# Security Solutions

# SOFTWARE ENGINEERING AND PROJECT MANAGEMENT FOR SECURITY SOLUTIONS

# ABSTRACT

Our cybersecurity software is a comprehensive solution designed to protect your computer systems and networks from cyber threats. Using advanced techniques such as machine learning and behavioral analysis, our software detects and blocks various types of malware, including viruses, trojans, and ransomware.

In addition to preventing attacks, our software also provides real-time monitoring of network activity, identifying any unusual behavior and notifying the user immediately. The software includes a centralized dashboard that allows the user to manage and configure security settings for multiple devices and networks.Our software is easy to install and user-friendly, with a minimal impact on system performance. Regular updates ensure that the software is always up-to-date with the latest threats, providing reliable protection against emerging risks.

Overall, our cybersecurity software offers a robust and reliable solution for protecting your systems and data from cyber attacks, giving you peace of mind in an increasingly digital world.

Our cybersecurity software is a powerful tool that helps businesses and organizations protect their sensitive information and assets from cyber attacks. Using a combination of advanced threat detection technologies and behavioral analytics, our software monitors network activity in real-time, identifying and responding to potential threats before they can cause harm.

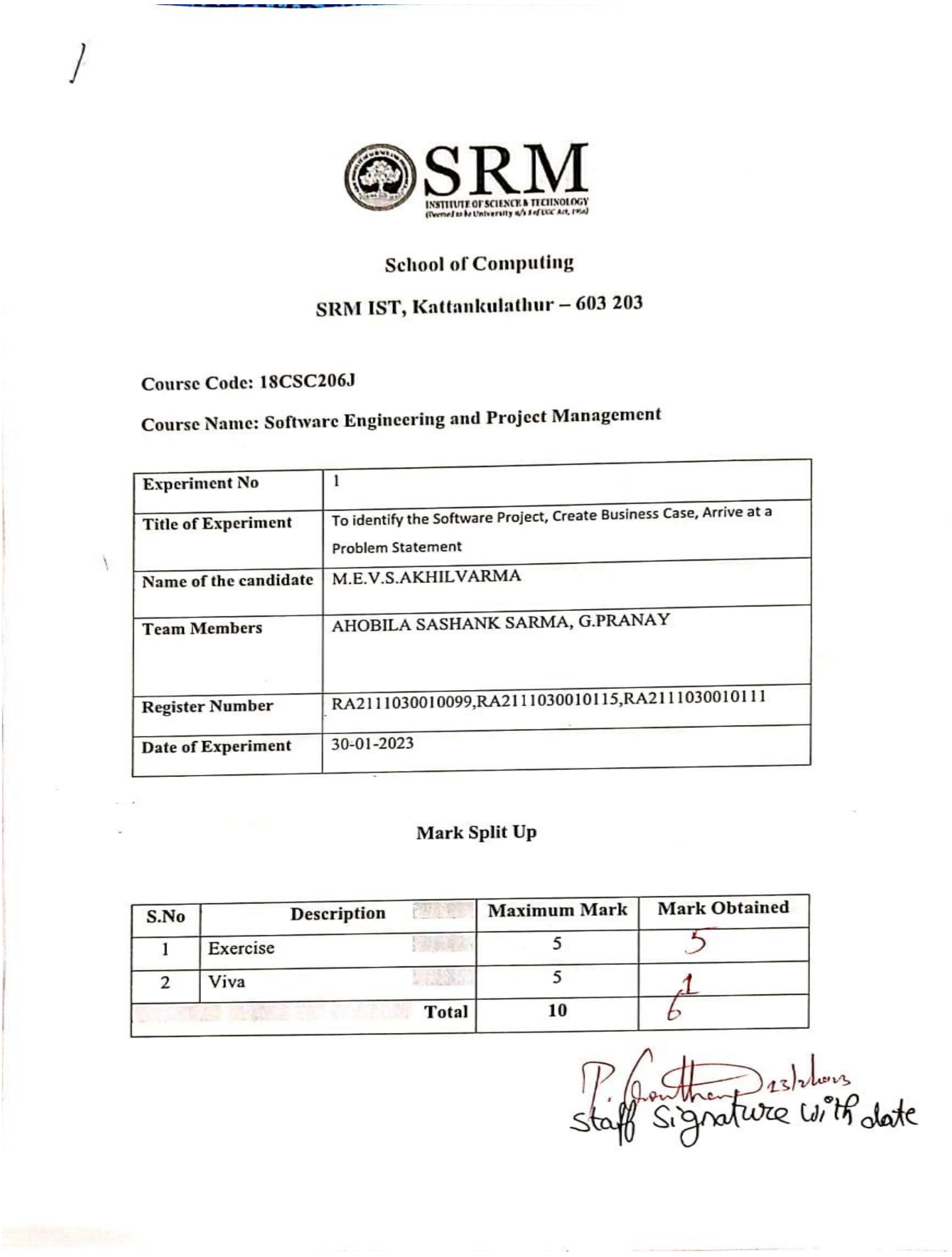
Our software is designed to be flexible and scalable, allowing businesses of all sizes to customize their security settings to meet their unique needs. Whether it's protecting against phishing scams, ransomware attacks, or other forms of cybercrime, our software provides comprehensive protection across all endpoints, including desktops, laptops, mobile devices, and servers.

## TABLE OF CONTENTS

## LIST OF FIGURES

## LIST OF ABBREVIATIONS

1)SWOT- strengths, weaknesses, opportunities, and threats
2)PCI DSS- Payment Card Industry Data Security Standard
3)HIPAA- Health Insurance Portability And Accountability Act
4)HTML- Hyper Text Markup Language
5)CSS- Cascading Styling Sheets
6)PHP -Hypertext Preprocessor



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

**School of Computing**

**SRM IST, Kattankulathur – 603 203**

**Course Code: 18CSC206J**

**Course Name: Software Engineering and Project Management**

| | |
|---|---|
| **Experiment No** | 1 |
| **Title of Experiment** | To identify the Software Project, Create Business Case, Arrive at a Problem Statement |
| **Name of the candidate** | M.E.V.S.AKHILVARMA |
| **Team Members** | AHOBILA SASHANK SARMA, G.PRANAY |
| **Register Number** | RA2111030010099,RA2111030010115,RA2111030010111 |
| **Date of Experiment** | 30-01-2023 |

**Mark Split Up**

| S.No | Description | Maximum Mark | Mark Obtained |
|---|---|---|---|
| 1 | Exercise | 5 | 5 |
| 2 | Viva | 5 | 1 |
| | **Total** | 10 | 6 |

P. Gowthaman 13/2/2023
Staff Signature with date

## Aim

To Frame a project team, analyze and identify a Software project. To create a business case and Arrive at a Problem Statement for the <title of the project>

## Team Members:

| S. No | Register No | Name | Role |
|---|---|---|---|
| 1 | RA2111030010111 | AHOBILA SASHANK SARMA | Lead/Rep |
| 2 | RA2111030010115 | G.PRANAY | Member |
| 3 | RA2111030010099 | MANTHENA ESWAR VENKATA SATYA AKHIL VERMA | Member |

**Project Title:** To identify the Software Project, Create Business Case, Arrive at a Problem Statement

## Project Description

- The main goal of the security solutions limited is to find the vulnerabilities and fix those vulnerabilities in the company's software and to give the security to the companies from hackers.
- The main challenge is to give the guarantee that we will hundred percent security to companies because in india there are so many hackers who steal the company's data and the main challenge is the company should trust our team that we will give the hundred percent assurance that we will secure their software for that we should show our skills and capabilities to the companies.

Business Case: Security solutions limited

# ONE PAGE BUSINESS CASE TEMPLATE

| | |
|---|---|
| **DATE** | 30-01-2023 |
| **SUBMITTED BY** | AHOBILA SASHANK SARMA, G.PRANAY, MANTHENA<br>ESWAR VENKATA SATYA AHKIL VERMA |
| **TITLE / ROLE** | SECURITY SOLUTIONS LIMITED |

LOG

## THE PROJECT

This project aims to solve the vulnerabilities of the software and the servers. The vulnerabilities are the main cause of hacking. If the hackers finds any vulnerabilities he is able to hack the software with that vulnerabilities. This project goal is give the security to the hacker. The strong firewall should be their to prevent hacking from the hackers and we will develop the strong firewall to prevent the hacking from the hackers.

## THE HISTORY

So many companies are facing the issues to protect their software and data from the companies. It's more important to the company to protect their data. India is in top five in the world that there are so many cyber crimes happening in India and there are so many hackers in India. There so much need for the companies to protect their data, software and servers. The situation is very worse in our country there are so many cyber crimes happened in India.

## LIMITATIONS

For this project we need to give the special training to the employees and it will cost little expensive but not that much expensive. For this project the employee should work complete 24 hours because hacker can attack any time for that case it will cost little expensive the more employees should be there. We need high professionals for this kind of the project to build the firewall. If any employee have lack of skills he should not appointed in this project.

## APPROACH

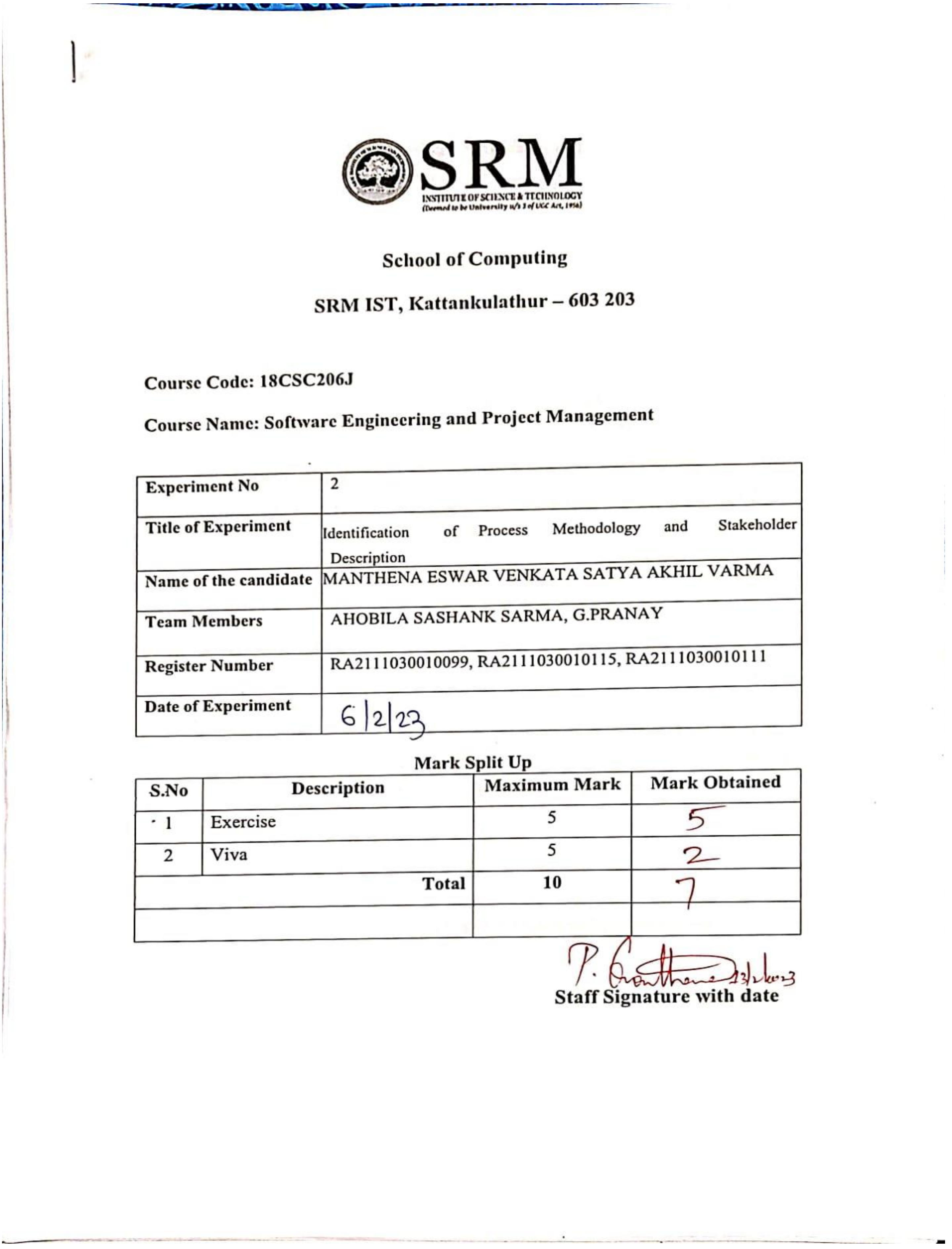
To complete this Project we need high professional employees. First of all the company should trust our skills and capabilities. We should clear all kind of vulnerabilities because even the small vulnerability can hack the entire system. We should clear all kind of vulnerabilities in the short time because the delay of the time can cause many problems in the software. The company should be ready to give the good pay to the employees because it more important to protect their data

## BENEFITS

The benefits this project to the company is their software and data will be 100 percent secured and there are no vulnerabilities in the software and the company is secured from the hackers and it will done in less expensive when compared to other projects.

Result

Thus, the project team formed, the project is described, the business case was prepared and the problem statement was arrived.



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

**School of Computing**

**SRM IST, Kattankulathur – 603 203**

**Course Code: 18CSC206J**

**Course Name: Software Engineering and Project Management**

| | |
|---|---|
| **Experiment No** | 2 |
| **Title of Experiment** | Identification of Process Methodology and Stakeholder Description |
| **Name of the candidate** | MANTHENA ESWAR VENKATA SATYA AKHIL VARMA |
| **Team Members** | AHOBILA SASHANK SARMA, G.PRANAY |
| **Register Number** | RA2111030010099, RA2111030010115, RA2111030010111 |
| **Date of Experiment** | 6/2/23 |

**Mark Split Up**

| **S.No** | **Description** | **Maximum Mark** | **Mark Obtained** |
|---|---|---|---|
| 1 | Exercise | 5 | 5 |
| 2 | Viva | 5 | 2 |
| | **Total** | **10** | 7 |
| | | | |

13/2/2023

**Staff Signature with date**

Aim

To identify the appropriate Process Model for the project and prepare Stakeholder and User Description.

Team Members:

| Sl No | Register No | Name | Role |
|---|---|---|---|
| **1** | **RA2111030010111** | **AHOBILA SASHANK SARMA** | **Rep/Member** |
| **2** | **RA2111030010115** | **G.PRANAY** | **Member** |
| **3** | **RA2111030010099** | **MANTHENA ESWAR VENKATA SATYA AKHIL VERMA** | **Member** |

**Project Title: SECURITY SOLUTIONS**

**Selection of Methodology**

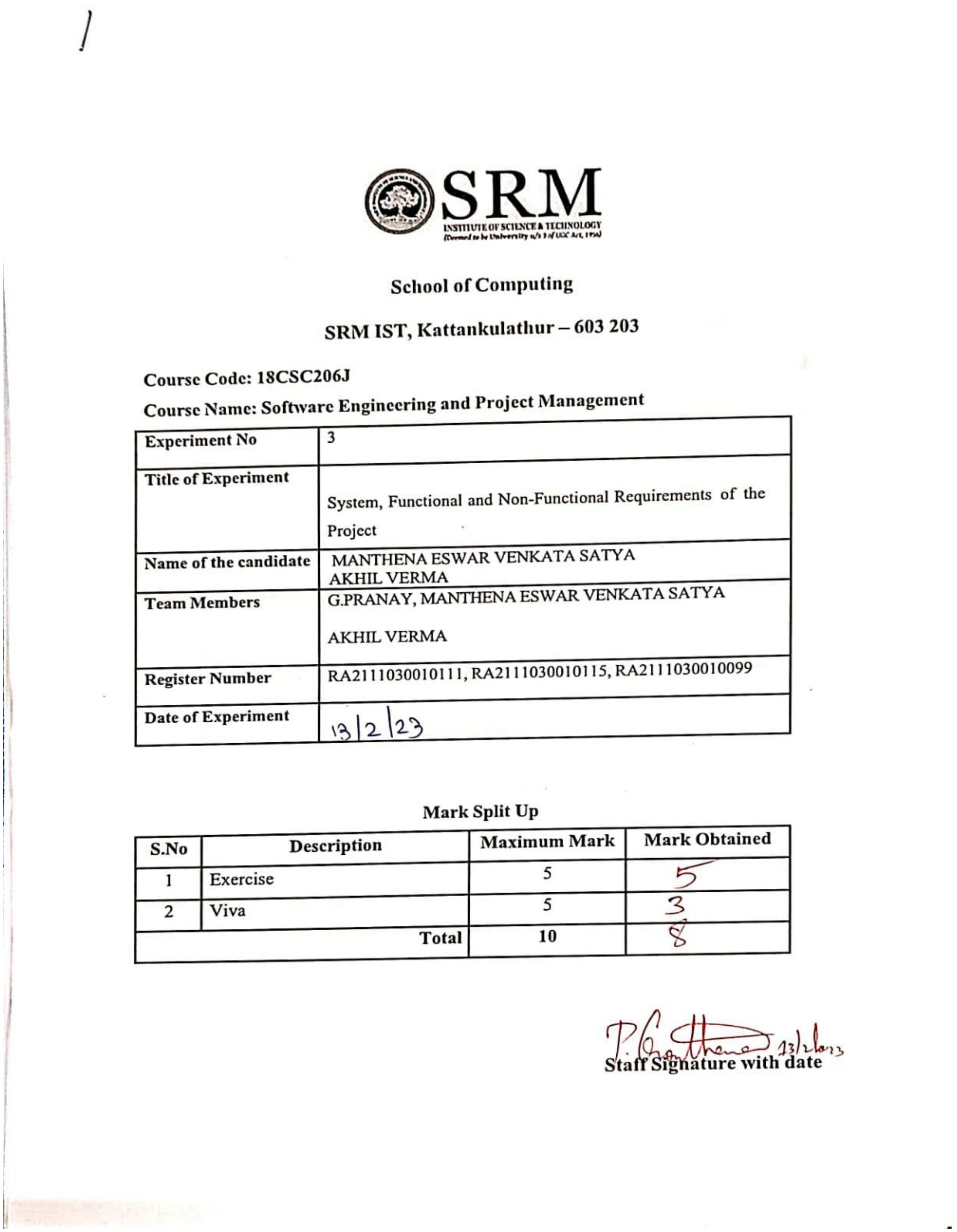
- For this project we select agile methodology because this methodology helps us to involves constant collaboration with stake holders because this project should be update constantly and it needs constant collaboration stake holders then only this project will be successful and in this methodology we can change the plan and design by the review of the customers and to launch the new updates to project.

Incorporate information to below table regarding stakeholders ofthe project [Make useof below examples

| Stakeholder Name | Activity/ Area /Phase | Interest | Influence | Priority (High/ Medium/ Low) |
|---|---|---|---|---|
| OWNER | To achieve goals and to increase the sales | HIGH | HIGH | 1 |
| INVESTORS | To provide the financial resources | MED | HIGH | 1 |
| SPONSOR | To provide the new technology to the world and funding to the project | MED | HIGH | 2 |
| EMPLOYEES | To develop the project and to achieve the goal | HIGH | HIGH | 3 |
| PROJECT MANAGER | To lead the project in a correct way to complete the project in particular time | MED | HIGH | 3 |
| CUSTOMERS | Provides feedback | HIGH | MED | 3 |
| RESOURCE MANAGER | To get the resources to the project on time | LOW | MED | 4 |
| SUPPLIERS | To manage the budget and to convince the customers | LOW | MED | 4 |
| SALES AND MARKETING HEAD | To sale the project to the customers and to create the interest in the project to the customers | MED | HIGH | 5 |

Result

Thus the Project Methodology was identified and the stakeholders were described.



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

### School of Computing

### SRM IST, Kattankulathur – 603 203

**Course Code: 18CSC206J**

**Course Name: Software Engineering and Project Management**

| | |
|---|---|
| **Experiment No** | 3 |
| **Title of Experiment** | System, Functional and Non-Functional Requirements of the Project |
| **Name of the candidate** | MANTHENA ESWAR VENKATA SATYA<br>AKHIL VERMA |
| **Team Members** | G.PRANAY, MANTHENA ESWAR VENKATA SATYA<br>AKHIL VERMA |
| **Register Number** | RA2111030010111, RA2111030010115, RA2111030010099 |
| **Date of Experiment** | 13/2/23 |

**Mark Split Up**

| S.No | Description | Maximum Mark | Mark Obtained |
|---|---|---|---|
| 1 | Exercise | 5 | 5 |
| 2 | Viva | 5 | 3 |
| | **Total** | **10** | 8 |

13/2/2023
**Staff Signature with date**

**Aim:**

To identify the system, functional and non-functional requirements for the project.

**Team Members:**

| S No | Register No | Name | Role |
|---|---|---|---|
| 1 | RA2111030010111 | AHOBILA SASHANK SARMA | Rep/Member |
| 2 | RA2111030010115 | G.PRANAY | Member |
| 3 | RA2111030010099 | MANTHENA ESWAR VENKATA SATYAAKHIL VERMA | Member |

**Project Title: Security solutions**

**System Requirements:**

- Microsoft Windows 11, 10, 8.1 fully patched (32- and 64-bit). Windows Enterprisenot supported.
- Build 4.11.1 or higher: macOS 10.15 and above
- Build 4.9.1: macOS 10.12 - 10.14
- Google Android smartphones and tablets 8 or higher
- Apple iOS 13 or later
- ChromeOS 102.0.5005 and higher
- 2 GB RAM
- 1.3 GB free drive space
- 1 GHz Processor. Architecture for Windows: x64, x86. Architecture for Mac: x64,x86, ARM64 (Rosetta II required)

**Functional Requirements:**

1. Threat detection and prevention: The company should provide security solutions that can detect and prevent various types of security threats, such as malware, viruses, phishing attacks, and unauthorized access.

2. Security monitoring and reporting: The company should provide real-time security monitoring and reporting tools to help customers identify and respond to potential threats.

3. Access control and identity management: The company should provide tools and solutions for access control and identity management, including password management, multi-factor authentication, and role-based access control.

4. Data encryption and protection: The company should provide solutions for data encryption and protection, to ensure that sensitive customer data is secure and confidential.

5. Incident response and recovery: The company should have a clear and effective incident response plan, with tools and resources for incident management and recovery.

6. Security consultation and training: The company should provide consultation and training services to help customers understand and manage their security risks.

7. Integration with third-party systems: The company's security solutions should be able to integrate with a wide range of third-party systems and tools, to ensure that customers can easily manage their security infrastructure.

**Non-Functional Requirements:**

1. Security: The company should have a robust and secure infrastructure, with appropriate security measures in place to protect against potential threats, such as hacking, data breaches, and physical security breaches.

2. Reliability: The company should provide a highly reliable service, with minimal downtime, to ensure that customers have constant access to their security services.

3. Performance: The company's security solutions should be optimized for fast processing and low latency, to provide real-time protection against threats.

4. Scalability: The company should be able to handle a large number of customers and requests without compromising on its performance or security.

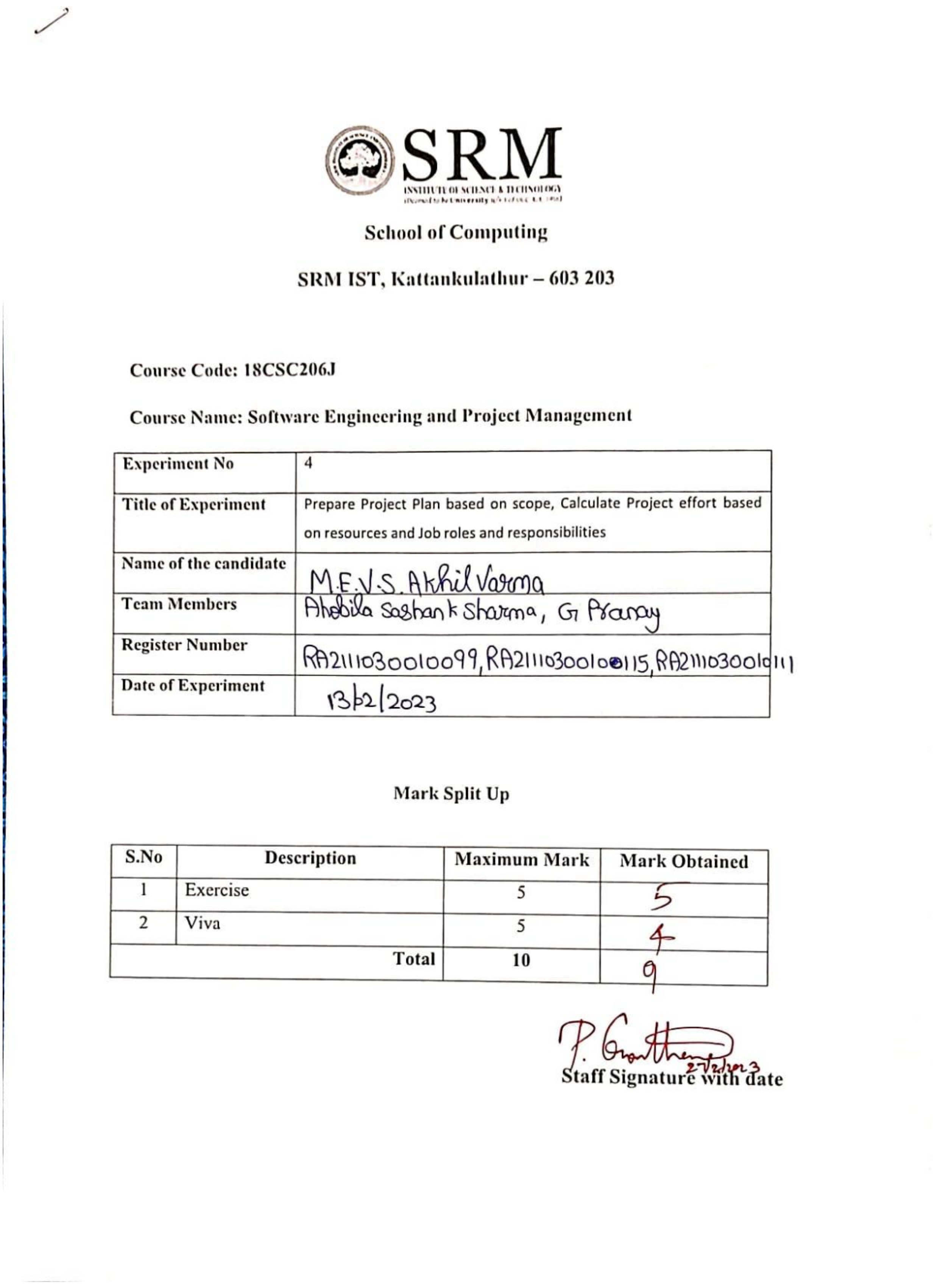
5. Compliance: The company should adhere to relevant regulations and standards, such as GDPR, HIPAA, or PCI-DSS, to ensure that customer data is secure and confidential.

6. Usability: The company's security solutions should be user-friendly, with clear and simple interfaces, to ensure that customers can easily use and understand them.

7. Interoperability: The company's security solutions should be able to integrate with a wide range of third-party systems and tools, to ensure that customers can easily manage their security infrastructure.

**Result:**

**Thus the requirements were identified and accordingly describe**



SRM
INSTITUTE OF SCIENCE & TECHNOLOGY

**School of Computing**

**SRM IST, Kattankulathur – 603 203**

**Course Code: 18CSC206J**

**Course Name: Software Engineering and Project Management**

| | |
|---|---|
| **Experiment No** | 4 |
| **Title of Experiment** | Prepare Project Plan based on scope, Calculate Project effort based on resources and Job roles and responsibilities |
| **Name of the candidate** | M.E.V.S. Akhil Varma |
| **Team Members** | Ahobila Sashank Sharma, G Pranay |
| **Register Number** | RA2111030010099, RA2111030010115, RA2111030010111 |
| **Date of Experiment** | 13/02/2023 |

**Mark Split Up**

| S.No | Description | Maximum Mark | Mark Obtained |
|---|---|---|---|
| 1 | Exercise | 5 | 5 |
| 2 | Viva | 5 | 4 |
| | **Total** | **10** | 9 |

27/2/2023
**Staff Signature with date**

## Aim

To Prepare Project Plan based on scope, Calculate Project effort based on resources, Find Job roles and responsibilities

**Team Members:**

| Sl No | Register No | Name | Role |
|---|---|---|---|
| 1 | RA2111030010111 | Ahobila Sashank Sarma | Lead |
| 2 | RA2111030010115 | G Pranay | Member |
| 3 | RA2111030010099 | Manthena Eswara Venkata Satya Akhil Varma | Member |

## 1. Project Management Plan

| FOCUS | DETAILS |
|---|---|
| Stakeholder | Identifying, Analyzing, Engaging stakeholders |
| Communication Management | Determine communication requirements, roles and responsibilities, tools and techniques. |
| Risk Management | Identifying, analysing, and prioritizing project risks |

1) Stakeholder:

| Stakeholder | Description | Engagement Strategy |
|---|---|---|
| Clients | Those who require security servicesRegularly | communicate and collaborate with clients to identify and address their specific security needs |
| Employees | Security personnel and support staff | Provide ongoing training and professional development opportunities, offer competitive salaries and benefits, and encourage open communication and feedback |

| | | |
|---|---|---|
| Suppliers | Vendors who provide equipment and other supplies | Establish and maintain strong relationships with suppliers, negotiate favorable pricing and terms, and ensure timely and reliable delivery of goods and services |
| Regulators | Government agencies responsible for regulating the security industry | Stay informed of regulatory requirements and compliance standards, proactively address any compliance issues, and participate in relevant industry associations and groups |
| Investors | Those who invest in the company | Communicate regularly with investors to provide updates on company performance and future plans, and actively seek their input and feedback |
| Community | The local community in which the company operates | Be a good corporate citizen by supporting local causes and charities, engaging in environmentally responsible practices, and promoting a positive public image |

2) Communication Management:

| Audience | Purpose | Message | Delivery Method | Frequency |
|---|---|---|---|---|
| Clients | Keep clients informed about security issues and updates | Regularly communicate with clients to provide updates on security measures and address any concerns or issues | Email, phone, in-person meetings | As needed or on a regular basis |
| Employees | Keep employees informed about company policies and procedures, training, and other relevant information | Regularly communicate with employees to provide updates on company policies and procedures, training opportunities, and other relevant information | Email, team meetings, internal newsletters | As needed or on a regular basis |

| | | | | |
|---|---|---|---|---|
| Investors | Keep investors informed about company performance and future plans | Regularly communicate with investors to provide updates on company performance and future plans, and address any questions or concerns | Investor calls, email, investor presentations | Quarterly or semi-annually |
| Community | Keep the local community informed about company activities and initiatives | Regularly communicate with the local community to provide updates on company activities and initiatives, and address any questions or concerns | Press releases, social media, community events | As needed or on a regular basis |

3) Risk Management :

| Risk Category | Risk Description | Likelihood of Occurrence | Impact on Business | Mitigation Strategy |
|---|---|---|---|---|
| Employee Turnover | High employee turnover rate due to low job satisfaction | Medium | High | Increase employee engagement through training and recognition programs |
| Security Breach | Unauthorized access to client data | Low | High | Implement strict access controls and regularly update security protocols |
| Workplace Accidents | Workplace accidents resulting in employee injury or property damage | High | Medium | Conduct regular safety audits and provide ongoing safety training |
| Natural Disasters | Disruption of operations due to natural disasters such as floods, fires, or earthquakes | Low | High | Develop and implement a comprehensive disaster recovery plan |

# 2. Estimation

## 2.1. Effort and Cost Estimation

| PROJECT | TASKS | EFFORT (IN HOURS ) | HOURLY RATE (INR) | COST |
|---|---|---|---|---|
| Security Assessment | Conduct security assessment of client premises | 50 | 2,000 | 1,00,000 |
| Security Training | Develop and deliver security training for client employees | 100 | 1500 | 1,50,000 |
| Security System Installation | Install and configure security systems at client premises | 200 | 1,000 | 2,00,000 |
| Security Monitoring | Provide ongoing security monitoring services | 500 | 300 | 1,50,000 |
| Security – | Provide security consulting services to clients | 150 | 1,500 | 2,25,000 |
| TOTAL | | 1,000 | | 825,000 |

## 2.2. Infrastructure/Resource Cost [CapEx]

| Description | Description | Cost |
|---|---|---|

| | | |
|---|---|---|
| Security Team | Regular maintenance and repair of security equipment, such as cameras, alarms, and access control systems | Annual maintenance contract costs or hourly service costs, which vary based on the type and number of equipment. For example: Cameras (1200 - 1500 per year), Access Control Systems (1500 - 2,000 per year), Alarms (3300 - 7700 per year) |
| Security Equipment | Regular maintenance and upgrades of security software, such as surveillance software, access control software, and incident management software | Annual maintenance contract costs or hourly service costs, which vary based on the type and number of software licenses. For example: Surveillance Software (5500 - 1,500 per year), Access Control Software (3300 - 8800 per year), Incident Management Software (5000 - 9,500 per year) |
| Security Software | Ongoing training and professional development for security personnel, including certification programs and continuing education courses | Training program costs and associated travel expenses. For example: Certified Protection Professional (CPP) program (1,000 - 2,000 per person), Security Awareness Training (50 - 100 per person), Security Management Training (500 - 1,000 per person) |
| Office Space | Salaries and benefits for support staff, such as administrative assistants and technical support personnel | Salaries and benefits costs, which vary based on level of experience, expertise, and location. For example: Administrative Assistant (25,000 - 550,000 per year), Technical Support Specialist (40,000 - 80,000 per year) |

## 2.3. Maintenance and Support Cost [OpEx]

| Resource | Description | Cost |
|---|---|---|

| | | |
|---|---|---|
| Equipment Maintenance | Regular maintenance and repair of security equipment, such as cameras, alarms, and access control systems | Annual maintenance contract costs or hourly service costs, which vary based on the type and number of equipment. For example: Cameras (20000 - 500000 per year), Access Control Systems (5000 - 10,000 per year), Alarms (3000 - 7000 per year) |
| Software Maintenance | Regular maintenance and upgrades of security software, such as surveillance software, access control software, and incident management software | Annual maintenance contract costs or hourly service costs, which vary based on the type and number of software licenses. For example: Surveillance Software (5000 – 15,000 per year), Access Control Software (3300 - 8000 per year), Incident Management Software (5000 – 15,000 per year) |
| Personnel Training | Ongoing training and professional development for security personnel, including certification programs and continuing education courses | Training program costs and associated travel expenses. For example: Certified Protection Professional (CPP) program (10,000 - 20,000 per person), Security Awareness Training (500 - 1100 per person), Security Management Training (5000 - 1,000 per person) |
| Support Staff | Salaries and benefits for support staff, such as administrative assistants and technical support personnel | Salaries and benefits costs, which vary based on level of experience, expertise, and location. For example: Administrative Assistant (25,000 - 450,000 per year), Technical Support Specialist ($40,000 - $80,000 per year) |

# 3. Project Team Formation

## 3.1. Identification Team members

| Task | Security Officer | Security Manager | Security Director | Chief Security Officer |
|---|---|---|---|---|
| Develop Security Policies and Procedures | R | A | I | C |
| Conduct Security Risk Assessments | R | A | I | C |
| Develop and Implement Security Plans | A | R | I | C |
| Conduct Security Training and Awareness Programs | A | R | I | C |
| Manage Security Personnel and Operations |  | A | R | C |
| Manage Security Budget and Resources |  | A | R | C |
| Oversee Security Compliance and Regulatory Requirements |  |  | A | C |

| Name | Role | Responsibilities |
|---|---|---|
| A Sashank | Key Business User, Technical Lead | Provide clear business and user requirements<br>Design the end-to-end architecture |

| | | |
|---|---|---|
| G Pranay | Security Operations, Penetration Tester | Provision required Services<br>Define Test Cases and Perform Testing |
| M Akhil varma | Security Architect, Business Analyst | Design the cost effective, highly available and scalable architecture<br>Discuss and Document Requirements |

## 3.2 Responsibility Assignment Matrix

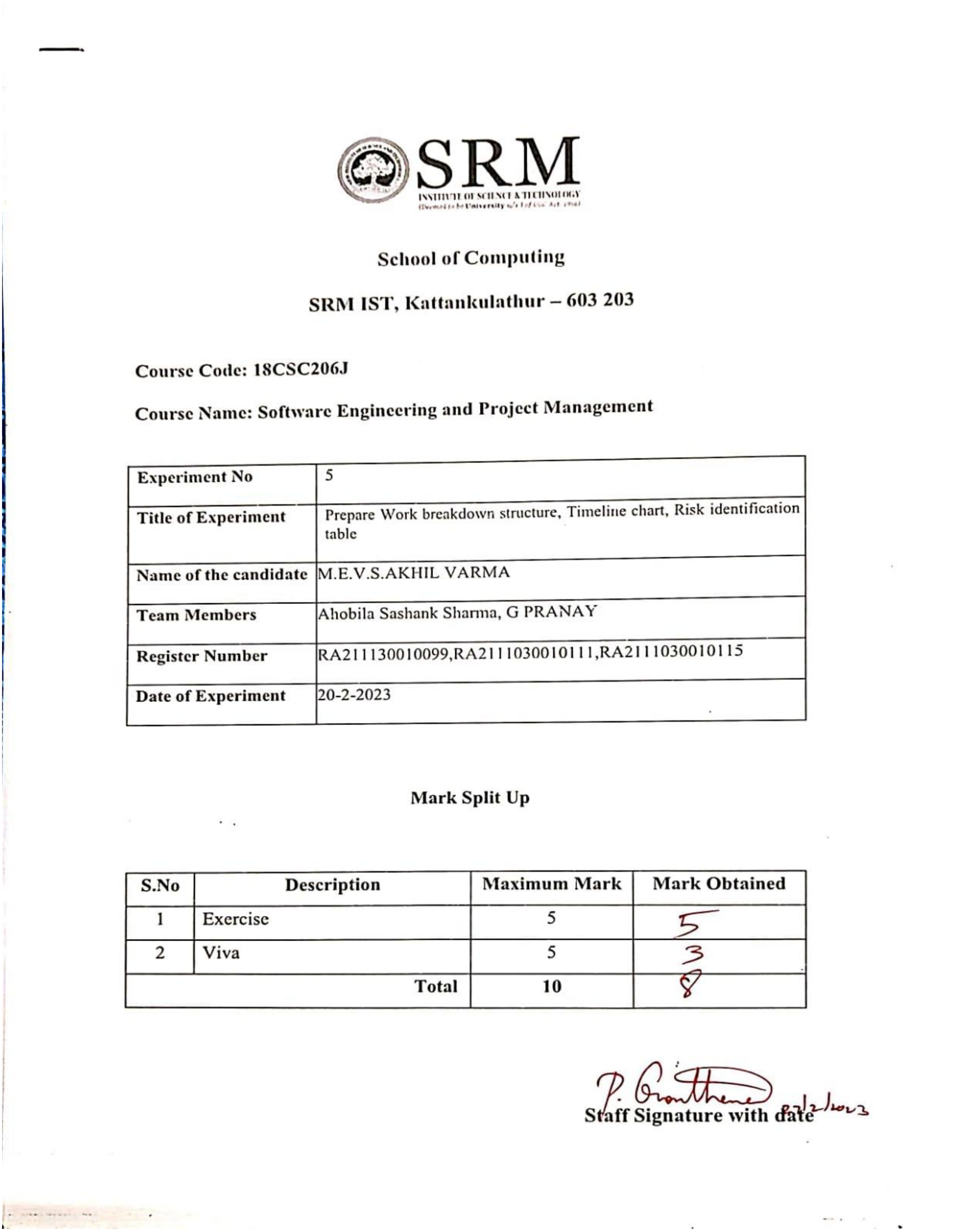
| | |
|---|---|
| A | Accountable |
| R | Responsible |
| C | Consult |
| I | Inform |

## Reference

1. https://www.pmi.org/
2. https://www.projectmanagement.com/
3. https://www.tpsgc-pwgsc.gc.ca/biens-property/sngp-npms/ti-it/ervcpgpm-dsfvpmpt-eng.html

## Result:

Thus, the Project Plan was documented successfully.



School of Computing

SRM IST, Kattankulathur – 603 203

**Course Code: 18CSC206J**

**Course Name: Software Engineering and Project Management**

| | |
|---|---|
| **Experiment No** | 5 |
| **Title of Experiment** | Prepare Work breakdown structure, Timeline chart, Risk identification table |
| **Name of the candidate** | M.E.V.S.AKHIL VARMA |
| **Team Members** | Ahobila Sashank Sharma, G PRANAY |
| **Register Number** | RA211130010099,RA2111030010111,RA2111030010115 |
| **Date of Experiment** | 20-2-2023 |

**Mark Split Up**

| S.No | Description | Maximum Mark | Mark Obtained |
|---|---|---|---|
| 1 | Exercise | 5 | 5 |
| 2 | Viva | 5 | 3 |
| | **Total** | **10** | 8 |

P. Gowthame 27/2/2023

**Staff Signature with date**

**Aim**

To Prepare Work breakdown structure, Timeline chart and Risk identification table

**Team Members:**

| Sl No | Register No | Name | Role |
|---|---|---|---|
| **1** | RA2111030010111 | Sashank | **Rep** |
| **2** | RA2111030010115 | Pranay | **Member** |
| **3** | RA2111030010099 | Akhil | **Member** |

**Work Breakdown Structure:**

1.Project Planning and Initiation

1.1 Define project objectives and scope

1.2 Conduct stakeholder analysis

1.3 Develop project charter

1.4 Define project management plan

1.5 Obtain project funding

2.Security Assessment and Planning

2.1 Conduct threat and risk assessments

2.2 Develop security policies and procedures

2.3 Design physical and technical security systems

2.4 Develop emergency response and incident management plans

2.5 Conduct security audits

3.Security Operations

3.1 Security personnel recruitment and training

3.2 Security equipment procurement and maintenance

3.3 Security system installation and configuration

3.4 Security monitoring and surveillance

3.5 Response to security incidents

4.Security Consulting Services

4.1 Conduct security assessments and audits for clients

4.2 Develop security policies and procedures for clients

4.3 Design security systems for clients

4.4 Provide security training for clients

5.Project Management

5.1 Project schedule development and management

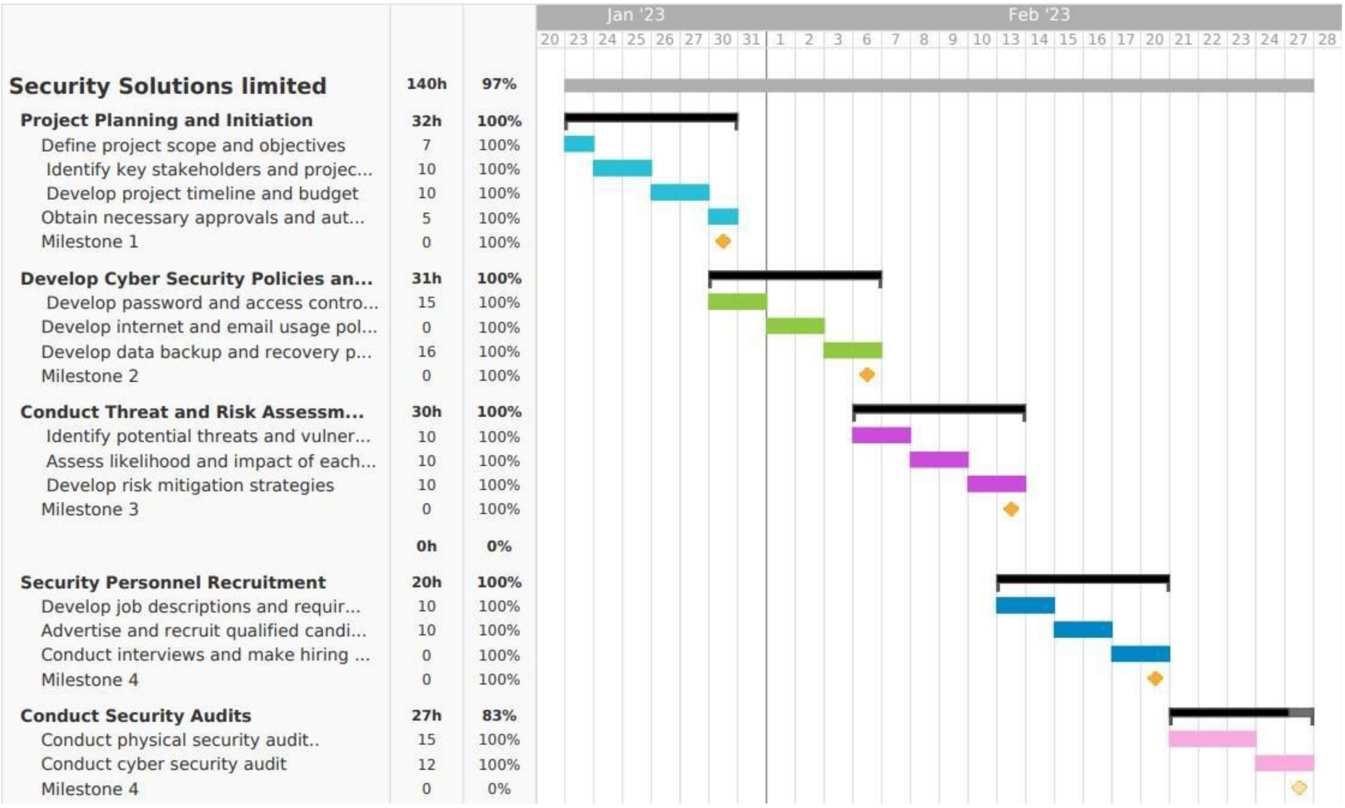
5.2 Project budget development and management

5.3 Project status reporting and communication

5.4 Risk management and issue resolution

5.5 Quality assurance and control

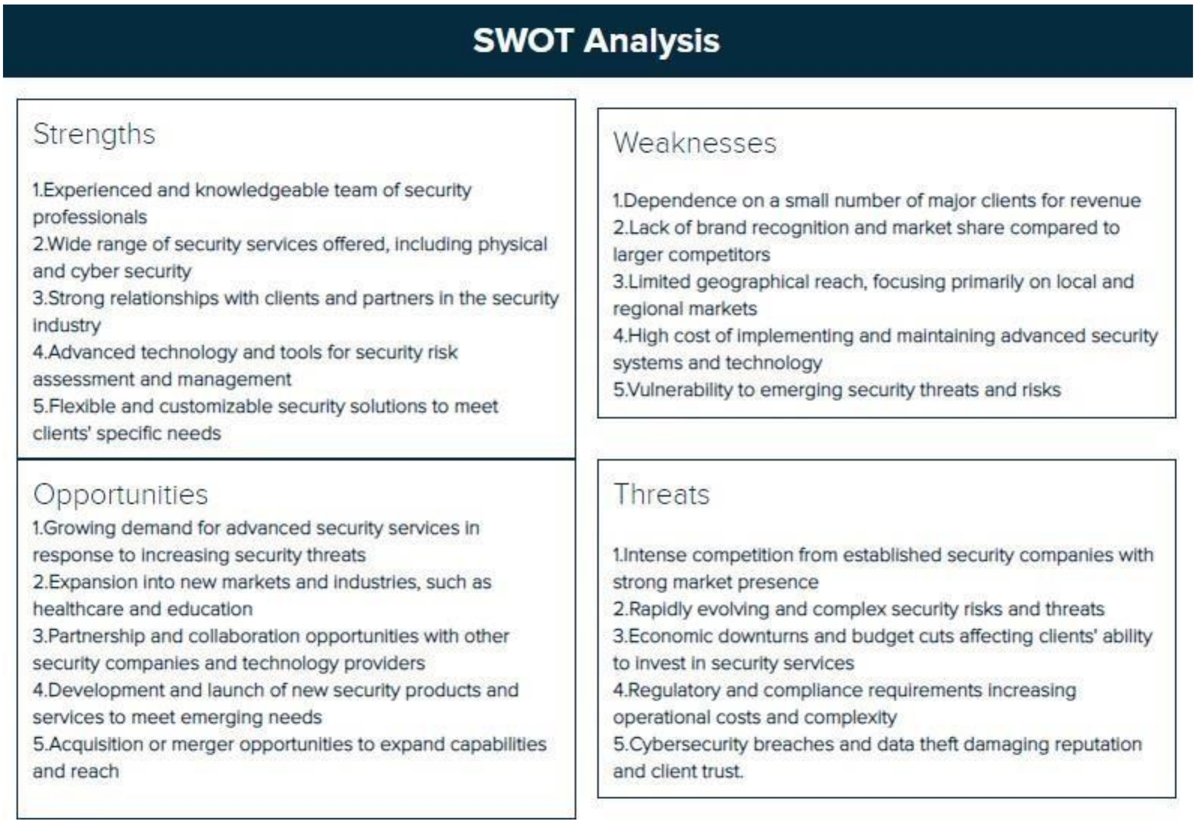
**TIMELINE – GANTT CHART :**



| | | |
|---|---|---|
| **Security Solutions limited** | **140h** | **97%** |
| **Project Planning and Initiation** | **32h** | **100%** |
| Define project scope and objectives | 7 | 100% |
| Identify key stakeholders and projec... | 10 | 100% |
| Develop project timeline and budget | 10 | 100% |
| Obtain necessary approvals and aut... | 5 | 100% |
| Milestone 1 | 0 | 100% |
| **Develop Cyber Security Policies an...** | **31h** | **100%** |
| Develop password and access contro... | 15 | 100% |
| Develop internet and email usage pol... | 0 | 100% |
| Develop data backup and recovery p... | 16 | 100% |
| Milestone 2 | 0 | 100% |
| **Conduct Threat and Risk Assessm...** | **30h** | **100%** |
| Identify potential threats and vulner... | 10 | 100% |
| Assess likelihood and impact of each... | 10 | 100% |
| Develop risk mitigation strategies | 10 | 100% |
| Milestone 3 | 0 | 100% |
| | **0h** | **0%** |
| **Security Personnel Recruitment** | **20h** | **100%** |
| Develop job descriptions and requir... | 10 | 100% |
| Advertise and recruit qualified candi... | 10 | 100% |
| Conduct interviews and make hiring ... | 0 | 100% |
| Milestone 4 | 0 | 100% |
| **Conduct Security Audits** | **27h** | **83%** |
| Conduct physical security audit.. | 15 | 100% |
| Conduct cyber security audit | 12 | 100% |
| Milestone 4 | 0 | 0% |

RISK ANALYSIS – SWOT &amp; RMMM:

SWOT analysis:



## SWOT Analysis

**Strengths**

1.Experienced and knowledgeable team of security professionals
2.Wide range of security services offered, including physical and cyber security
3.Strong relationships with clients and partners in the security industry
4.Advanced technology and tools for security risk assessment and management
5.Flexible and customizable security solutions to meet clients' specific needs

**Weaknesses**

1.Dependence on a small number of major clients for revenue
2.Lack of brand recognition and market share compared to larger competitors
3.Limited geographical reach, focusing primarily on local and regional markets
4.High cost of implementing and maintaining advanced security systems and technology
5.Vulnerability to emerging security threats and risks

**Opportunities**

1.Growing demand for advanced security services in response to increasing security threats
2.Expansion into new markets and industries, such as healthcare and education
3.Partnership and collaboration opportunities with other security companies and technology providers
4.Development and launch of new security products and services to meet emerging needs
5.Acquisition or merger opportunities to expand capabilities and reach

**Threats**

1.Intense competition from established security companies with strong market presence
2.Rapidly evolving and complex security risks and threats
3.Economic downturns and budget cuts affecting clients' ability to invest in security services
4.Regulatory and compliance requirements increasing operational costs and complexity
5.Cybersecurity breaches and data theft damaging reputation and client trust.

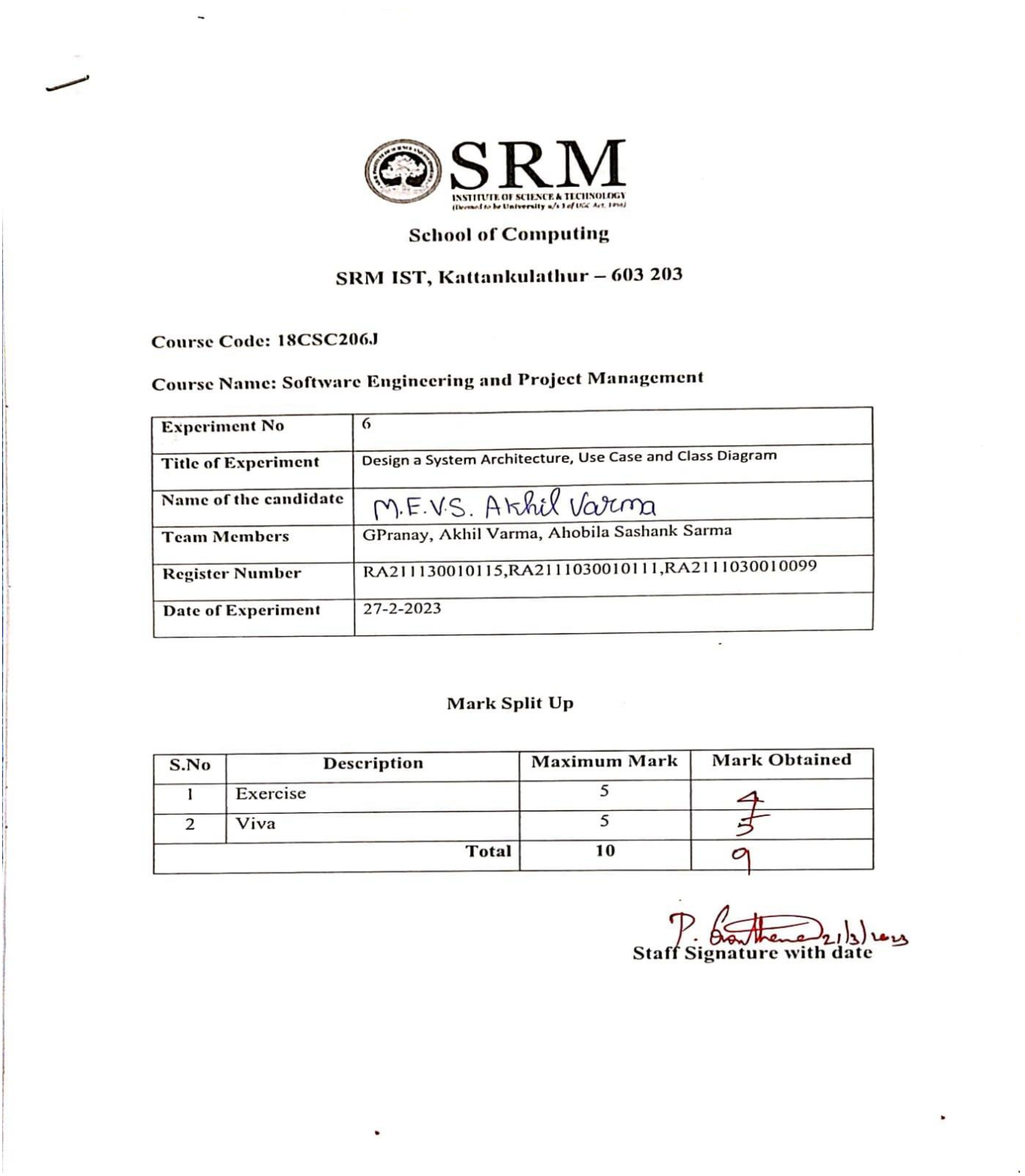
**Risk Mitigation, Monitoring, and Management Plan:**

| RISK CATEGORY | RISK DESCRIPTION | IMPACT | MITIGATION STRATEGY |
|---|---|---|---|
| Physical risks | Break-in to company permises by unauthorized persons | HIGH | Install security systems And access controls, conduct regular security audits |
| | Theft of company property by employees or third parties | HIGH | Implement strict inventory controls and conduct background checks on employees and contractors |
| | Workplace violence by disgruntled employees or outsiders | HIGH | Develop and implement a workplace violence prevention program, conduct employee training awareness programs |
| Cyber risks | Unauthorized access to company data or systems by hackers or insiders | HIGH | Implement firewalls, antivirus and intrusion detection systems, conduct regular vulnerability assessments and employee training on cybersecurity best practices |

| | | | |
|---|---|---|---|
| | Data breaches resulting in loss of sensitive or confidential information | HIGH | Implement strong authentication and encryption protocols, conduct regular backups and disaster recovery planning |
| | Social engineering attacks targeting employees or customers | MEDIUM | Conduct regular employee training and awareness programs, implement multi-factor authentication and security screening procedures |
| Operational risks | Failure of security equipment or systems due to technical issues or power outages | HIGH | Conduct regular maintenance and testing of security equipment and systems, implement backup power and contingency plans |

Result:

Thus, the work breakdown structure with timeline chart and risk table were formulated successfully.



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

**School of Computing**

**SRM IST, Kattankulathur – 603 203**

**Course Code: 18CSC206J**

**Course Name: Software Engineering and Project Management**

| | |
|---|---|
| **Experiment No** | 6 |
| **Title of Experiment** | Design a System Architecture, Use Case and Class Diagram |
| **Name of the candidate** | M.E.V.S. Akhil Varma |
| **Team Members** | GPranay, Akhil Varma, Ahobila Sashank Sarma |
| **Register Number** | RA211130010115,RA2111030010111,RA2111030010099 |
| **Date of Experiment** | 27-2-2023 |

**Mark Split Up**

| S.No | Description | Maximum Mark | Mark Obtained |
|---|---|---|---|
| 1 | Exercise | 5 | 4 |
| 2 | Viva | 5 | 5 |
| | **Total** | **10** | 9 |

21/3/2023
**Staff Signature with date**

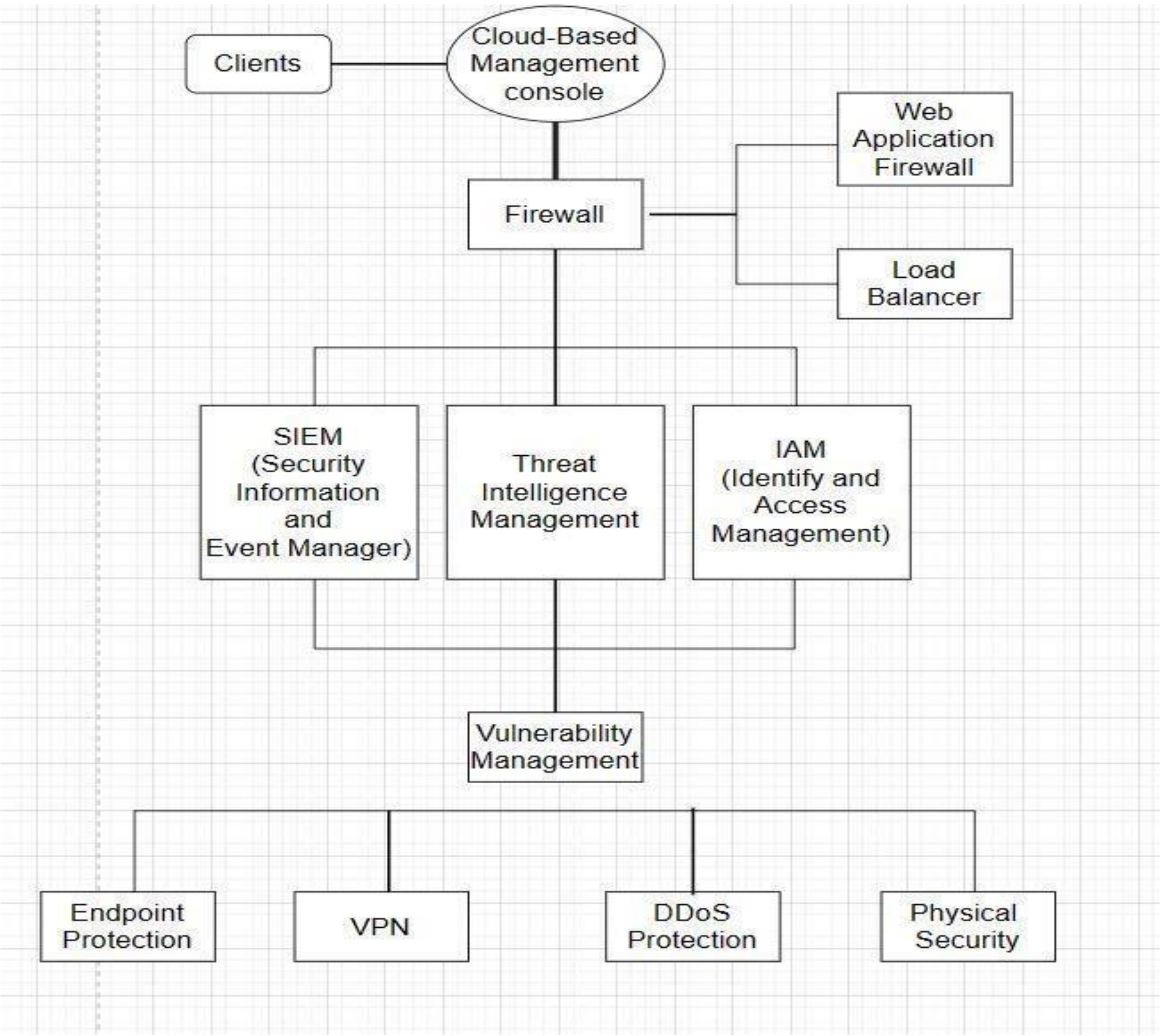
## Aim

To Design a System Architecture, Use case and Class Diagram

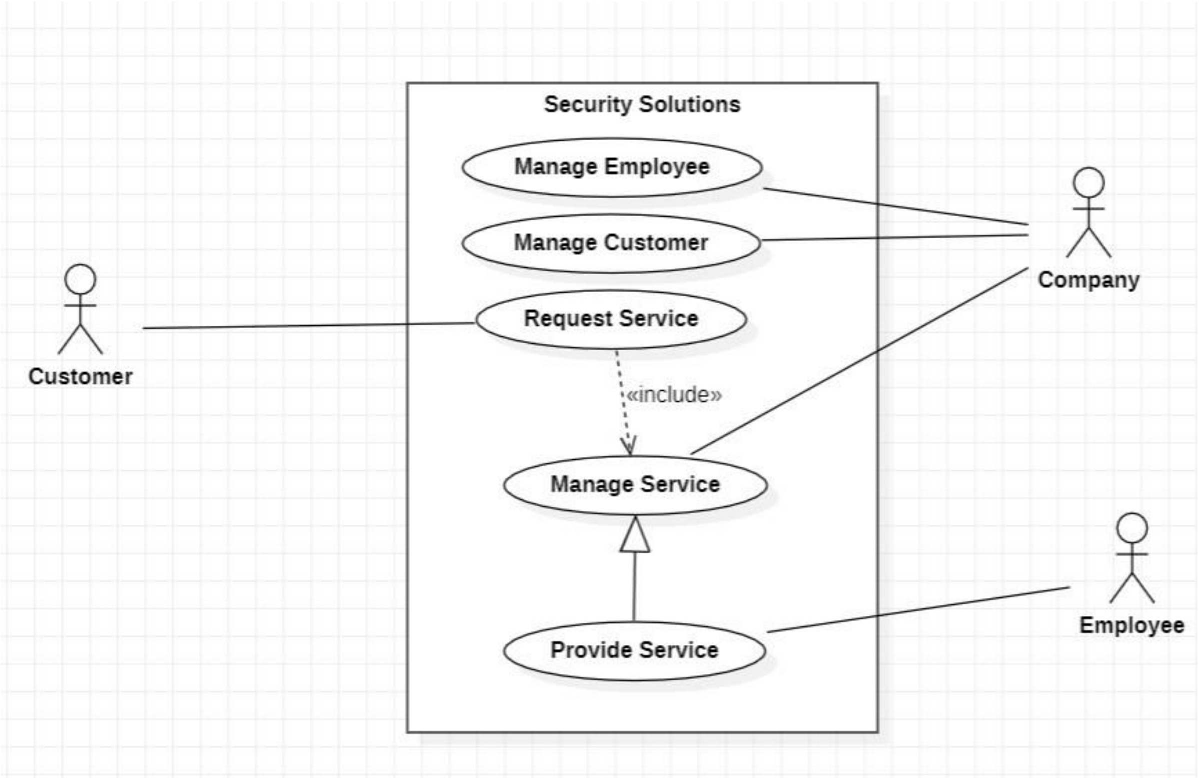
## Team Members:

| Sl No | Register No | Name | Role |
|---|---|---|---|
| 1 | RA2111030010111 | Ahobila Sashank sharma | Rep |
| 2 | RA2111030010115 | G Pranay | Member |
| 3 | RA2111030010099 | Akhil | Member |

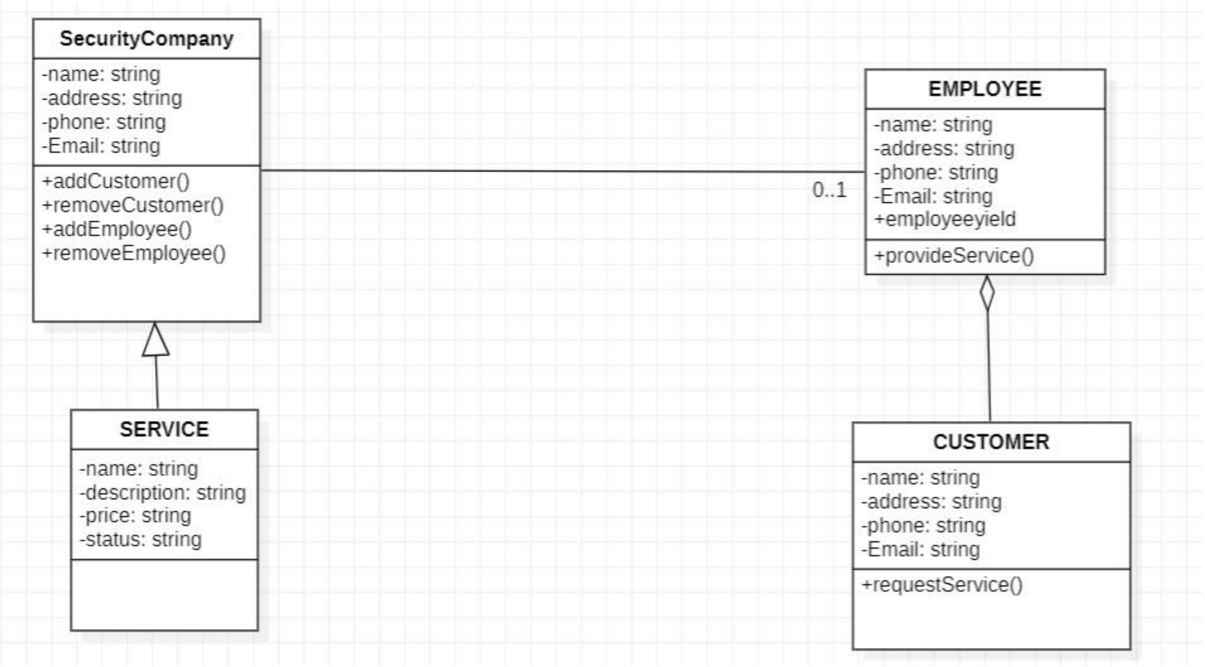
**System Architecture**:


Clients
Cloud-Based Management console
Web Application Firewall
Firewall
Load Balancer
SIEM (Security Information and Event Manager)
Threat Intelligence Management
IAM (Identify and Access Management)
Vulnerability Management
Endpoint Protection
VPN
DDoS Protection
Physical Security

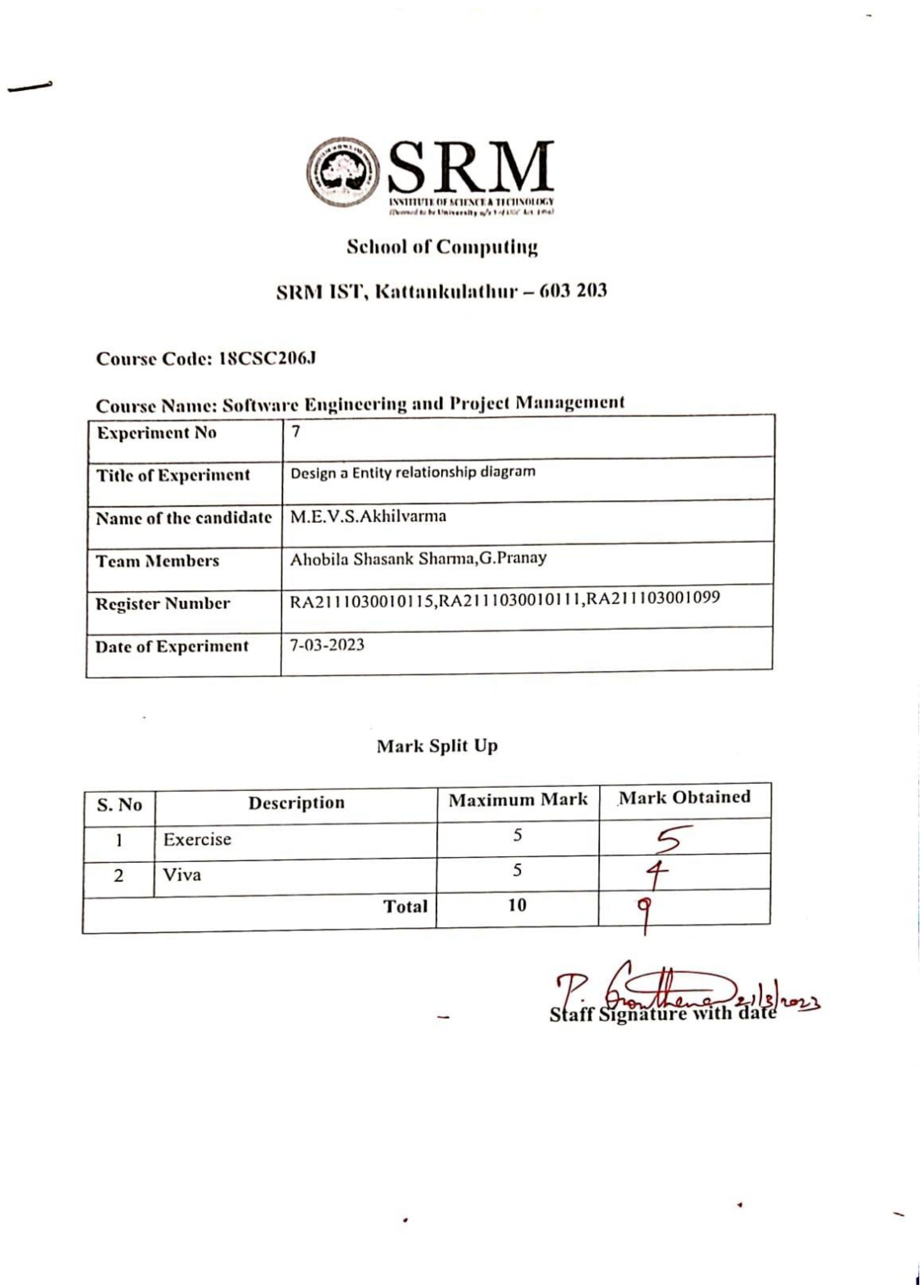
Use Case Diagram:



Class Diagram:



Result: Thus, the system architecture, use case and class diagram created successfully.



School of Computing

SRM IST, Kattankulathur – 603 203

Course Code: 18CSC206J

Course Name: Software Engineering and Project Management

| | |
|---|---|
| Experiment No | 7 |
| Title of Experiment | Design a Entity relationship diagram |
| Name of the candidate | M.E.V.S.Akhilvarma |
| Team Members | Ahobila Shasank Sharma,G.Pranay |
| Register Number | RA2111030010115,RA2111030010111,RA211103001099 |
| Date of Experiment | 7-03-2023 |

Mark Split Up

| S. No | Description | Maximum Mark | Mark Obtained |
|---|---|---|---|
| 1 | Exercise | 5 | 5 |
| 2 | Viva | 5 | 4 |
| | Total | 10 | 9 |

21/3/2023
Staff Signature with date

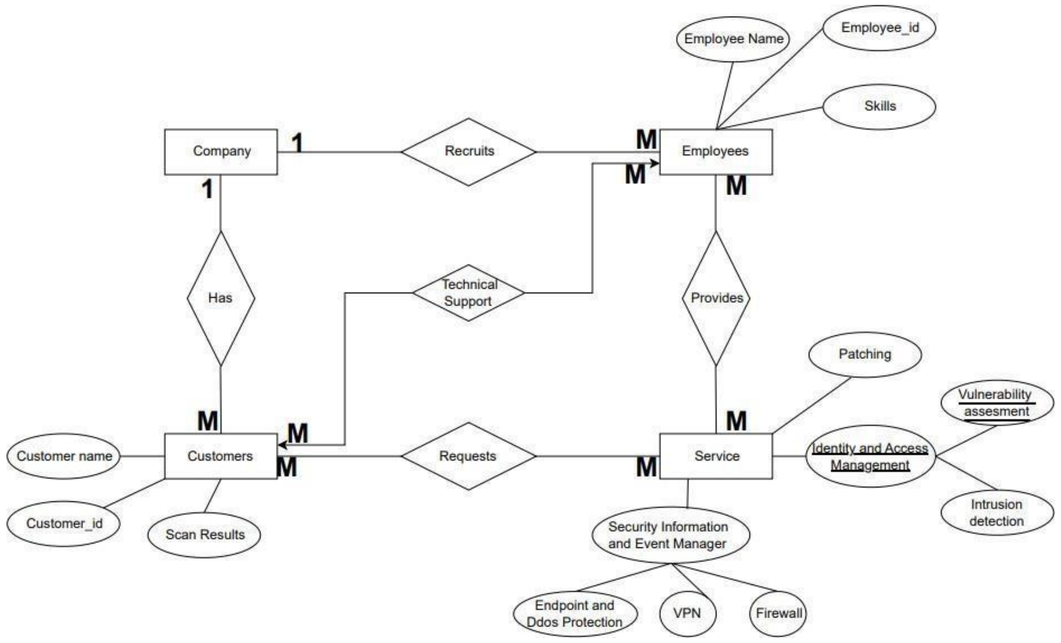
## Aim

To create the Entity Relationship Diagram

## Team Members:

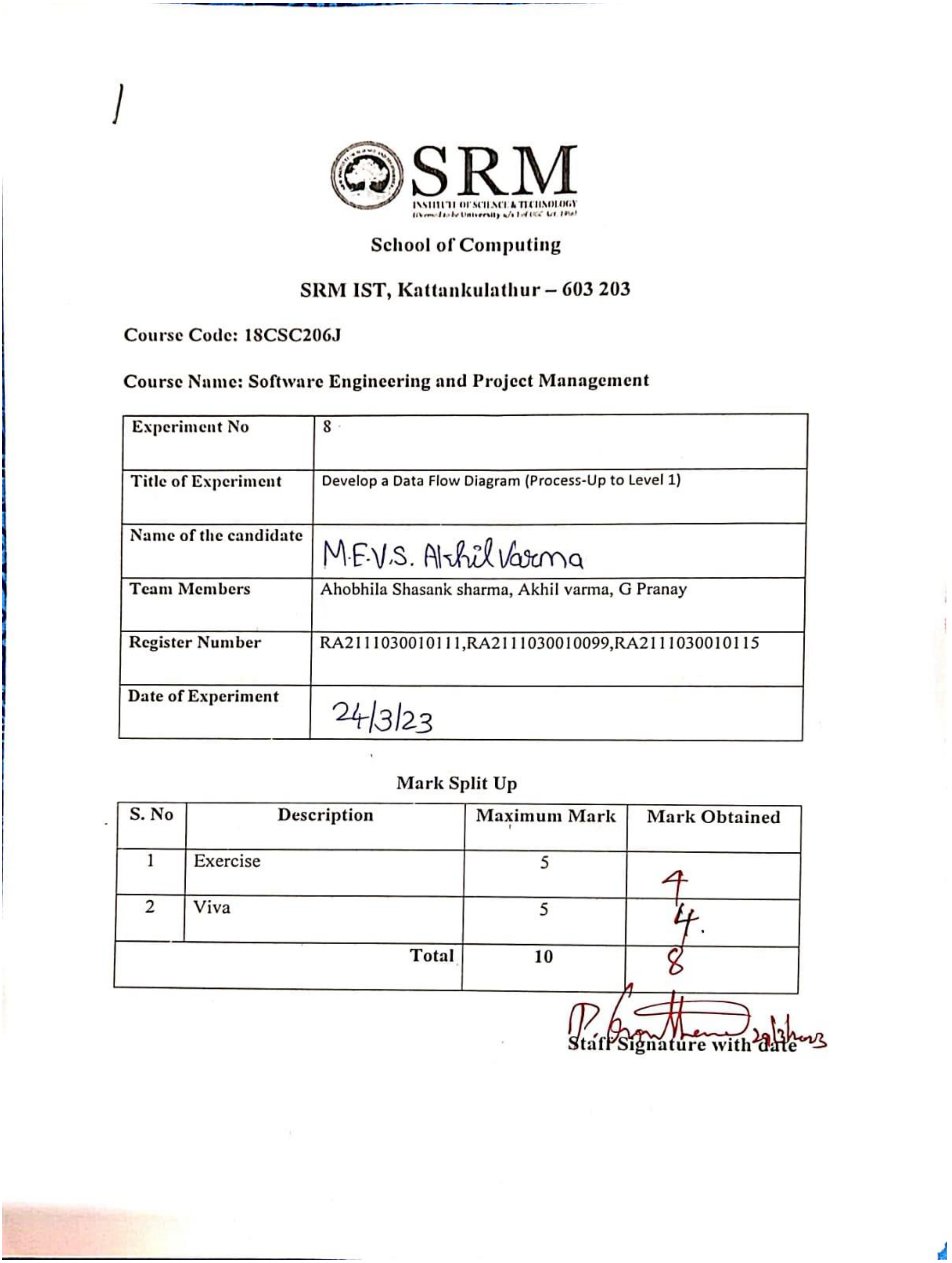
| S No | Register No | Name | Role |
|---|---|---|---|
| **1** | **RA2111030010111** | **Ahobila Sashank Sharma** | **Rep** |
| **2** | **RA2111030010115** | **G Pranay** | **Member** |
| **3** | **RA2111030010099** | **Akhil Varma** | **Member** |

Entity Relationship Diagram:



Result:

Thus, the entity relationship diagram was created successfully.



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

## School of Computing

## SRM IST, Kattankulathur – 603 203

**Course Code: 18CSC206J**

**Course Name: Software Engineering and Project Management**

| | |
|---|---|
| **Experiment No** | 8 |
| **Title of Experiment** | Develop a Data Flow Diagram (Process-Up to Level 1) |
| **Name of the candidate** | M.E.V.S. Akhil Varma |
| **Team Members** | Ahobhila Shasank sharma, Akhil varma, G Pranay |
| **Register Number** | RA2111030010111,RA2111030010099,RA2111030010115 |
| **Date of Experiment** | 24/3/23 |

**Mark Split Up**

| S. No | Description | Maximum Mark | Mark Obtained |
|---|---|---|---|
| 1 | Exercise | 5 | 4 |
| 2 | Viva | 5 | 4. |
| | **Total** | **10** | 8 |

29/3/23
**Staff Signature with date**

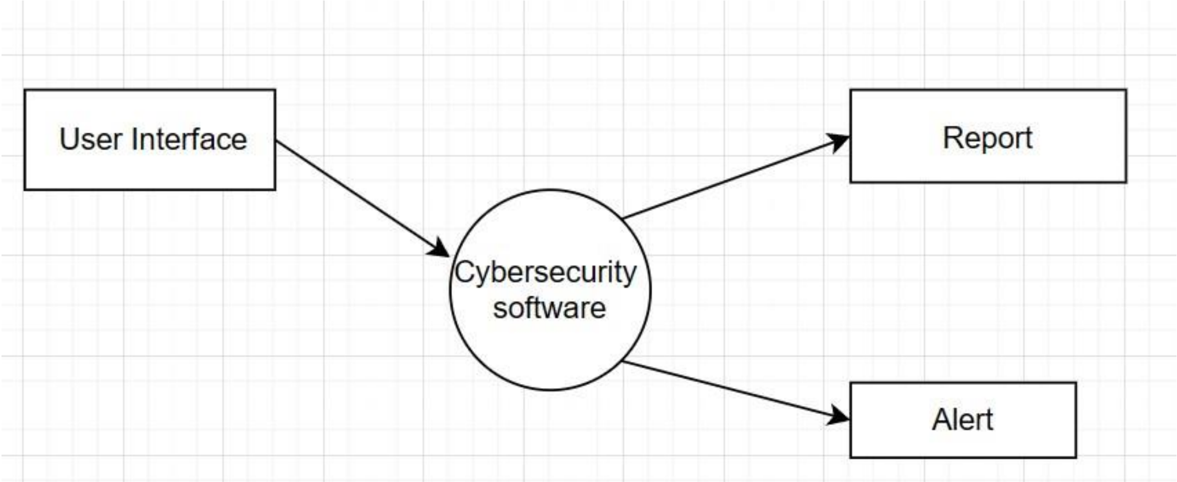
**Aim**

To develop the data flow diagram up to level 1 for the Security Solution limited

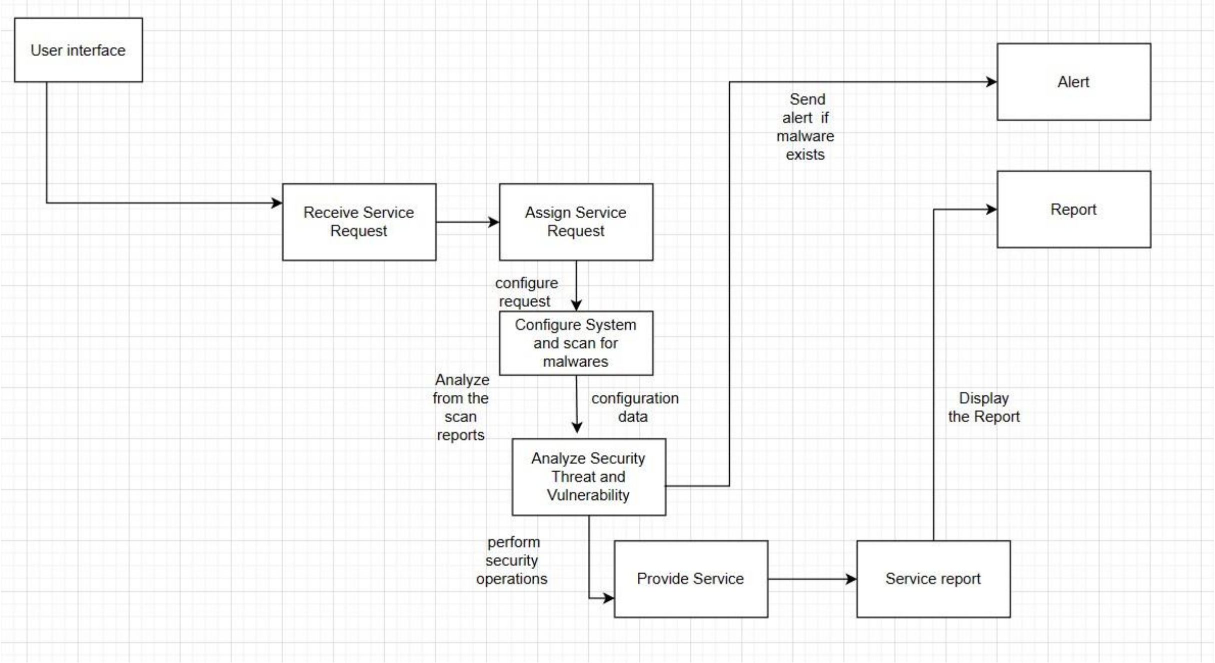
**Team Members:**

| S No | Register No | Name | Role |
|---|---|---|---|
| 1 | RA2111030010111 | Ahobhila Shasank sharma | Rep |
| 2 | RA2111030010099 | Akhil Varma | Member |
| 3 | RA2111030010115 | G Pranay | Member |

**Data flow diagram:**
**DFD Level 0:**

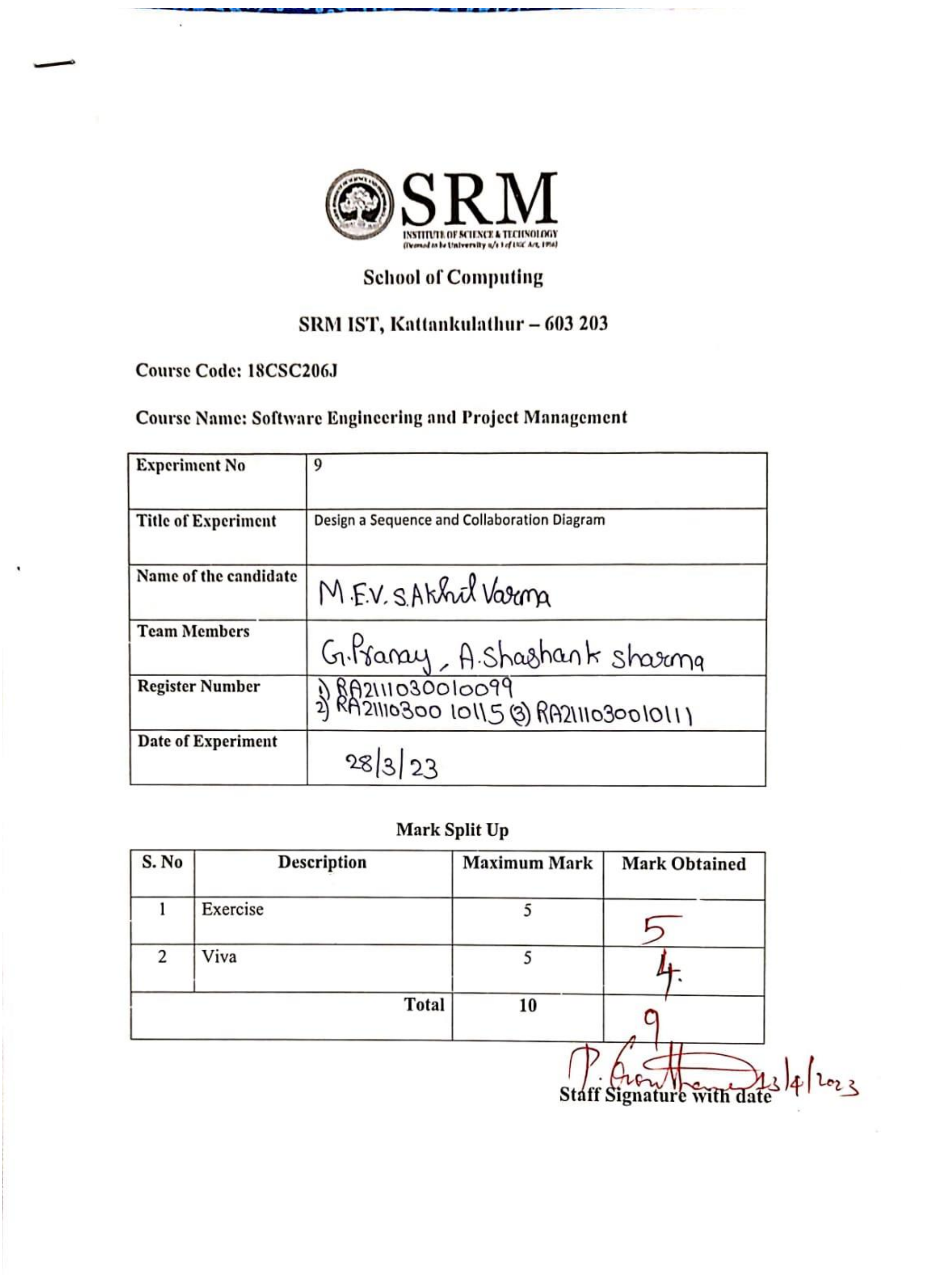


## DFD Level 1:


User interface
Receive Service Request
Assign Service Request
configure request
Configure System and scan for malwares
Analyze from the scan reports
configuration data
Analyze Security Threat and Vulnerability
perform security operations
Provide Service
Service report
Send alert if malware exists
Alert
Report
Display the Report

Result:

Thus, the data flow diagrams have been created for the Security Solution limited.



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

School of Computing

SRM IST, Kattankulathur – 603 203

Course Code: 18CSC206J

Course Name: Software Engineering and Project Management

| | |
|---|---|
| **Experiment No** | 9 |
| **Title of Experiment** | Design a Sequence and Collaboration Diagram |
| **Name of the candidate** | M.E.V. S.Akhil Varma |
| **Team Members** | G.Pranay , A.Shashank sharma |
| **Register Number** | 1) RA2111030010099<br>2) RA2111030010115 (3) RA2111030010111 |
| **Date of Experiment** | 28/3/23 |

**Mark Split Up**

| S. No | Description | Maximum Mark | Mark Obtained |
|---|---|---|---|
| 1 | Exercise | 5 | 5 |
| 2 | Viva | 5 | 4. |
| | **Total** | **10** | 9 |

Staff Signature with date 13/4/2023

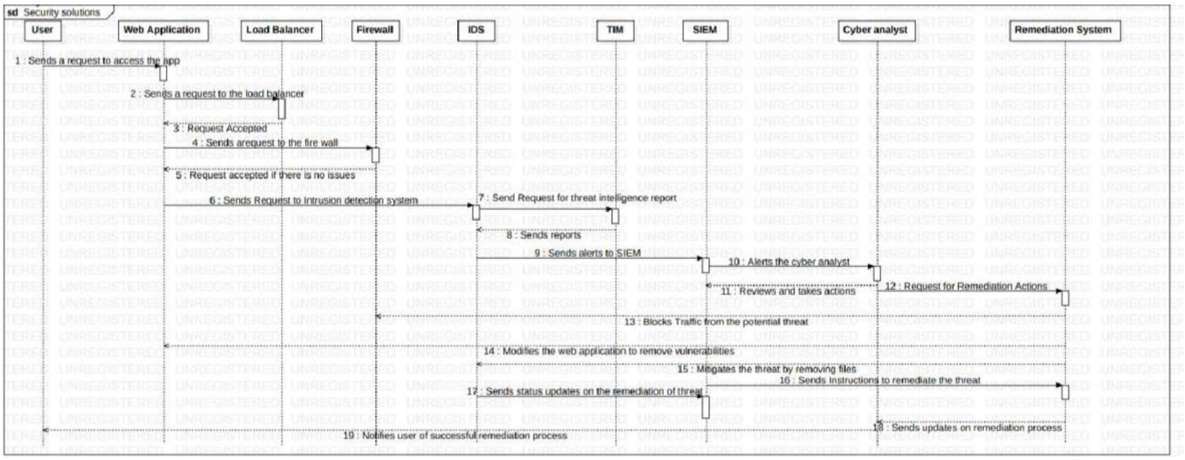
## Aim

To create the sequence and collaboration diagram for the security solutions limited.

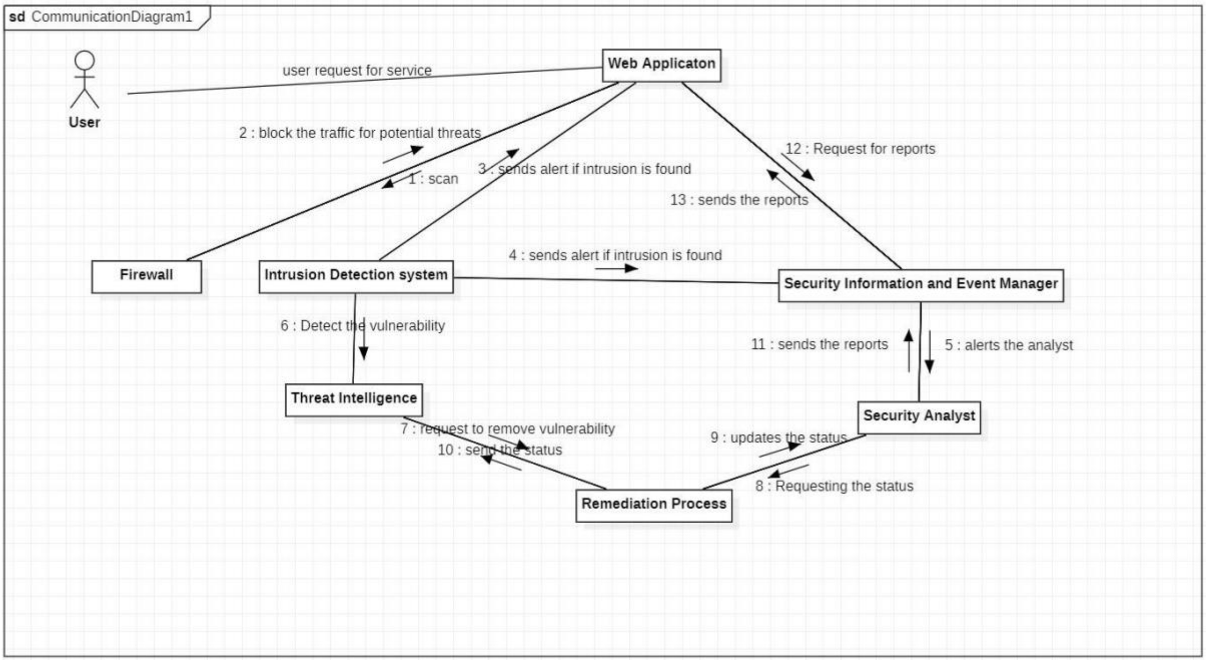
## Team Members:

| S No | Register No | Name | Role |
|---|---|---|---|
| **1** | **RA2111030010111** | **AHOBILA SASHANK SARMA** | **Rep/Member** |
| **2** | **RA2111030010115** | **G.PRANAY** | **Member** |
| **3** | **RA2111030010099** | **VENKATA SATYA AKHIL VERMA** | **Member** |

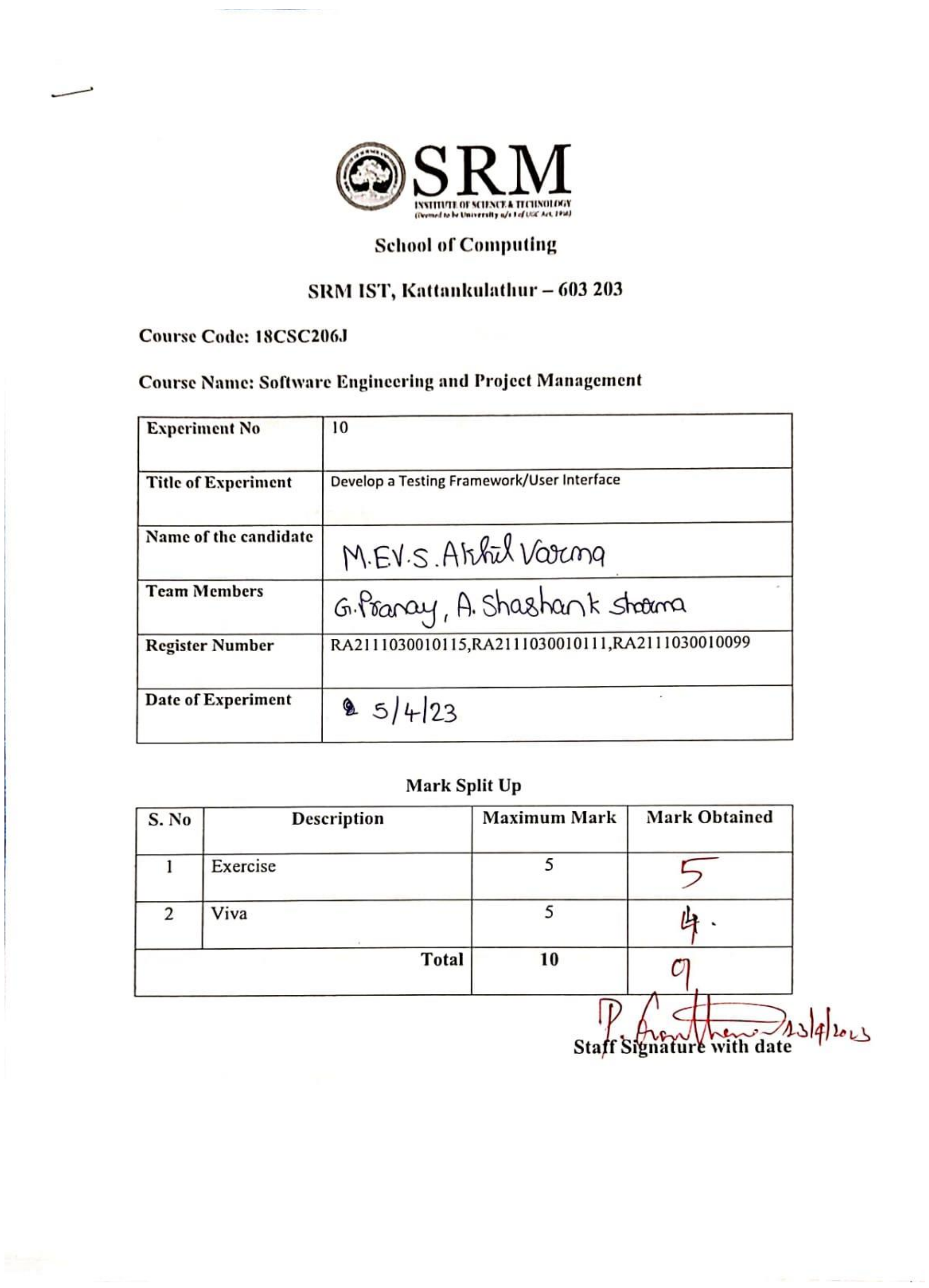
## Sequence Diagram:


sd Security solutions
User
Web Application
Load Balancer
Firewall
IDS
TIM
SIEM
Cyber analyst
Remediation System
1 : Sends a request to access the app
2 : Sends a request to the load balancer
3 : Request Accepted
4 : Sends arequest to the fire wall
5 : Request accepted if there is no issues
6 : Sends Request to Intrusion detection system
7 : Send Request for threat intelligence report
8 : Sends reports
9 : Sends alerts to SIEM
10 : Alerts the cyber analyst
11 : Reviews and takes actions
12 : Request for Remediation Actions
13 : Blocks Traffic from the potential threat
14 : Modifies the web application to remove vulnerabilities
15 : Mitigates the threat by removing files
16 : Sends Instructions to remediate the threat
17 : Sends status updates on the remediation of threat
18 : Sends updates on remediation process
19 : Notifies user of successful remediation process

## Collaboration Diagram:


sd CommunicationDiagram1
User
user request for service
Web Applicaton
2 : block the traffic for potential threats
1 : scan
3 : sends alert if intrusion is found
12 : Request for reports
13 : sends the reports
Firewall
Intrusion Detection system
4 : sends alert if intrusion is found
Security Information and Event Manager
6 : Detect the vulnerability
11 : sends the reports
5 : alerts the analyst
Threat Intelligence
Security Analyst
7 : request to remove vulnerability
10 : send the status
9 : updates the status
8 : Requesting the status
Remediation Process

Result: Thus, the sequence and collaboration diagrams were created for the Security solutions limited.



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

School of Computing

SRM IST, Kattankulathur – 603 203

**Course Code: 18CSC206J**

**Course Name: Software Engineering and Project Management**

| | |
|---|---|
| **Experiment No** | 10 |
| **Title of Experiment** | Develop a Testing Framework/User Interface |
| **Name of the candidate** | M.E.V.S. Akhil Varma |
| **Team Members** | G. Pranay, A. Shashank Sharma |
| **Register Number** | RA2111030010115,RA2111030010111,RA2111030010099 |
| **Date of Experiment** | 5/4/23 |

**Mark Split Up**

| S. No | Description | Maximum Mark | Mark Obtained |
|---|---|---|---|
| 1 | Exercise | 5 | 5 |
| 2 | Viva | 5 | 4. |
| | **Total** | **10** | 9 |

P. Aravinthan 23/4/2023

**Staff Signature with date**

**Aim**

To develop the testing framework and/or user interface framework for the Security Solutions limited.

**Team Members:**

| S No | Register No | Name | Role |
|---|---|---|---|
| 1 | RA2111030010111 | AHOBILA SASHANK SARMA | Rep/Member |
| 2 | RA2111030010115 | G.PRANAY | Member |
| 3 | RA2111030010099 | MANTHENA ESWAR VENKATA SATYA AKHIL VERMA | Member |

# Executive Summary

**Scope:**

To make sure that the systems and data that it is intended to secure are effectively protected, cybersecurity software must be put through rigorous testing. The user interface, network communication, data storage, and encryption techniques should all be tested, along with every other aspect of the software. **Objective:**

It is the goal of cybersecurity software testing to find and fix any flaws that an attacker might use against it. The testing should verify that the software is capable of detecting and preventing common attack vectors, such as malware, phishing, and unauthorized access.

**Approach:**

The following actions should be taken as part of a thorough testing strategy for cybersecurity software:

1) **Requirements Analysis:** Identify the functional and non-functional requirements of the software and use them as a basis for testing.

2) **Test Planning:** Develop a testing plan that defines the test scenarios, test cases, and test data to be used.
3) **Test Execution**: Execute the test cases according to the testing plan and document the results.

4) **Vulnerability Assessment:** Conduct vulnerability assessments to identify any weaknesses in the software.

5) **Penetration Testing:** Conduct penetration testing to simulate real-world attacks and assess the effectiveness of the software's security measures.

6) **Reporting:** Document and report all findings and recommendations for remediation.

7) **Retesting:** Verify that all identified issues have been resolved and conduct additional testing to ensure that the fixes did not introduce new vulnerabilities.

## Test Plan Scope of Testing

The scope of testing for cybersecurity software includes evaluating the effectiveness and integrity of the software's security mechanisms in protecting the system and data it is designed to secure. Here are some areas that should be included in the scope of testing for cybersecurity software:

1. **Authentication and access control:** Verify that the software effectively manages user authentication and access controls to prevent unauthorized access.

2. **Data protection:** Evaluate the software's data protection measures, including encryption, hashing, and key management, to ensure that sensitive data is adequately protected.

3. **Network security**: Test the software's network security measures, such as firewalls and intrusion detection/prevention systems, to identify potential vulnerabilities and verify that they are properly configured.

4. **Vulnerability assessments:** Conduct vulnerability assessments to identify any weaknesses in the software and prioritize remediation efforts.

5. **Penetration testing:** Conduct penetration testing to simulate real-world attacks and assess the effectiveness of the software's security measures.

6. **Security incident response:** Test the software's incident response capabilities to verify that it can detect, contain, and remediate security incidents.

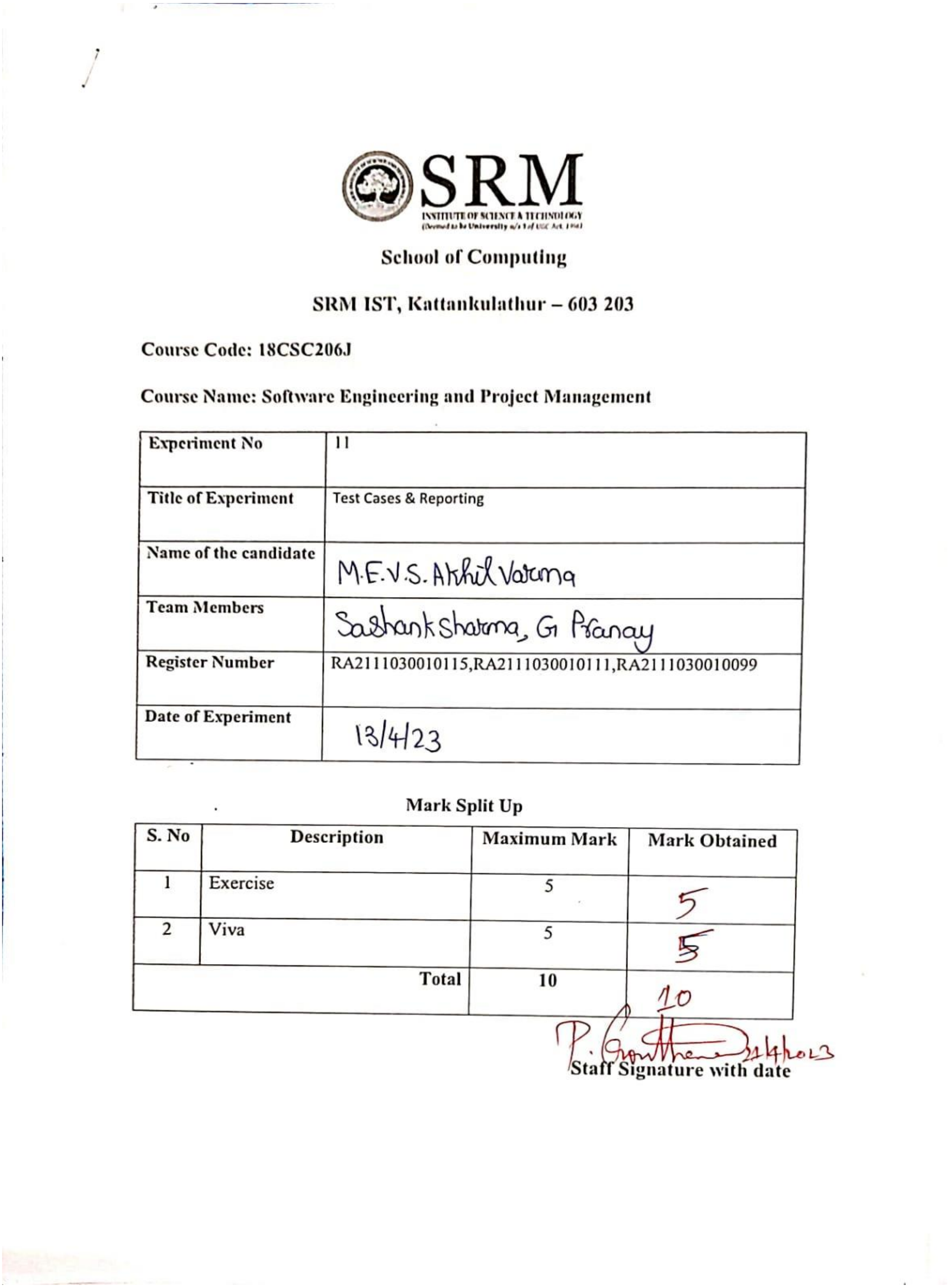
7. **Compliance testing:** Verify that the software meets relevant security compliance requirements, such as HIPAA or PCI DSS.

# Types of Testing, Methodology, Tools

| Category | Methodology | Tools Required |
|---|---|---|
| Vulnerability Assessment | Static Analysis, Dynamic Analysis | Nessus, OpenVAS, Retina, Nmap, Metasploit |
| Penetration Testing | Black Box Testing, White Box Testing, Gray Box Testing | Burp Suite, OWASP ZAP, Metasploit, Nmap |
| Security Configuration Review | Manual Review, Automated Scanning | CIS-CAT, Security Center, Qualys Policy Compliance |
| Risk Assessment Threat | Modeling, Attack Trees, Risk Matrices | Microsoft Threat Modeling Tool, IriusRisk, RiskLens |
| Security Compliance Testing | Manual Review, Automated Scanning | CIS-CAT, Security Center, Qualys Policy Compliance |
| Security Code Review | Static Analysis, Manual Review | Checkmarx, Veracode, SonarQube |
| Security Incident Response Testing | Tabletop Exercises, Simulations | IBM Resilient, CyberRange, NIST SP 800-61 Rev 2 |

**Result**:

Thus, the testing framework/user interface framework has been created for the Security Solutions.



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

School of Computing

SRM IST, Kattankulathur – 603 203

Course Code: 18CSC206J

Course Name: Software Engineering and Project Management

| | |
|---|---|
| Experiment No | 11 |
| Title of Experiment | Test Cases & Reporting |
| Name of the candidate | M.E.V.S. Akhil Varma |
| Team Members | Sashank Sharma, G Pranay |
| Register Number | RA2111030010115,RA2111030010111,RA2111030010099 |
| Date of Experiment | 13/4/23 |

Mark Split Up

| S. No | Description | Maximum Mark | Mark Obtained |
|---|---|---|---|
| 1 | Exercise | 5 | 5 |
| 2 | Viva | 5 | 5 |
| | Total | 10 | 10 |

P. Gowthame 21/4/2023
Staff Signature with date

**Aim**

To develop the test cases manual with manual test case report for the Security Solutions.

**Team Members:**

| S No | Register No | Name | Role |
|---|---|---|---|
| 1 | RA2111030010111 | Ssashank sarma | Rep |
| 2 | RA2111030010115 | G Pranay | Member |
| 3 | RA2111030010099 | Akhil varma | Member |

**Test**

**1. Scenario:[ Malware Detection] Preconditions:**

1)A clean computer system is available for installation of the cybersecurity software

2)The cybersecurity software is downloaded and available for installation

3)Access to a sample malware file for testing purposes

**Execution Steps:**

1)Install the cybersecurity software on a clean computer system

2)Launch the software and configure it for malware detection

3)Download a sample malware file to the computer system

4)Run a full system scan with the cybersecurity software

5)Wait for the scan to complete

6)Review the scan results to verify if the malware was detected

**Expected Outcome:**

The cybersecurity software detects the sample malware file and reports it as a threat during the system scan. The software should also provide appropriate recommendations for removing the malware from the system.

**Remarks:**

This test case is critical for verifying the malware detection capabilities of the cybersecurity software, which is a key component of its functionality. It is important to ensure that the software can effectively detect and remove all types of malware to ensure the security of the computer system.

**Obstacles:**

One of the obstacles to executing this test case could be the availability of the sample malware file. It may also be challenging to recreate a realistic malware scenario for testing purposes. **Seeking Help:**

The cybersecurity team can help by providing guidance on where to obtain sample malware files and how to create realistic malware scenarios for testing. They can also provide technical assistance with configuring the cybersecurity software for malware detection.

**2. Scenario: [Phishing Detection] Preconditions:**

1)A clean computer system is available for installation of the cybersecurity software

2)The cybersecurity software is downloaded and available for installation

3)Access to a known phishing website for testing purposes

**Execution Steps:**

**Test**

1)Install the cybersecurity software on a clean computer system

2)Launch the software and configure it for phishing detection

3)Access a known phishing website using a web browser

4)Wait for the cybersecurity software to detect the phishing attempt

5)Verify that the software alerts the user of the phishing attempt and provides instructions on how to avoid it

**Expected Outcome:**

The cybersecurity software should be able to detect the phishing attempt and alert the user with appropriate instructions to avoid the phishing attempt. This test case is critical to verify that the cybersecurity software can protect the user from phishing attacks, which are a common form of cybercrime.

**Remarks:**

Phishing attacks are becoming more sophisticated and can be difficult to detect. It is important to ensure that the cybersecurity software can effectively detect and alert the user of these attempts to prevent them from becoming victims of cybercrime.

**Obstacles:**

One of the obstacles to executing this test case is identifying a known phishing website to use for testing. It may also be challenging to ensure that the test environment accurately simulates a real-world phishing attempt.

**Seeking Help:**

The cybersecurity team can help by providing guidance on identifying known phishing websites for testing and providing technical assistance with configuring the cybersecurity software for phishing detection. They can also provide recommendations for creating a realistic test environment.

**3. Scenario:[ Backup and Recovery]**

**Preconditions:**

A clean computer system is available for installation of the cybersecurity software

The cybersecurity software is downloaded and available for installation Access

to critical files and data to backup and test the restore process with **Execution**

**Steps:**

1)Install the cybersecurity software on a clean computer system

**Test**

2) Configure the software to perform regular backups of important files and data

3) Create a backup of the system or select an existing backup to restore from

4) Delete a critical file or folder from the system

5) Initiate the restore process using the selected backup

6) Verify that the deleted file or folder has been successfully restored **Expected Outcome:**

The cybersecurity software should be able to perform regular backups of important files and data and restore them in case of a data loss event. The restore process should be easy to initiate, and the deleted file or folder should be successfully restored.

**Remarks:**

Backup and recovery is a critical function of the cybersecurity software, and it is important to ensure that it is working effectively. This test case is necessary to verify that the backup and recovery process is easy to use and reliable in the event of data loss.

**Obstacles:**

One of the obstacles to executing this test case is ensuring that the backup and recovery process is properly configured to backup critical files and data. It may also be challenging to recreate a realistic data loss scenario for testing purposes.

**Seeking Help:**

The cybersecurity team can help by providing guidance on configuring the backup and recovery process to ensure critical files and data are being backed up. They can also provide technical assistance with initiating the restore process and verifying that the deleted files or folders have been successfully restored.

**Functional Test Cases:**

| Test ID (#) | Test Scenario | Test Case | Execution Steps | Expected Outcome | Status | Remarks |
|---|---|---|---|---|---|---|
| 1 | Authentication | Valid Login | 1. Launch the software<br>2. Enter valid username and password | The user is authenticated and redirected to the appropriate page | Pass | Resource constraint, need additional equipment |
| 2 | Authorization | Access Control | 1. Attempt to access sensitive data or functionalities without authorization<br>2. Attempt to access sensitive data or functionalities with proper authorization | Unauthorized access is denied, authorized access is granted | Pass | Resource constraint, need additional personnel |
| 3 | Malware Detection | Real-time Protection | 1. Launch the software<br>2. Attempt to download a file infected with known malware | The software detects and blocks the malware threat in real-time | Incomplete | Testing in progress |
| 4 | Phishing Detection | Alert Notification | 1. Launch the software 2. Visit a website with a known phishing attempt | The software alerts the user of the potential phishing attempt | Incomplete | Testing in progress |

| | | | | | | |
|---|---|---|---|---|---|---|
| 5 | Backup and Recovery | Data Recovery | 1. Launch the software<br>2. Attempt to recover a previously backed-up file | The software successfully recovers the file | Incomplete | Testing in progress |

**Non Functional Test Cases:**

| Test ID (#) | Test Scenario | Test Case | Execution Steps | Expected Outcome | Status | Remarks |
|---|---|---|---|---|---|---|
| 1 | Performance | Response Time | 1. Launch the software<br>2. Perform various operations | The software responds to user inputs in a timely manner, with no significant delays | Incomplete | Testing in progress |
| 2 | Usability | User Interface | 1. Launch the software<br>2. Evaluate the user interface design and layout | The software's user interface is easy to navigate and understand, with intuitive design and clear instructions | Incomplete | Testing in progress |
| 3 | Compatibility | Platform Compatibility | 1. Install the software on various platforms<br>2. Test basic functionalities on each platform | The software operates smoothly on all supported platforms, with no compatibility issues | Not executed | Resource constraint, need additional equipment |
| 4 | Security | Data Protection | 1. Attempt to access sensitive data or files | The software restricts unauthorized | Incomplete | Testing in progress |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | without proper authorization 2. Test the software's ability to encrypt and protect user data | access to sensitive data and files, and effectively encrypts and protects user data | | |
| 5 | Reliability | Stability | 1. Launch the software<br>2. Perform various operations over a period of time | The software remains stable and reliable, with no unexpected crashes or errors | Incomplete | Testing in progress |

| **Category** | **Progress Against Plan** | **Status** |
|---|---|---|
| Functional Testing | Amber | Incomplete |
| Non-functional Testing | Green | Complete |
| Resource Constraints | Red (Lack of equipment and personnel) | Ongoing |
| Overall Testing | Amber (Behind schedule) | Incomplete |

Result:

Thus, the test case manual and report has been created for the Security Solutions.

## School of Computing

## SRM IST, Kattankulathur – 603 203

**Course Code: 18CSC206J**

**Course Name: Software Engineering and Project Management**

| | |
|---|---|
| **Experiment No** | 12 |
| **Title of Experiment** | Provide the details of Architecture Design/Framework/ Implementation |
| **Name of the candidate** | M.E.V.S.AKHIL VARMA |
| **Team Members** | G.Pranay, sashank sharma |
| **Register Number** | RA2111030010099,RA2111030010111,RA2111030010115 |
| **Date of Experiment** | 25/4/23 |

### Mark Split Up

| S. No | Description | Maximum Mark | Mark Obtained |
|---|---|---|---|
| 1 | Exercise | 5 | |
| 2 | Viva | 5 | |
| | **Total** | **10** | |

**Staff Signature with date**

**Aim**

To provide the details of architectural design/framework/implementation

**Team Members:**

| S No | Register No | Name | Role |
|---|---|---|---|
| 1 | RA2111030010111 | Sashank sharma | Rep/Member |
| 2 | RA2111030010115 | G Pranay | Member |
| 3 | RA2111030010099 | Akhil varma | Member |

**Architectural Design:**

The e-commerce web application will have a layered architecture design that separates the different components of the application. The layers will include the Presentation layer, the Business Logic layer, and the Data Access layer. This design will help in enhancing the security, scalability, and maintainability of the application.

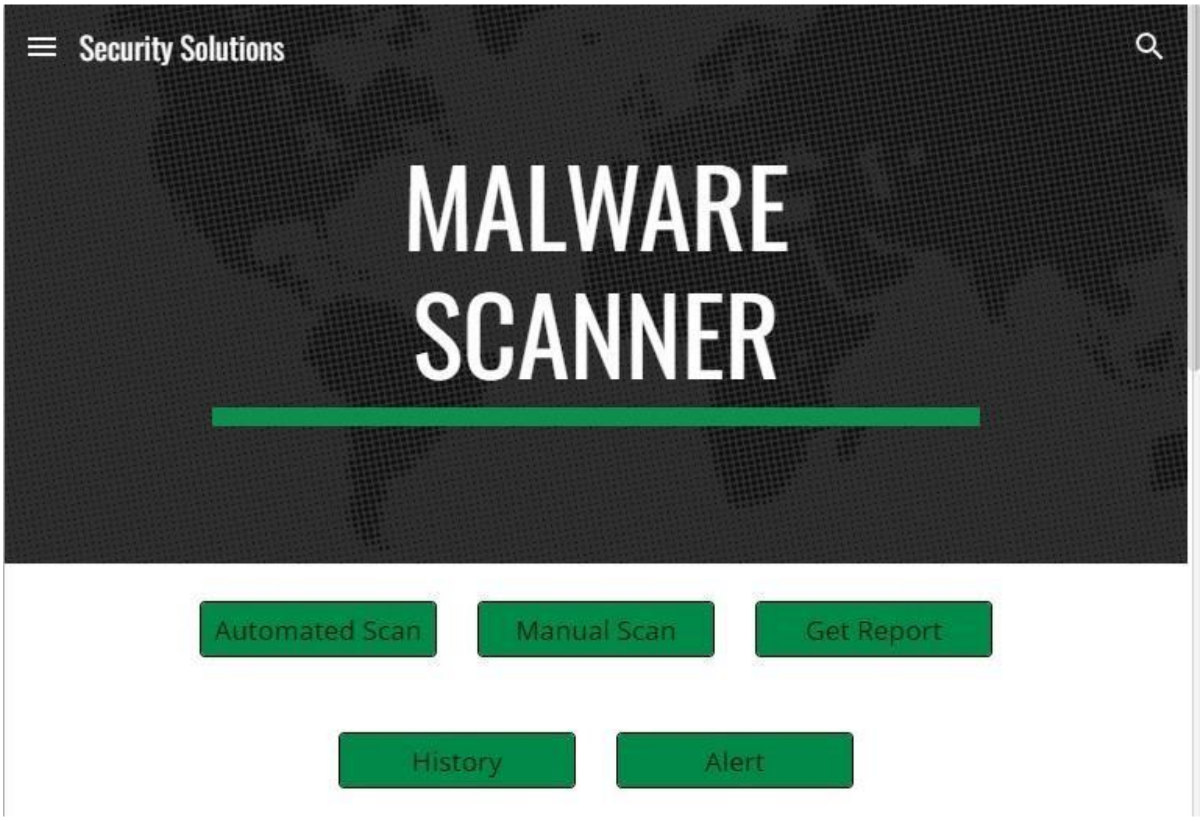
**Framework:**

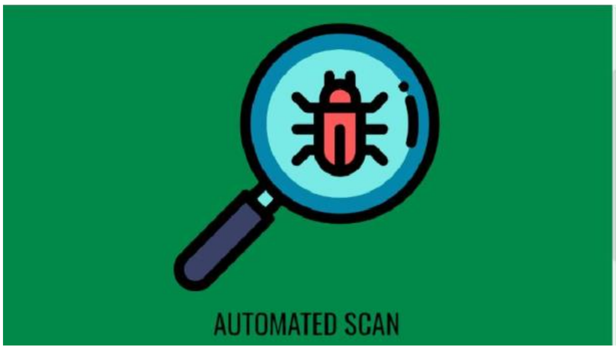
The web application will be built using the popular PHP programming language and the Laravel web framework. Laravel is a secure, scalable, and easy-to-use framework that simplifies the development of web applications. It also has built-in security features that help in preventing common web application vulnerabilities.

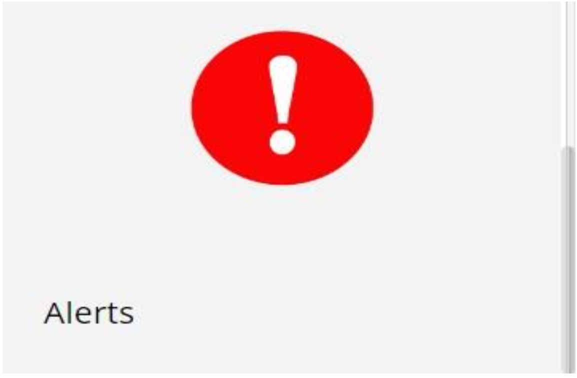
The Presentation layer will be responsible for handling the user interface of the web application. It will use HTML, CSS, and JavaScript to create the visual components of the application. The Business Logic layer will handle the application's logic and will be responsible for processing user requests and interacting with the database. The Data Access layer will interact with the database and handle data retrieval and storage.

**Malware Detection Module:**

The malware detection module will be responsible for detecting malware on a user's device. It will use various scanning techniques to identify malicious files and processes running on the system. The module will have a database of known malware signatures that it will use to detect malware. The user will be alerted if malware is detected, and the software will quarantine the infected files.

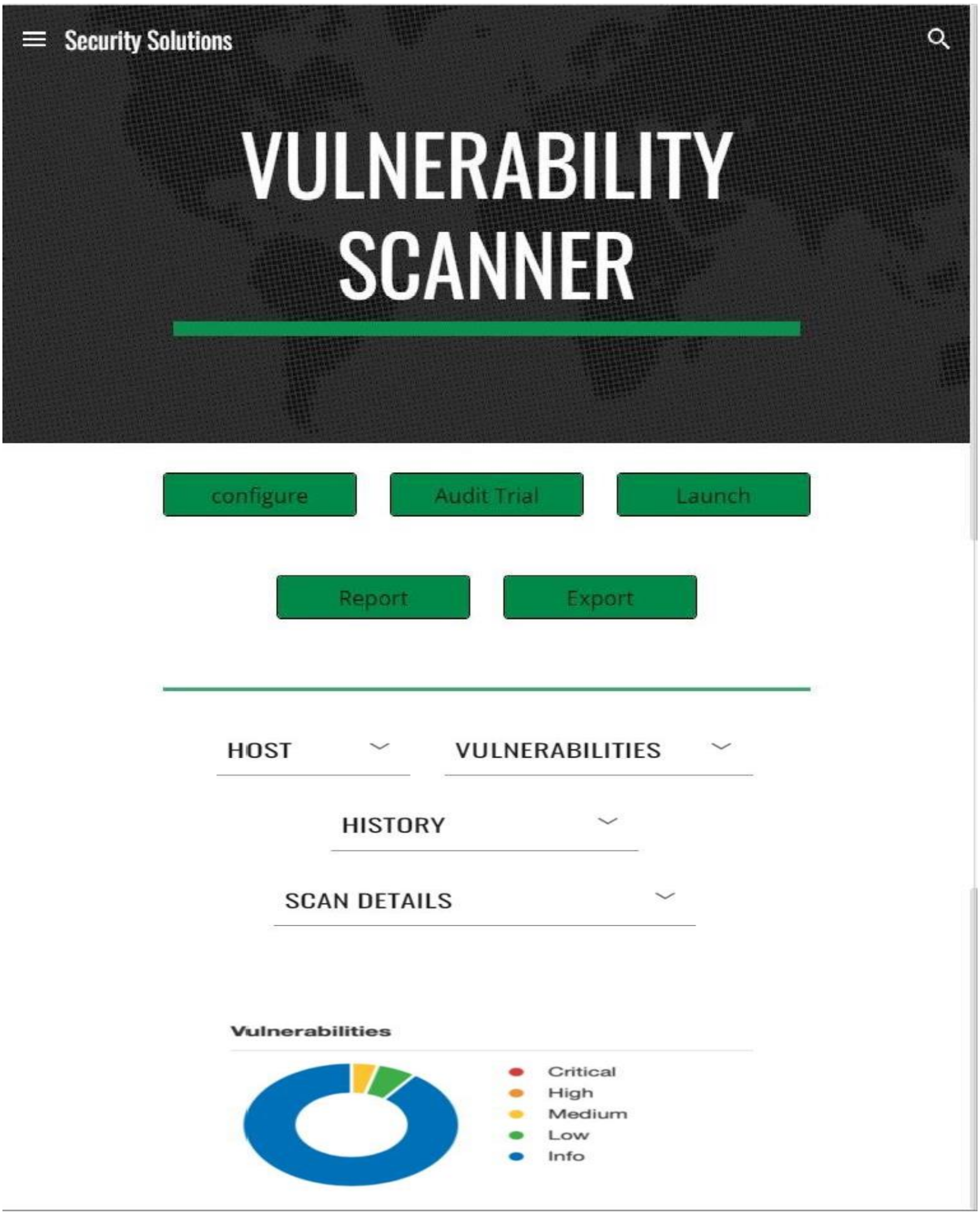






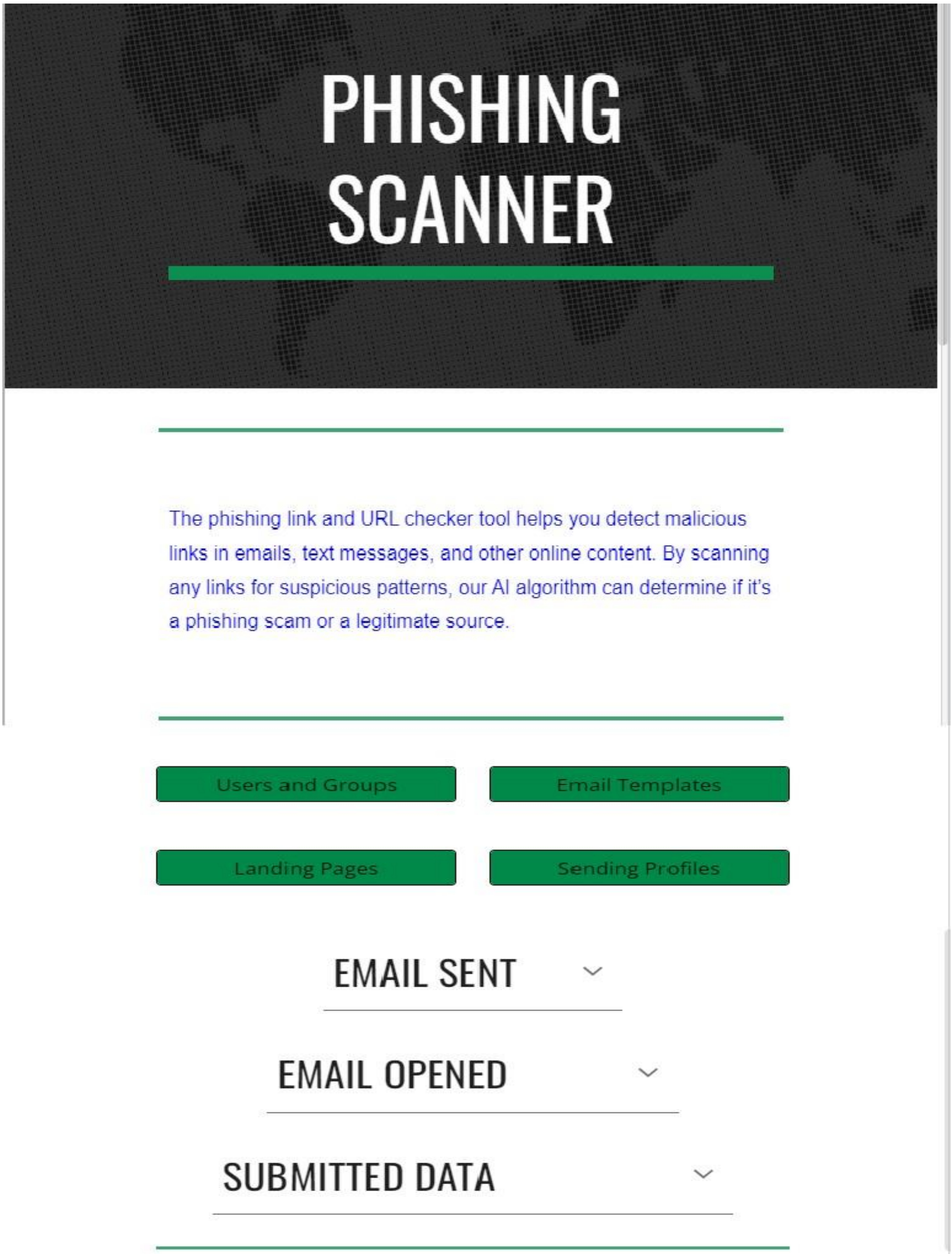
**Vulnerability Assessment Module:**

The vulnerability assessment module will identify and assess potential vulnerabilities in the user's device or network. It will scan for known vulnerabilities in software applications, operating systems, and other components that could be exploited by attackers. The module will provide recommendations on how to fix the identified vulnerabilities, such as applying security patches or upgrading software versions.



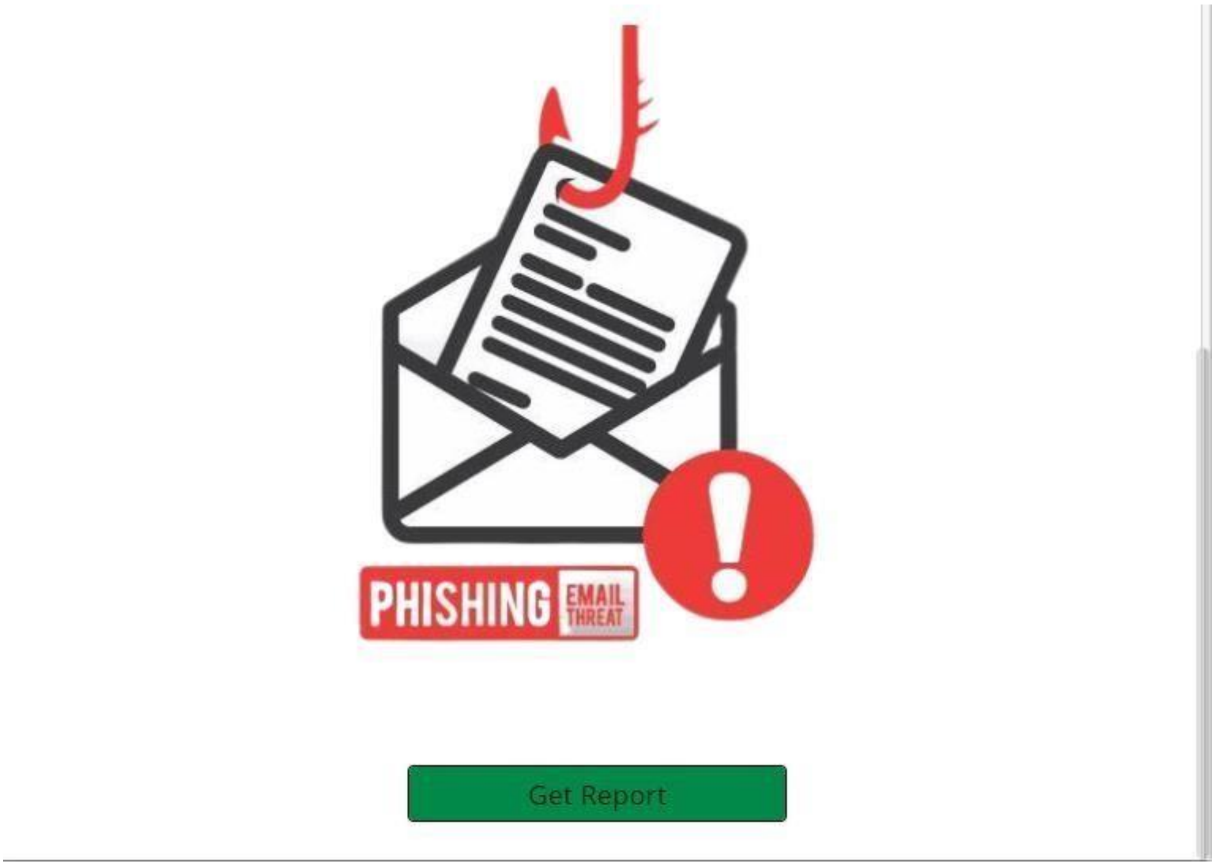
## Phishing Protection Module:

The phishing protection module will help protect the user from phishing attacks. It will scan incoming emails and URLs for known phishing patterns and indicators of compromise. If a phishing attempt is detected, the module will block the email or URL and alert the user. The module will also provide education and training resources to help the user recognize and avoid.



PHISHING SCANNER

The phishing link and URL checker tool helps you detect malicious links in emails, text messages, and other online content. By scanning any links for suspicious patterns, our AI algorithm can determine if it's a phishing scam or a legitimate source.



Result:

Thus, the details of architectural design/framework/implementation along with the screenshots were provided.

## CONCLUSION:

In today's digital age, cybersecurity is a critical concern for businesses, organizations, and individuals alike. The increasing frequency and sophistication of cyber attacks means that robust and reliable cybersecurity software is essential for protecting against data breaches, financial losses, and other forms of cybercrime.

Effective cybersecurity software should combine advanced threat detection technologies with behavioral analytics, real-time monitoring, and customizable security settings. It should be easy to install and use, with minimal impact on system performance, and should provide regular updates to stay up-to-date with the latest threats.

In conclusion, investing in high-quality cybersecurity software is crucial for protecting your digital assets and ensuring the security and privacy of your sensitive information. By choosing a reliable and comprehensive cybersecurity solution, you can stay on.

Cybersecurity is a critical concern in today's digital age, and effective cybersecurity software is essential for protecting against cyber threats. The best cybersecurity software should include advanced threat detection technologies, real-time monitoring, customizable security settings, easy installation and use, and regular updates. By investing in high-quality cybersecurity software, individuals and businesses can safeguard their digital assets, protect sensitive information, and stay ahead of evolving threats.

## REFERENCES:

1)https://www.totalav.com/free-download

2) https://www.manageengine.com/log-management/siem-solution-log360.html?utm_source=guru99&utm_medium=tp_cpc&utm_campaign=log360_cybersec

3) https://www.acunetix.com/plp/dast/?utm_medium=3rdparty&utm_source=guru99&utm_campaign=cybersecurity-software-tools&utm_content=listing

4) https://www.nortonlifelock.com/in/en/legal/?SID=cybersecurity-software-tools&cjid=9170115&clickid=4b9e9346e3f211ed832d00140a18ba72&af_sub4=aff&af_sub5=CJ&c=CJ&cjevent=4b9e9346e3f211ed832d00140a18ba72

5) https://www.pmi.org/about/learn-about-pmi/what-is-project-management

6) https://project-management.com/what-is-project-management/

**APPENDIX:**

**1) Glossary of Terms: A list of terms and definitions related to cybersecurity, including technical terms and acronyms.**

**2)Risk Assessment Template: A template for conducting a comprehensive risk assessment, including identifying threats, vulnerabilities, and potential impacts.**

**3)Incident Response Plan: A step-by-step guide for responding to a cybersecurity incident, including communication protocols, containment procedures, and recovery strategies.**

**4)Security Policy Template: A template for developing a comprehensive security policy that outlines best practices for protecting digital assets, including data classification, access controls, and employee training.**

**5)Vendor Assessment Checklist: A checklist for assessing the cybersecurity practices of third-party vendors and service providers, including evaluating their risk management processes and data protection protocols.**

**6)Compliance Requirements: A list of regulatory compliance requirements related to cybersecurity, including industry-specific standards such as HIPAA or PCI DSS.**