkumar

SIGNATURE

Mr.M.SENTHILKUMAR.MCA,.
SUPERVISOR
Assistant Professor
Dept. of Computer Applications
J.K.K. Munirajah College of Technology
T.N. Palayam

Submitted for the Project Viva-Voce examination held on 05.09.2022

5.9.22 M.Senthilkumar MCA,MPhil

INTERNAL EXAMINER

EXTERNAL EXAMINER

PRINCIPAL
JKK MUNIRAJAH COLLEGE
OF TECHNOLOGY
T.N. PALAYAM (Po)-638 506,
GOBI (Tk), ERODE (Dt).

ABSTRACT

Bug-Tracking mechanism is employed only is some of the large software development houses. Most of the others never bothered with bug tracking at all, and instead simply relied on shared lists and email to monitor the status of defects. This procedure is error-prone and tends to cause those bugs judged least significant by developers to be dropped or ignored.

Bug-Tracking System is an ideal solution to track the bugs of a product, solution or an application. Bug Tacking System allows individual or groups of developers to keep track of outstanding bugs in their product effectively. This can also be called as Defect Tracking System.The Bug Tracking System can dramatically increase the productivity and accountability of individual employees by providing a documented work flow and positive feedback for good performance.

Features:

- Product and Component based
- Creating & Changing Bugs at ease
- Query Bug List to any depth
- Reporting & Charting in more comprehensive way
- User Accounts to control the access and maintain security
- Simple Status & Resolutions
- Multi-level Priorities & Severities
- Targets & Milestones for guiding the programmers
- Attachments & Additional Comments for more information
- Robust database back-end

CHAPTER 1

INTRODUCTION

1.1 Purpose

The main objective of this system is develop flawless system, which is access real time information from anywhere in the world, 24 hours a day 365 days in a year. Another aim is that manage hundred of projects in multiple locations or just a few. The another main objective of this system is track the all the defects or bugs in the project and make the project user friendly and bugs free system.

1.2 Existing System

In any software development bugs are inevitable. Let it be in any kind of product bugs arise at any phase of development. One has to take a great care in the proper maintenance and resolution of the bugs. In the Existing system the bugs are not properly maintained and they are simply relied on shared lists and email to monitor the bugs.

In this type of system it becomes difficult to track a bug if a bug is over looked then it may cause tremendous errors in the next phase and can improve the cost of project whatever necessary effort spent on the bug maintenance may not be worthy. So bug history has to be maintained properly. And there is no efficient search technique.

One has to search the whole database for the details of particular bug which might have occurred sometime earlier. It is both time consuming and error prone. And it is very difficult to share the bug among several users as there is no proper maintenance

of the bugs. In order to have an efficient product bugs must be maintained properly and should be resolved in time both to reduce time and money spent on the development.

1.3 Proposed System

- This system maintains the products, Bugs and bug Tracking. It has advantage of maintaining bug history it stores all the details from bug origin to bug resolution.
- Each product can have versions for easy maintenance of the product and all the user of the product is stored in the database. It provides the advantage of maintaining users to the bugs and resolutions provided by them.
- Our System provides the searching based on status, priority, and operating system.
- It provides with user and bug hierarchy, which would be helpful in knowing the relation between bugs and users allotted to the bug.
- It is provided with a fully authenticated system with password encryption. And has the facility for storing attachments for a bug.
- One can keep a track of the bug in a product with much lower cost and effort.
- The most advantage of this system is maintaining log records which are helpful in knowing any errors or misuse of the system by other users.

CHAPTER 9

CONCLUSION

User comes to the search engine and makes a query, typically by giving key words, the engine looks up the index and provides a listing of best-matching web pages according to its criteria, usually with a short summary containing the document's title and sometimes parts of the text.

Most search engines employ methods to rank the results to provide the "best" results first. How a search engine decides which pages are the best matches, and what order the results should be shown in, varies widely from one engine to another.

Search engine is technically the software and algorithms used to perform a search, the term have become synonymous with the website itself.

FUTURE ENHANCEMENT

Currently, this project is a simple prototype, but it can be improvised in future with some enhancements. At present, there is no live chat feature for helping clients which can be added in future . An online help document also can be added on the home page of the website which would give instructions for setup and installation. Currently, this project supports only English language. However, in future, multiple language support can be included. In addition, features such as scrum-ban boards and ability to build reports based on the bug history can be included. This would help software professionals in statistical analysis. Lastly, user interface can be enhanced by including the ability to configure Agile boards based on sprint cycle. As most of the software industry is adapting Agile methodology, this feature would benefit all organizations.

AN EFFICIENT SPAMDETECTION TECHNIQUE FOR IOT DEVICES USING MACHINE LEARNING

APROJECTREPORT

Submittedby

NITHYA A (731220622002)

inpartialfulfillmentfortheawardofthedegree

of

MASTER OF COMPUTER APPLICATION

J.K.K.MUNIRAJAH COLLEGE OF TECHNOLOGYT.N.PALAYAM,GOBI-638512

ANNAUNIVERSITY:CHENNAI600025

SEPTEMBER 2022

ANNA UNIVERSITY: CHENNAI 600 025

BONAFIDE CERTIFICATE

Certified that this project report on **"AN EFFICIENT SPAM DETECTION TECHNIQUE FOR IOT DEVICES USING MACHINE LEARNING "** is the bonafide work of **"NITHYA A (731220622002)"** who carried out the project work under my supervision.

SIGNATURE
Dr.N.SATHYABALAJI.M.E,M.I.S.T.E.,Ph.D.,
HEAD OF THE DEPARTMENT
Associate Professor
Dept. of Computer Applications
J.K.K. Munirajah College of Technology
T.N. Palayam

SIGNATURE
Mrs.A.KANIMOZHI.MCA., M.Phil.,
SUPERVISOR
Assistant Professor
Dept. of Computer Applications
J.K.K. Munirajah College of Technology
T.N. Palayam

Submitted for the Project Viva-Voce examination held on 5/9/2022

INTERNAL EXAMINER

EXTERNAL EXAMINER

PRINCIPAL
JKK MUNIRAJAH COLLEGE
OF TECHNOLOGY
T.N. PALAYAM (Po)-638 506.
ERODE (Dt).

ABSTRACT

The Internet of Things (IoT) is a group of millions of devices having sensors and actuators linked over wired or wireless channel for data transmission. IoT has grown rapidly over the past decade with more than 25 billion devices are expected to be connected by 2020. The volume of data released from these devices will increase many-fold in the years to come. In addition to an increased volume, the IoT devices produces a large amount of data with a number of different modalities having varying data quality defined by its speed in terms of time and position dependency. In such an environment, machine learning algorithms can play an important role in ensuring security and authorization based on biotechnology, anomalous detection to improve the usability and security of IoT systems. On the other hand, attackers often view learning algorithms to exploit the vulnerabilities in smart IoT-based systems. Motivated from these, in this project, we propose the security of the IoT devices by detecting spam using machine learning. To achieve this objective, Spam Detection in IoT using Machine Learning framework is proposed. In this framework, five machine learning models are evaluated using various metrics with a large collection of inputs features sets. Each model computes a spam score by considering the refined input features. This score depicts the trustworthiness of IoT device under various parameters. REFIT Smart Home dataset is used for the validation of proposed technique. The results obtained proves the effectiveness of the proposed scheme in comparison to the other existing schemes.

PRINCIPAL
JKK MUNIRAJAH COLLEGE
OF TECHNOLOGY
T.N. PALAYAM (Po)-638 506.
GOBI (Tk), ERODE (Dt).

CHAPTER 1
INTRODUCTION

1.1 About the project

Internet of Things (IoT) enables convergence and implementations between the real world objects irrespective of their geographical locations. Implementation of such network management and control make privacy and protection strategies utmost important and challenging in such an environment. IoT applications need to protect data privacy to fix security issues such as intrusions, spoofing attacks, DoS attacks, DoS attacks, jamming, eavesdropping, spam, and malware. The safety measures of IoT devices depend upon the size and type of organization in which it is imposed.

The behavior of users forces the security gateways to cooperate. In other words, we can say that the location, nature, application of IoT devices decides the security measures. For instance, the smart IoT security cameras in the smart organization can capture the different parameters for analysis and intelligent decision making. The maximum care to be taken is with web based devices as maximum number of IoT devices are web dependent. It is common at the workplace that the IoT devices installed in an organization can be used to implement security and privacy features efficiently.

For example, wearable devices collect and send user's health data to a connected smartphone should prevent leakage of information to ensure privacy. It has been found in the market that 25-30% of working employees connect their personal IoT devices with the organizational network.

The expanding nature of IoT attracts both the audience, i.e., the users and the attackers. However, with the emergence of ML in various attacks scenarios, IoT devices choose a defensive strategy and decide the key parameters in the security protocols for trade-off between security, privacy and computation. This job is challenging as it is usually difficult for an IoT system with limited resources to estimate the current network and timely attack status.

A. Contributions Based upon the above discussions, following contributions are presented in this paper. 1) The proposed scheme of spam detection is validated using five different machine learning models. 2) An algorithm is proposed to compute the spamicity score of each model which is then used for detection and intelligent decision making. 3) Based upon the spamicity score computed in previous step, the reliability of IoT devices is analyzed using different evaluation metrics. B. Organization Rest of the paper is structured as follows. Section II discussed the related work. Section III illustrated the proposed scheme. Results are discussed and analyzed in Section IV. Finally, the paper is concluded in Section V.

CHAPTER 9
CONCLUSION AND ENHANCEMENT

The proposed framework, detects the spam parameters of IoT devices using machine learning models. The IoT dataset used for experiments is preprocessed by using feature engineering procedure. By experimenting the framework with machine learning models, each IoT appliance is awarded with a spam score. This refines the conditions to be taken for successful working of IoT devices in a smart home. In future, we are planning to consider the climatic and surrounding features of IoT device to make them more secure and trustworthy.

FUTURE ENHANCEMENT

- We are planning to consider the climatic and surrounding features of IoT device to makethem more secure and trustworthy.
- IoT devices using AI models will be able to clearly delineate their spam bounds. Using a highlight design technique, the IoT dataset used for testing is pre-processed. Using artificial intelligence (AI) algorithms, each IoT device receives.
- This improves the conditions necessary for smart home IoT devices to functioneffectively.

ACCESS CONTROL FOR CLOUD BASED DATA STORAGE

A PROJECT REPORT

Submitted by

A.K.THARUN VISHAL (731220622005)

In partial fulfillment for the award of the degree

of

MASTER OF COMPUTER APPLICATIONS

J.K.K.MUNIRAJAH COLLEGE OF TECHNOLOGY

T.N.PALAYAM, GOBI-638506

ANNA UNIVERSITY::CHENNAI 600025

SEPTEMBER 2022

PRINCIPAL
JKK MUNIRAJAH COLLEGE
OF TECHNOLOGY
T.N. PALAYAM (Po)-638 506.
GOBI (Tk), ERODE (Dt).

ANNA UNIVERSITY:CHENNAI 600 025

BONAFIDE CERTIFICATE

Certified that this project report on **"ACCESS CONTROL FOR CLOUD BASED DATA STORAGE"** is the bonafide work of **"A.K.THARUN VISHAL (731220622005)"** who carried out the project work under my supervision.

SIGNATURE
Dr.N.SATHYABALAJI.M.E,M.I.S.T.E.,Ph.D.,
HEAD OF THE DEPARTMENT
Associate Professor
Dept. of Computer Applications
J.K.K. Munirajah College of Technology
T.N. Palayam

SIGNATURE
Mr.M.SENTHILKUMAR.MCA,.
SUPERVISOR
Assistant Professor
Dept. of Computer Applications
J.K.K. Munirajah College of Technology
T.N. Palayam

Submitted for the Project Viva-Voce examination held on 05.09.2022

INTERNAL EXAMINER

EXTERNAL EXAMINER

PRINCIPAL
JKK MUNIRAJAH COLLEGE
OF TECHNOLOGY
T.N. PALAYAM (Po)-638 506.
GOBI (Tk), ERODE (Dt).

ABSTRACT

Distributed computing is a high-level breakthrough in the making. Information storage is a huge headache for everyone in this world. Distributed computing is an excellent solution for storing and retrieving data in the most straightforward and quickest way possible. Security is the most pressing concern in distributed computing. I'm attempting to show another approach for giving distributed computing had admission control in this paper. In distributed computing, this architecture provides secured admittance control. It adopts a progressive construction and use a clock to provide more granular access control. We can easily transmit, download, and delete documents from and to the cloud using this method. Access Control, Cloud Computing, and Cloud Privacy are some of the terms on the list. the National Institute of Standards and Technology states that. This decentralised computing has numerous advantages, especially in ubiquitous administrations where everyone can access PC administrations over the internet. You may create a device with a small display, processor, and RAM using distributed computing. Different types of equipment,such as extra memory, are not required. It will make our new invention gadgets smaller. In addition, it lowers our framework's costs. Virtualization, will on- demand configuration, Internet administration delivery, and it open source programming are all examples of distributed computing.

CHAPTER 1
INTRODUCTION

Due to its extensive list of advantages, which includes access freedom and the lack of local data management, in many Internet-based commercial products (such as Apple iCould). Nowadays, a growing number of people and businesses prefer to outsource their data to faraway clouds in order to avoid having to upgrade their local data management facilities or devices. However, one of the biggest barriers preventing Internet users from embracing cloud- based storage services generally may be their concern about security breaches involving outsourced data. Outsourced data may need to be subsequently shared with others in many practical scenarios. Alice, a Dropbox user, might send her friends pictures. Without employing data encryption, Alice must first create a sharing link and then distribute it to others in order to share the images. The sharing link may be exposed at the Dropbox administration level, even though it guarantees some level of access restriction over unauthorized users (for example, those who are not Alice's friends) (e.g., administrator could reach the link).

A simple solution to prevent shared photos from being accessed by system "insiders" is to specify the group of authorized data users before encrypting the data. However, Alice might not always be aware of who will be receiving or using the photos. Alice might only be aware of attributes related to photo receivers. Here, conventional public key encryption is used (e.g., Paillier Encryption),That cannot be used since it requires the encryptor to know who the data recipient is beforehand. It is therefore desirable to provide a policy-based encryption method over the outsourced photographs, such that Alice may use the mechanism to set access policies over the encrypted photos to ensure that only a select group of authorized people can access the photos. A frequent exploit known as a resource-exhaustion attack exists in cloud-based storage services.

1.1 DOMAIN OVERVIEW

One of the emerging developments is distributed computing. It addresses a fundamental shift in perspective in the way frameworks are communicated [8]. "Distributed computing is a model for enabling pervasive, advantageous, on-request network access to a common pool of configurable figuring assets (e.g., networks, servers, capacity, applications, and administrations) that can be quickly provisioned and delivered with insignificant administration exertion or specialist organization connection. A malicious service user may launch denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks to consume the resources of the cloud storage service server in order to disrupt the cloud service because a (public) cloud may not have any control over download requests (i.e., a service user may send an unlimited number of download requests to the cloud server).Could not fulfill the service needs of sincere customers. Due to increased resource demand, the "pay-as-you-go" model runs the risk of upsetting the economy. Users of cloud services will experience a sharp increase in costs as the attacks intensify. This is referred to as an Economic Denial of Sustainability (EDoS) assault, which attacks the financial resources of cloud adopters.

1.2 SCOPE OF THE PROJECT

Distributed computing attacks have grown in tandem with the advent of cloud applications. As a result of these attacks, we urgently require a more advanced distributed computing security policy. Access control is a strategy or approach that allows, denies, or restricts access to a framework. It may also detect clients attempting to gain access to an unapproved system. One application can relay on another's identification thanks to access control [8]. The traditional model for access control, application-driven access control [1] is a common access control architecture in each application monitors and manages its own set of clients, isn't possible in cloud-based systems. Because we need a lot of memory for this strategy, we'll need a lot of RAM to store the client's nuances, such as username and secret phrase. As a result, the cloud necessitates a client-driven access control system, in which each client solicitation to any specialist organization is packed with the client's personality and privilege data. In distributed computing, we currently have a plethora of processes for access control. These, on the other hand, are not obtained and effective. As a result of this problem, we are attempting to suggest a new and more effective access control technique for distributed computing.

CONCLUSION

It is a highly efficient model for providing cloud computing access control. It has a hierarchical structure and uses a clock to provide a time-based decryption key. In cloud computing, this paradigm ensures both security and access control. Registration, file upload, file download, and file deletion are the major operations in this model.

We presented the idea of SE-EPOM and defined its security definitions in this work. Cloud computing is an enigma anyone can get lost in. But just like any other technology, cloud computing is also a double edged sword. On one end lies the promise of lightning fast technology, a huge array of applications to use, seemingly unlimited storage space. On the other end lie various security threats which emerge with shared spaces such as breach of confidentiality, hampering of data integrity and nonavailability of data. In this paper, we have proposed a framework which encrypts a file before it is uploaded on to the cloud. AES (Advanced Encryption Standard) is one of the most secure encryption algorithms and not many attacks are successful on data which is encrypted using AES. This proposal solves the problem of most, if not all, of the threats that data stored in the cloud faces. Our framework also suggests the use of login id and password to ensure authentic and authorized access to a user's data. Thus, if used securely, cloud computing provides a user with amazing benefits and overcomes its only disadvantage of security threat.

FUTURE ENHANCEMENT

The proposed framework can be developed in the form of a mobile application using the various operating systems such as android, iOS, Windows and Symbian. It can also be integrated with any of the social networking sites to exchange data securely in its encrypted form. The algorithm can also be enhanced to not only encrypt text files but also audio and video files.

INTERNSHIP

Request Letter For Internship

1.4.2022
T.N.Palayam

FROM,

Head Of The Department,
Department of Master of Computer Applications,
Jkk Munirajah College of Technology,
T.N.Palayam,
Erode-638506
Tamilnadu.

TO

THE HR,
iROID Technologies,
Coimbatore.

Dear Sir,

On Behalf of JKK Munirajah College of Technology,I wish to request for permission to attend the internship in your company. Our college is reputed at providing quality education in the various courses.

I wish to undertake an internship program for final year students of Master of Computer Applications of JKK Munirajah College of Technology . I believe that your company will give more practical knowledge during this internship program. So kindly allow our students to attend the internship program for 45 days (10.4.2023 T0 24.5.2023)to improve his knowledge and also I attached students detail to this letter.

NAME OF THE STUDENTS:**(MONISHA.S, PERINBARAJ.S, PRADEESHKUMAR.N, SOWMIYA.R)**

Thank you in Advance

Yours faithfully,

Head Of The Department,
Department of Master of Computer Applications,
JKK Munirajah College of Technology,
T.N.Palayam,Erode-638506
Tamilnadu.

PRINCIPAL
JKK MUNIRAJAH COLLEGE
OF TECHNOLOGY
T.N. PALAYAM (Po)-638 506.
GOBI (TK), ERODE (Dt).

Gmail

Internship
1message

Mon 03 April 2023 at 10.00a.m

From: ARCHANA.P<archanap@jkkmct.edu.in>
Date:Mon03April2023at10.00a.m
Subject:Internship-reg
To:iROID Technologies<info@iroidtechnologies.com>

Dear SIR,

I am requesting to be joining your IROID technologies. The requirements are exactly what I have prepared for and hoped to do. I feel confident that I can make a significant contribution to your organization while at the same time learning from your staff.

Additionally, I shall complete all insurance forms for the new intern orientation. I look forward to working with you and your fine team. I appreciate your confidence in me and providing the chance to work with and observe your outstanding staff.

Ref:The following students:

(Monisha.S, Perinbaraj.S, Pradeeshkumar.N, Sowmiya.R)

Sincerely,

Final Year MCA Students,
JKK Munirajah College of Technology,
T.N.Palayam,Erode-638506,Tamilnadu.

PRINCIPAL
JKK MUNIRAJAH COLLEGE
OF TECHNOLOGY
T.N. PALAYAM (Po)-638 506.
GOBI (Tk), ERODE (Dt).

Gmail

Internship
1message

Wed 05 April 2023at11.30p.m

From:iROIDtechonologies<info@iroidtechnologies.com>
Date:Wed05April2022at11.30p.m
Subject:Internship-reg
To:ARCHANA.P<archanap@jkkmct.edu.in>

Dearsir,

I am writing to confirm my acceptance of your internship offer of **10.04.2023 to 24.05.2023**and to tell you how to be joining our **iROID technologies**. The requirements are exactly what I have prepared for and hoped to do. I feel confident that I can make a significant contribution to your organization while at the same time learning from my staff.

As we discussed, I will report at 8:30 a.m. on **APRIL 10, 2023**and will be ready to take on my first assignment as an intern for my company. Additionally, I shall complete all insurance forms for the new intern orientation. I look forward to working with you and your fine team. I appreciate your confidence in me and providing the chance to work with and observe your outstanding staff.

Ref:The following students:

(Monisha.S, Perinbaraj.S,Pradeeshkumar.N, Sowmiya.R)

Sincerely,
Anjana Ayithamattam(MBA)
HR Executive,
iROID Technologies,
2nd floor, Trust Building,
Kayyath Lane Palarivattom,
Cochin-25

PRINCIPAL
JKK MUNIRAJAH COLLEGE
OF TECHNOLOGY
T.N. PALAYAM (Po)-638 506.
GOBI (Tk), ERODE (Dt).

2nd floor,
Trust Building,
Kayyath Lane Palarivattom,
Cochin-25

Anjana Ayithamattam,
HR Executive,
Phone No: +91 8129855155

INDUSTRIAL TRAINING CERTIFICATE

TO WHOM SO EVERIT MAY CONCERN

This is to certify that **Monisha.S**, studying **II-Year** Master of ComputerApplicationsatJ.K.K.MunirajahCollegeofTechnology,T.N.Palayam,Gobi (TK),Erode District-638506 had undergone the Internship program at iROIDTechnologiesduring**10.04.2023to24.05.2023**.

His conduct and character was good during the training period.

Date:24.05.2023

Place:Cochin

For iROIDtechnologies,

PRINCIPAL
JKK MUNIRAJAH COLLEGE
OF TECHNOLOGY
T.N. PALAYAM (Po)-638 506.
GOBI (Tk), ERODE (Dt).

2nd floor,
Trust Building,
Kayyath Lane Palarivattom,
Cochin-25

AnjanaAyithamattam,
HR Executive,
PhoneNo: +91 8129855155

INDUSTRIALTRAININGCERTIFICATE

TO WHOM SO EVERIT MAY CONCERN

This is to certify that **PERINBARAJ.S**, studying **II-Year** Master of Computer Applications at J.K.K.Munirajah College of Technology,T.N.Palayam, Gobi(TK), Erode District-638 506 had undergone the Internship program at iROID Technologies during**10.04.2023to24.05.2023**.

His conduct and character was good during the training period.

Date:24.05.2023

Place:Cochin

For iROIDtechnologies,

PRINCIPAL
JKK MUNIRAJAH COLLEGE
OF TECHNOLOGY
T.N. PALAYAM (Po)-638506.
GOBI (Tk), ERODE (Dt).

2nd floor,
Trust Building,
Kayyath Lane Palarivattom,
Cochin-25

Anjana Ayithamattam,
HR Executive,
PhoneNo: +91 8129855155

INDUSTRIALTRAININGCERTIFICATE

TO WHOM SO EVERIT MAY CONCERN

This is to certify that **PRADEESHKUMAR.N**, studying **II-Year** Master of ComputerApplicationsatJ.K.K.MunirajahCollegeofTechnology,T.N.Palayam,Gobi(TK), Erode District-638 506 had undergone the Internship program at iROID Technologies during**10.04.2023to24.05.2023**.

His conduct and character was good during the training period.

Date:24.05.2023

Place:Cochin

For iROIDtechnologies,

PRINCIPAL
JKK MUNIRAJAH COLLEGE
OF TECHNOLOGY
T.N. PALAYAM (Po)-638 506.
GOBI (Tk), ERODE (Dt).

2nd floor,
Trust Building,
Kayyath Lane Palarivattom,
Cochin-25

AnjanaAyithamattam,
HR Executive,
PhoneNo: +91 8129855155

INDUSTRIALTRAININGCERTIFICATE

TO WHOM SO EVERIT MAY CONCERN

This is to certify that **SOWMIYA.R**, studying **II-Year** Master of ComputerApplicationsatJ.K.K.MunirajahCollegeofTechnology,T.N.Palayam, Gobi(TK), Erode District-638 506 had undergone the Internship program at iROID Technologies during**10.04.2023 to 24.05.2023**.

His conduct and character was good during the training period.

Date:24.05.2023

Place:Cochin

PRINCIPAL
JKK MUNIRAJAH COLLEGE
OF TECHNOLOGY
T.N. PALAYAM (Po)-638 506.
GOBI (Tk), ERODE (Dt).

For iROIDtechnologies,