Faculty of Engineering and Technology
Project Work - Student Log Book

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

Project ID : G245

Degree/Program	B.Tech	**Specialization**	Computer Science Engineering
Academic Year	2018	**Semester**	8
Course Code	CS1050	**Couse Title**	Major Project

Name	**Register Number**	**Department**	**Mobile Number**	**Email**
Kaumudi Gupta	RA1411003010474	CSE	9087933125	kaumudi_gupta@srmuniv.edu.in
Sumedha Khurana	RA1411003010478	CSE	9940127958	sumedha_khurana@srmuniv.edu.in

Working Title of the Project	Anomaly and Misuse based Network Intrusion Detection System
Project Site and Location	Chennai
Name and address of the company /organisation(Applicable for projects with industry or industry support)	SRM Institute of Science and Technology, Kattankulathur

	Supervisor	**External Supervisor(if applicable)**
Name	MANOJ KUMAR G	
Designation	Assistant Professor (OG)	
Department		
Campus	ktr	
Email	manojkumar.na@ktr.srmuniv.ac.in	
Phone	7418244264	

Mission Statment

Product Description

The use of information and technology by different types of devices generates a large quantity of data packets that contains confidential and personal information. The packets are used to send data over an network. Hackers try to manipulate our data or gain illegal access to the files. Due to this reason, it is necessary to use computer security tools, such as Intrusion Detection Systems (IDS). This work presents an IDS that can perform the packet-based analysis. The flows are organized to be processed by machine learning methods. We design a network intrusion detection system that alarms the admin in case of any kind of intrusion or misuse of data. We are implementing this system using Support vector machine(SVM) algorithm, Weka and Java in various stages to overcome the challenges. Various shortcomings like Misuse of data, port scanning, denial of services will be dealt with in this system. Training data will be used to train the network and perform the testing of the system.

Assumptions and Constraints

We assume that the network is a local area network where the data is collected on a day to day basis.

Stakeholders

Educational Institutions, Non Governmental Organizations, Public sector, Private Companies , MNCs, Hospitals and places where confidential data is stored and they want to protect that data.

Division of Work and Contributors

From Date	To Date	Activities or Components of the project	Register Number of Individual Contributor	Register Number of Joint Contributors
06/08/2017	11/08/2017	Going through various papers in order to select the most viable topic for the major project. We went through several IEEE conference and transaction papers in order to understand the topic under discussion and to formulate how we would go about this project. We established the fact that security is one of the major concerns these days hence, we decided to take up this project.	RA1411003010478	RA1411003010474
20/08/2017	01/09/2017	Formulation of the basic strategy of we are going to go about the project and preparation of the PPT for the zeroth review.	RA1411003010478	RA1411003010474
09/09/2017	15/09/2017	Updation of the PPT to incorporate some changes suggested by the supervisor regarding the format of the presentation and addition of three new slides.	RA1411003010478	RA1411003010474
01/12/2017	31/12/2017	Worked on the initial module of the project and gathered the data sets required. We surfed through the web to obtain real-time data sets and acquired the KDD Cup99 data sets.	RA1411003010474	RA1411003010478
01/01/2018	14/01/2018	We prepared for the first review. We wrote the literature survey , came up with the architecture diagram, made a presentation about our project.	RA1411003010474	RA1411003010478
14/01/2018	1/02/2018	We wrote the code in Java for initial data processing and used weka tool to filter out the useless attributes in our data set.	RA1411003010474	RA1411003010478
02/02/2018	18/02/2018	We wrote our research paper which we presented at the conference and then, submitted it for the publication.	RA1411003010474	RA1411003010478
03/02/2018	22/02/2018	We completed approximately 70		

Summary record of major progress meetings with supervisors

Meeting Date	Progress since Last Meeting	Outcome of Meeting	Target Date	Other Issues	Next Meeting
10/10/2017	Modifications in the topic and base paper	IEEE conference base paper was asked to be changed	14/10/2017		15/10/2017
15/10/2017	IEEE transaction paper from the year 2017 was chosen and title of the project was updated	IEEE transaction paper was accepted.	20/10/2017		21/10/2017
21/10/2017	A powerpoint presentation was prepared depicting the idea and the abstract.	Some changes were recommended by the guide like format of the PPT	25/10/2017		09/11/2017
09/11/2017	Changes recommended in the ppt were made.	The PPT was verified by the supervisor and given a green signal.	13/11/2017		13/11/2017
13/11/2017	We were ready with our abstract and PPT to present it in front of the panel.	Zeroth review was conducted.	05/01/2018		06/01/2018
06/01/2018	We developed the initial model by collecting the required data set and studying the base thoroughly.	The viability of the project was evaluated. The supervisor also made sure the viability of the project was evaluated. The supervisor also made sure that we were able to apply what we had in our mind.	10/01/2018		13/01/2018
13/01/2018	We were ready to display our initial model for the first review.	First review was conducted.	14/01/2018		05/02/2018

Meeting Date	**Progress since Last Meeting**	**Outcome of Meeting**	**Target Date**	**Other Issues**	**Next Meeting**
05/02/2018	We started writing our research paper and submitted the abstract for the research day publication.	We were appreciated and encouraged for further work.	11/02/2018		15/02/2018
15/02/2018	We finished writing the paper and submitted it for the publication	Some changes were suggested by the guide and we immediately worked on it.	20/02/2018		22/02/2018
22/02/2018	Our paper was selected for research day .	We were asked to prepare for second review	23/02/2018		23/02/2018
23/02/2018	We were ready to showcase the progress on our project where in we planned to implement SVM for the process of detection.	The panel liked our idea, however recommended some changes in order to obtain distinct results.	23/02/2018		15/03/2018
15/03/2018	We presented our paper at NCBCS conference which was held in SRM.	Our paper was selected for the publication.	28/03/2018		02/04/2018

Worksheet / Data collection / Observation etc

Worksheet/ Data Collection / Observation etc
Our survey data was collected from UCI respository. The dataset is known as KDD-CUP99. The raw training data was about four gigabytes of compressed binary TCP dump data from seven weeks of network traffic. This was processed into about five million connection records.
We further processed the data by using weka tool and wrote the code in Java for the same.
Accuracy of about 98.79

Faculty of Engineering and Technology
Project Work - Student Log Book

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

Zeroth Review

Register Number : RA1411003010474

Reviewer Name	**Specific Comment**	**General Comment**	**Presentation(10)**	**Viva(10)**	**Total(20)**
				Average	

Faculty of Engineering and Technology
Project Work - Student Log Book

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

Zeroth Review

Register Number : RA1411003010478

Reviewer Name	**Specific Comment**	**General Comment**	**Presentation(10)**	**Viva(10)**	**Total(20)**
				Average	

Review I

Register Number : RA1411003010474

Reviewer Name	**Specific Comment**	**General Comment**	**Literature Survey(10)**	**Architecture Diagram(5)**	**Demo(15)**	**Total(30)**
					Average	

Faculty of Engineering and Technology
Project Work - Student Log Book

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

Review I

Register Number : RA1411003010478

Reviewer Name	Specific Comment	General Comment	Literature Survey(10)	Architecture Diagram(5)	Demo(15)	Total(30)
					Average	

Faculty of Engineering and Technology
Project Work - Student Log Book

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

Review II

Register Number : RA1411003010474

Reviewer Name	**Specific Comment**	**General Comment**	**Presentation(10)**	**Algorithm(20)**	**Demo(20)**	**Total(50)**
					Average	

Faculty of Engineering and Technology
Project Work - Student Log Book

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

Review II

Register Number : RA1411003010478

Reviewer Name	**Specific Comment**	**General Comment**	**Presentation(10)**	**Algorithm(20)**	**Demo(20)**	**Total(50)**
					Average	

Faculty of Engineering and Technology
Project Work - Student Log Book

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

Final Review

Register Number : RA1411003010474

Reviewer Name	**Specific Comment**	**General Comment**	**Presentation (10)**	**Outcome (10)**	**Demo (25)**	**Project Diary (20)**	**Journal Publication (30)**	**Total (50)**
							Average	

Final Review

Register Number : RA1411003010478

Reviewer Name	Specific Comment	General Comment	Presentation (10)	Outcome (10)	Demo (25)	Project Diary (20)	Journal Publication (30)	Total (50)
							Average	