VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"Jnana Sangama", Belagavi-560014, Karnataka

A PROJECT REPORT ON

"AUTOMATED SMART SYSTEM FOR DETECTING CYBER BOT ATTACKS IN 5G NETWORKS"

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE

BACHELOR OF ENGINEERING
IN
COMPUTER SCIENCE & ENGINEERING

Submitted By

DEEKSHA K	**(1SV19CS025)**
ANUSHA B	**(1SV19CS008)**
ESRA BANU	**(1SV19CS029)**
NAGAKRUPA D R	**(1SV19CS045)**

Under the guidance of

Mr. Shanmukaswamy C V B.E., M.E. MISTE

Associate Professor, Dept. of CSE.
SIET, Tumakuru

SHRIDEVI
EDUCATION

PRINCIPAL
SIET, TUMKUR.

Department of Computer Science and Engineering

SHRIDEVI INSTITUTE OF ENGINEERING AND TECHNOLOGY
(Affiliated To Visvesvaraya Technological University)
Sira Road, Tumakuru – 572 106, Karnataka.
2022-23

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that, the project entitled "AUTOMATED SMART SYSTEM FOR DETECTING CYBER BOT ATTACKS IN 5G NETWORKS" has been successfully carried out by 1. Deeksha K [1SV19CS025], 2. Anusha B [1SV19CS008], 3. Esra Banu [1SV19CS029] and 4. Nagakrupa D R [1SV19CS045], bonafide students of Shridevi Institute of Engineering and Technology, Tumakuru in partial fulfillment for the award of **Bachelor of Engineering** in **Computer Science & Engineering** of the **Visvesvaraya Technological University, Belagavi** during the academic year **2022-23.** It is certified that all the corrections/suggestions indicated for internal assessments have been incorporated in the report. The Project report has been approved as it certifies the academic requirements in respect of project work prescribed for the Bachelor of Engineering Degree.

24/5/23

Signature of Guide
Mr. Shanmukaswamy C V B.E., M.E.,MISTE
Associate Professor,
Dept. of CSE,
SIET, Tumakuru.

Signature of H.O.D
Dr. Basavesha D B.E., MTech.,MISTE ,PhD
Associate Professor & HOD
Dept. of CSE,
SIET, Tumakuru.

Signature of Principal
Dr.Narendra Viswanath M.E., Ph.D., MIE, MISTE, MIWS., FIV.
Principal,
SIET, Tumakuru

PRINCIPAL
S.I.E.T. TUMKUR.

External Viva

Name of the Examiners

1. Dr. Basavesha D
2. Kalasimuddin

Signature with Date

24/5/23.

25/5/23

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

DECLARATION

We, **1. Deeksha K [1SV19CS025], 2. Anusha B [1SV19CS008], 3. Esra Banu [1SV19CS029], and 4. Nagakrupa D R [1SV19CS045],** student of VIII semester **B.E** in Computer Science & Engineering, at Shridevi Institute of Engineering & Technology, Tumakuru, hereby declare that, the project work-II entitled **"AUTOMATED SMART SYSTEM FOR DETECTING CYBER BOT ATTACKS IN 5G NETWORKS"**, embodies the report of our project work carried out by our team under the guidance of **Mr. Shanmukaswamy C V, Associate Professor, Department of CSE**, SIET, Tumakuru as partial fulfillment of requirements for the Project report in **Bachelor of Engineering in Computer Science & Engineering of Visvesvaraya Technological University, Belagavi**, during the academic year **2022-23**. The project has been approved as it satisfies the academic requirements in respect to the Project work.

PRINCIPAL
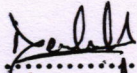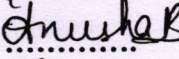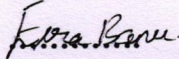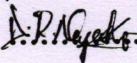S... T. TUMKUR.

Place: Tumakuru

Date: 24 - 05 - 2023

Student Name & Signature

Deeksha K	[1SV19CS025]	
Anusha B	[1SV19CS008]	
Esra Banu	[1SV19CS029]	
Nagakrupa D R	[1SV19CS045]	

Date: 23/05/2023

TO WHOM SO EVER IT MAY CONCERN

This is to certify that **Ms. DEEKSHA K** bearing USN **1SV19CS025** Student of **Shridevi Institute of Engineering and Technology** has successfully completed her Project Work titled "Automated Smart System For Detecting Cyber Bot Attacks In 5G Networks".

We wish every success in her career.

For ShriTEK Innovations

Authorized Signature

PRINCIPAL
SIET. TUMKUR.

Date: 23/05/2023

TO WHOM SO EVER IT MAY CONCERN

This is to certify that **Ms. ANUSHA B** bearing USN **1SV19CS008** Student of **Shridevi Institute of Engineering and Technology** has successfully completed her Project Work titled "Automated Smart System For Detecting Cyber Bot Attacks In 5G Networks".

We wish every success in her career.

For ShriTEK Innovations

Authorized Signature

PRINCIPAL
SIET. TUMKUR.

Date: 23/05/2023

TO WHOM SO EVER IT MAY CONCERN

This is to certify that **Ms. ESRA BANU** bearing USN **1SV19CS029** Student of **Shridevi Institute of Engineering and Technology** has successfully completed her Project Work titled "Automated Smart System For Detecting Cyber Bot Attacks In 5G Networks".

We wish every success in her career.

For ShriTEK Innovations

Authorized Signature

PRINCIPAL
SIET. TUMKUR.

Date: 23/05/2023

TO WHOM SO EVER IT MAY CONCERN

This is to certify that **Ms. NAGAKRUPA D R** bearing USN **1SV19CS045** Student of **Shridevi Institute of Engineering and Technology** has successfully completed her Project Work titled "Automated Smart System For Detecting Cyber Bot Attacks In 5G Networks".

We wish every success in her career.

For ShriTEK Innovations

Authorized Signature

PRINCIPAL
SIET. TUMKUR.

ACKNOWLEDGEMENT

This project work will be incomplete without thanking the personalities responsible for this venture, which otherwise would not have become a reality.

We express our profound gratitude to **Dr. Narendra Viswanath,** Principal, S.I.E.T, for his moral support towards completing our project work.

We would like to thank Head of Department **Dr. Basavesha D.** Head, Department of CSE, SIET for providing all the support and facility.

We would like to thank my guide **Mr. Shanmukaswamy C V, Associate Professor,** Department of Computer Science and Engineering, SIET for his help, sharing his technical expertise and timely advice.

We whole heartedly thank, **Mr. Girish L,** Assistant Professor, Project coordinator, Department of Computer Science and Engineering, for the support

We would like to express our sincere gratitude to all teaching and non-teaching faculty of the department of CSE for guiding us throughout the course of this project by giving valuable suggestion and encouragement.

PRINCIPAL
SIET. TUMKUR.

By,

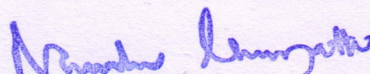|	
Deeksha K	**[1SV19CS025]**
Anusha B	**[1SV19CS008]**
Esra Banu	**[1SV19CS029]**
Nagakrupa D R	**[1SV19CS045]**

ABSTRACT

Today, botnets are the most common threat on the Internet and are used as the main attack vector against individuals and businesses. Cybercriminals have exploited botnets for many illegal activities, including click fraud, DDOS attacks, and spam production. This suggest a method for identifying the behaviour of data traffic using machine learning classifiers including genetic algorithm to detect botnet activities. By categorizing behaviour based on time slots, investigate the viability of detecting botnet behaviour without seeing a whole network data flow. This also evaluate the efficacy of two well-known classification methods with reference to this data. This demonstrate experimentally, using existing datasets, that it is possible to detect botnet activities with high precision.

The computers store data on cloud servers. That working model enables simple access worldwide, which is essential to all online businesses and services. It offers several really beneficial services. Even though the Internet can be beneficial, cybercrime is also on the rise. Information security flaws, identity theft, and other threats might threaten the confidence and reliability of the information. Attackers, also referred to as "Botmasters," disseminate Trojans, malware, or both, increasing the number of existing bots on the network. The attack mechanism of DDOS.

The botnet is a network of robot computers/servers, where an attacker can control and obtain access to the systems without even knowing how it will finish. many different machine learning algorithms have been put forth in the literature to develop various botnet detection models, almost all of these models and techniques are based on extracting features (or feature development), where various feature sets are derived from the available high-dimensional datasets based on some expertise and skills. On the other hand, it is discovered that the literature on botnet detection pays little attention to feature selection, which plays a crucial role in developing various machine learning models.

PRINCIPAL
SIL I. TUMKUR.