Raj Kumar Goel Institute of Technology Ghaziabad
5th KM. STONE, DELHI-MEERUT ROAD, GHAZIABAD (U.P)-201003

Department of Computer Science & Engineering

Final Year Project Approval Presentation on

Honeypots : Hackers Tracking

Students

Sanju Tomer(2000330109010)

Yugal Teotia(2000330109012)

Mohd Nadir(2000330109006)

Under the Guidance of

Ms. Kumud Alok

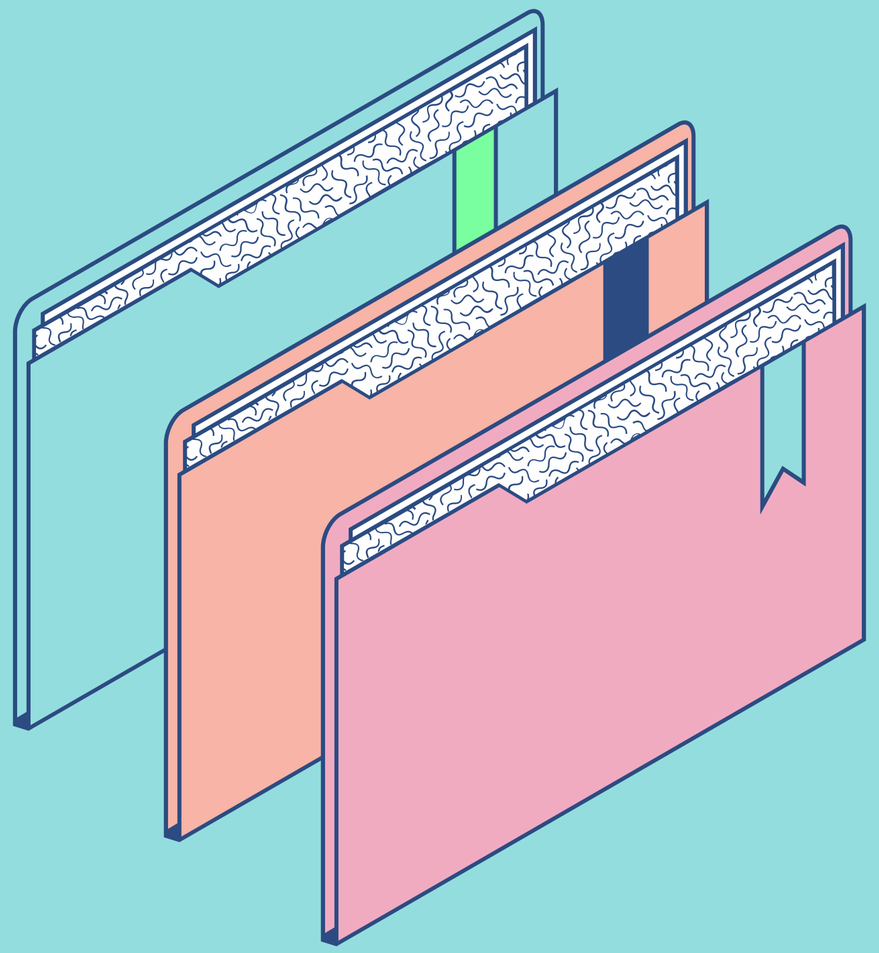
Department of CSE

HONEYPOTS

In computer terminology, a honey pot is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated, (un)protected, and monitored, and which seems to contain information or a resource of value to attackers.

OBJECTIVE

- In the digital arms race that is crackers vs. administrator, tightening the existing security holes will only force the crackers to get better, while the administrator get complacent.
- Of course, the true answer is for administrator and software programmers who actually take a little pride in their work, and do their jobs properly.
- Also, it would help if software companies would take some responsibility when they find security holes in their product, and to update accordingly.
- Hence our project "Honeypots: Tracking Hackers" is the sole answer to all such problems.



METHODOLOGY

- Deploy honeypots.
- Record attacker behavior.
- Analyze attacker behavior.
- Classify attacker behavior.
- Report findings.
- Make recommendations.

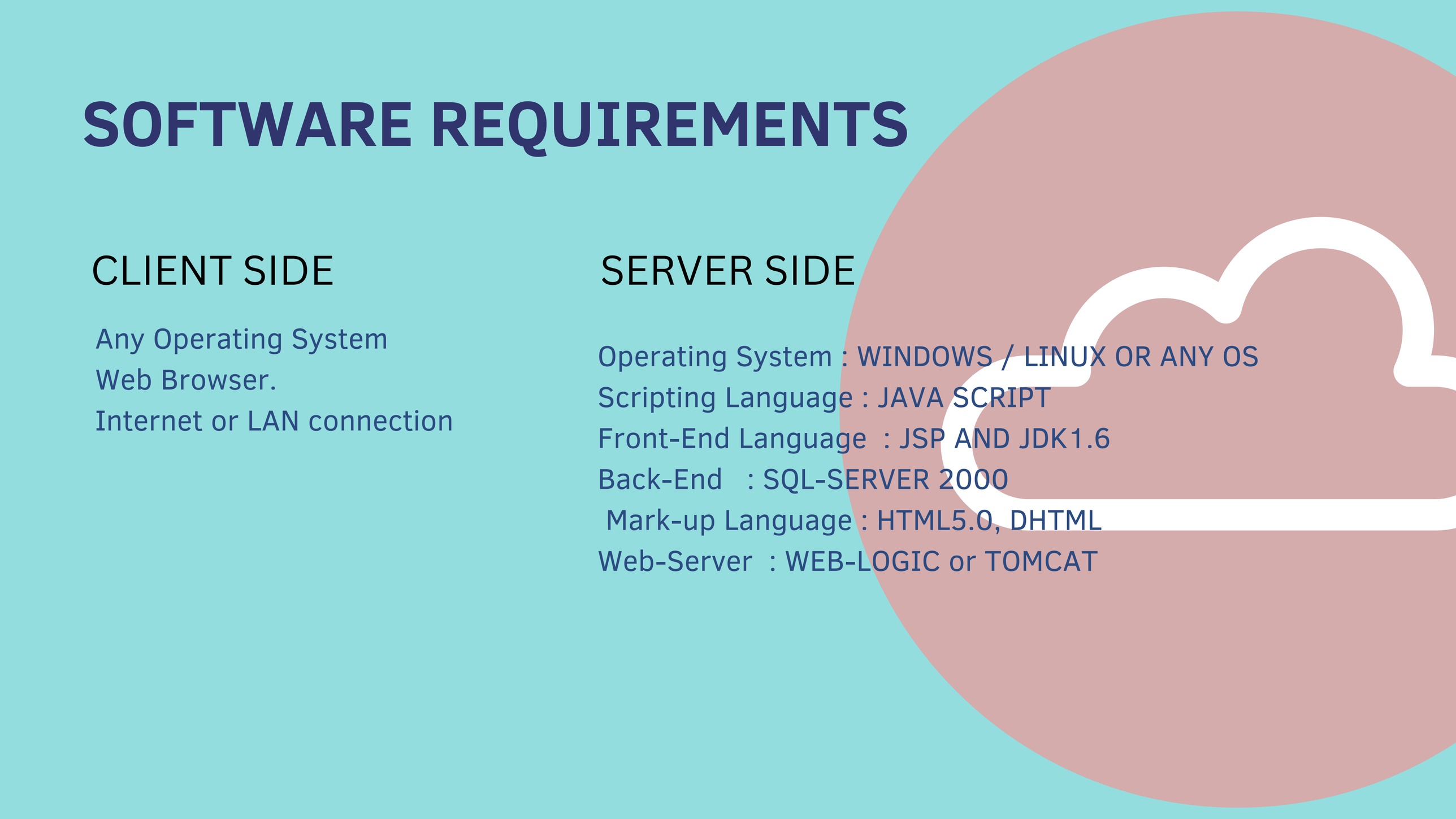
SOFTWARE REQUIREMENTS

CLIENT SIDE

Any Operating System
Web Browser.
Internet or LAN connection

SERVER SIDE

Operating System : WINDOWS / LINUX OR ANY OS
Scripting Language : JAVA SCRIPT
Front-End Language : JSP AND JDK1.6
Back-End : SQL-SERVER 2000
Mark-up Language : HTML5.0, DHTML
Web-Server : WEB-LOGIC or TOMCAT



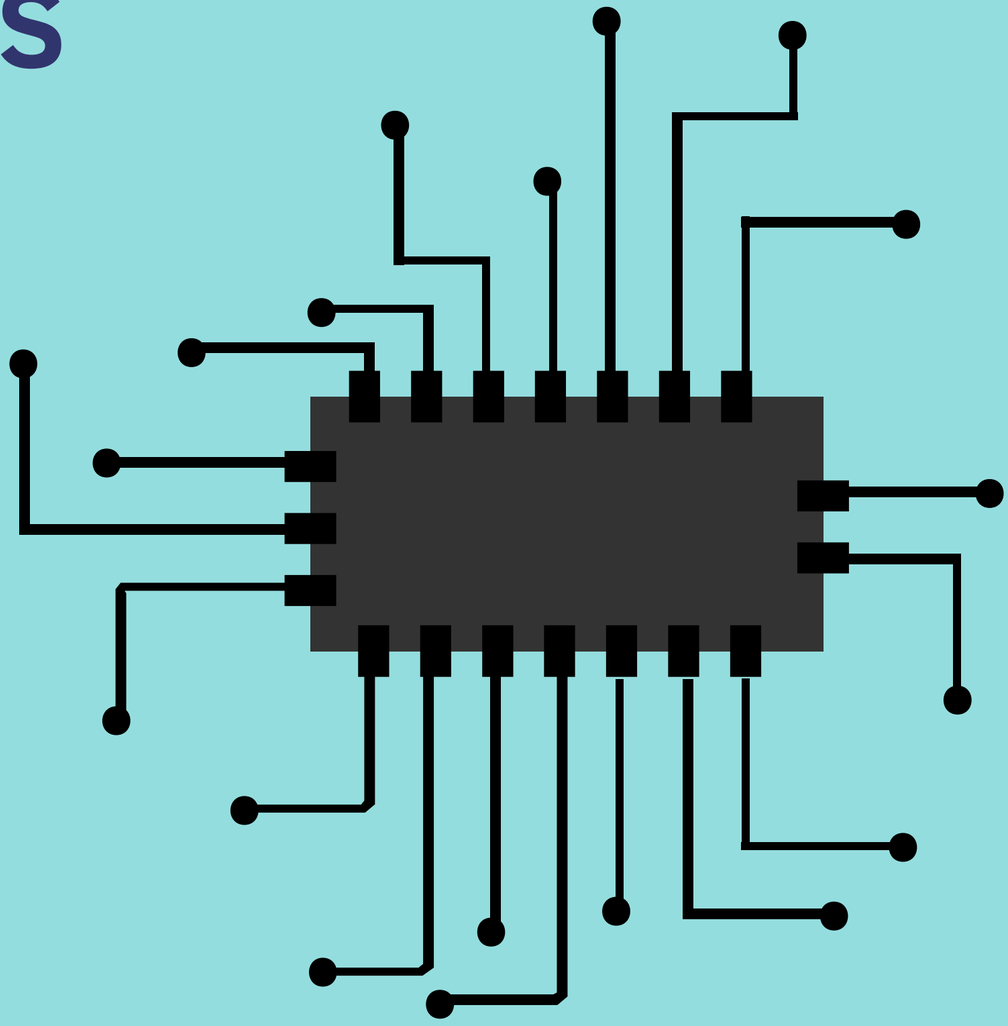
HARDWARE REQUIREMENTS

CLIENT SIDE

Processor : Pentium-4 or above
RAM : 1GB
Hard Disk : 160GB
Keyboard : Any
Mouse : Any

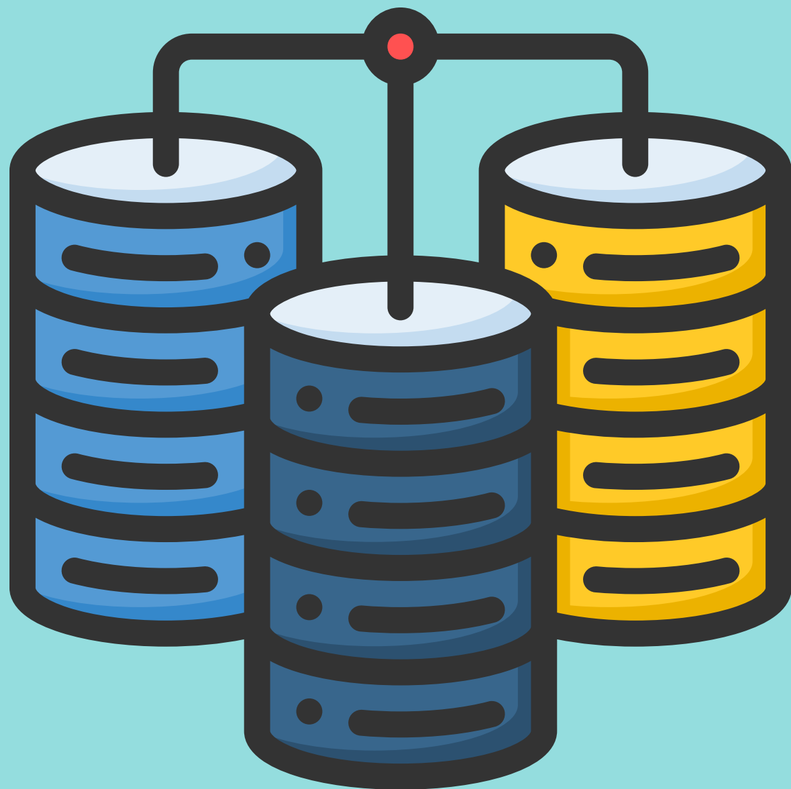
SERVER SIDE

Processor : Intel-C2D
RAM : 4 GB
Hard Disk : 500 GB
Keyboard : Any
Mouse : Any

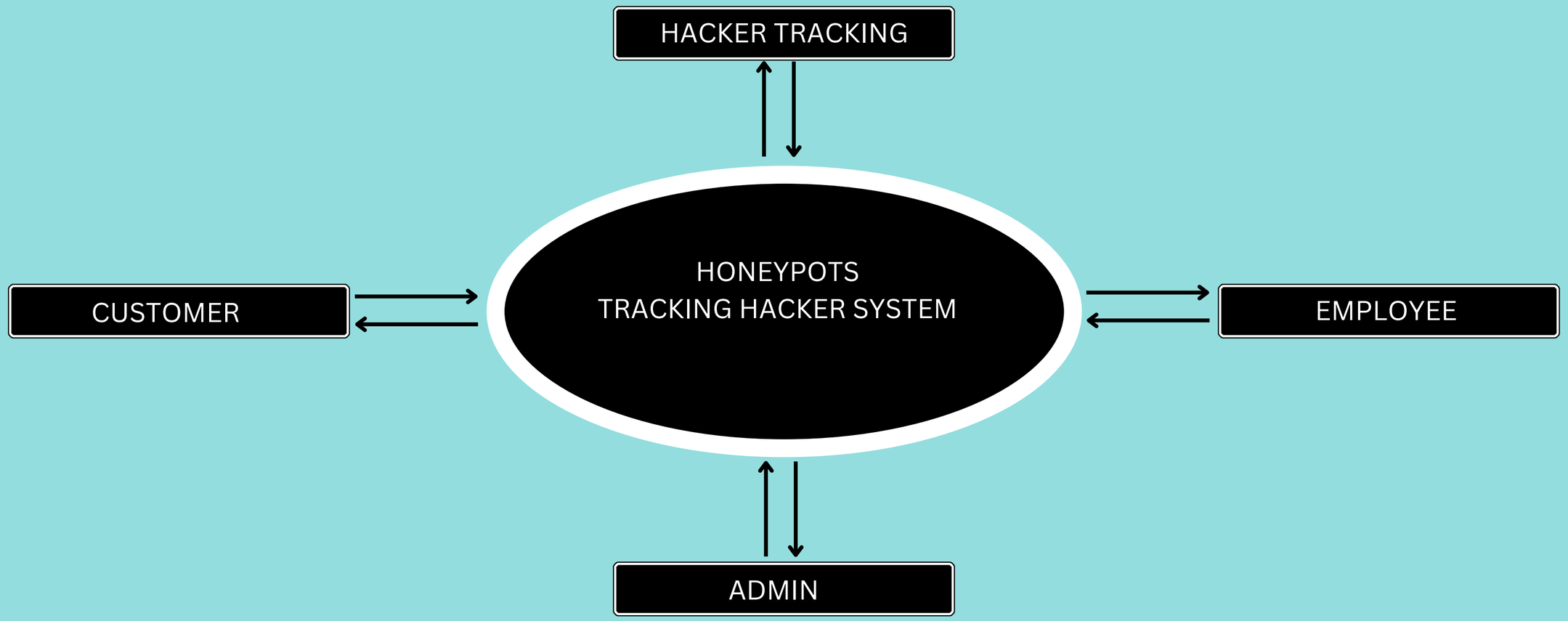


REQUIREMENT SPECIFICATION AND ANALYSIS

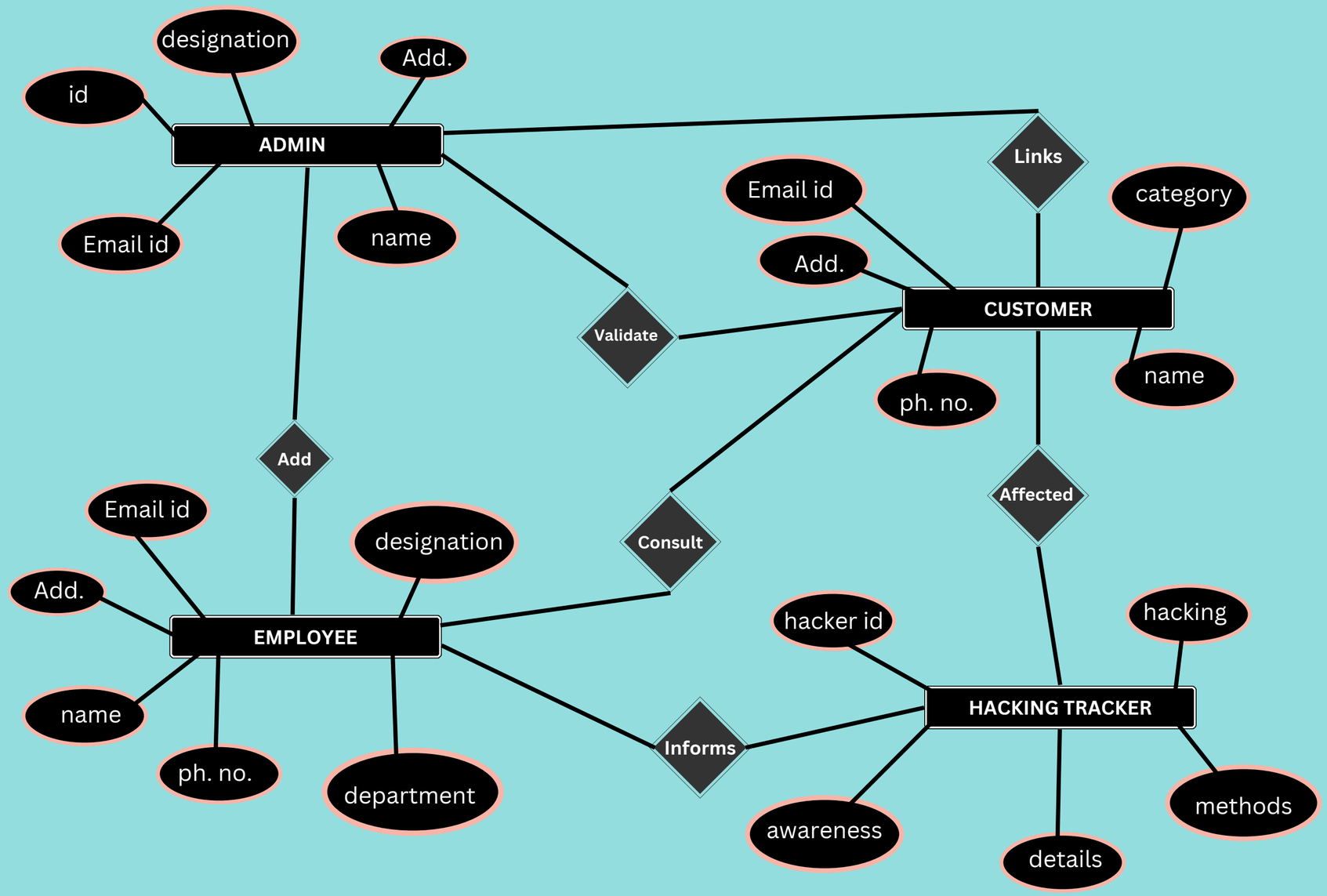
- The system must interface with SSH, HTTP, and HTTPS protocols
- The system will use a fake login page with key logger to record login attempts.
- The system will have the ability to record logs of all connection attempts.
- The system must contain a small intrusion detection system (IDS)



DATA FLOW DIAGRAM

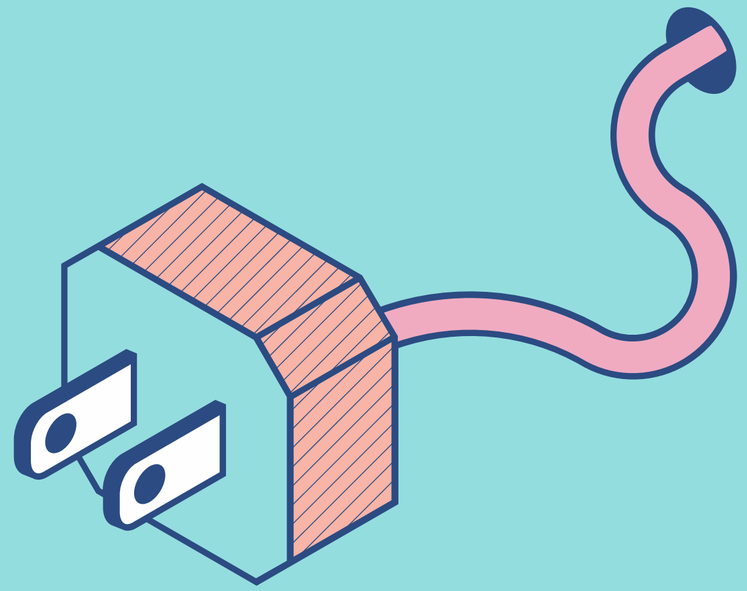


ER DIAGRAM

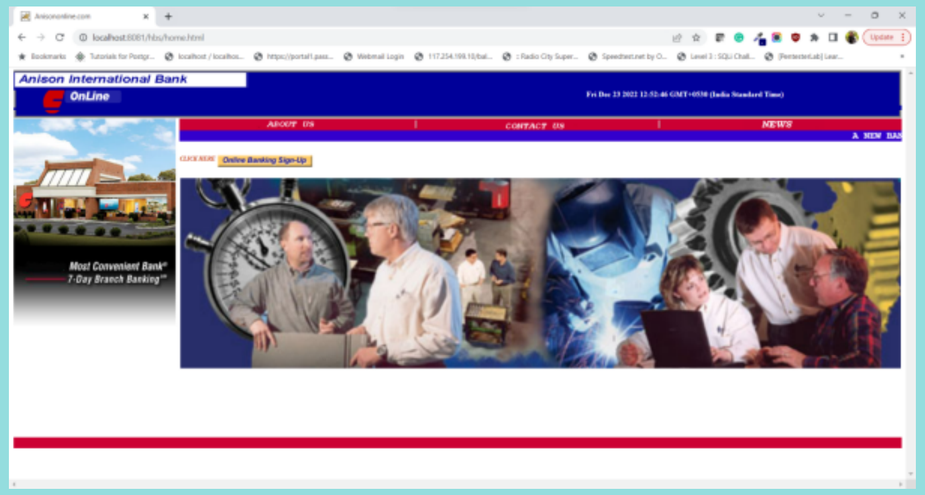

designation
Add.
id
ADMIN
Email id
name
Links
Email id
category
Add.
CUSTOMER
Validate
name
ph. no.
Add
Affected
Email id
designation
Consult
Add.
EMPLOYEE
hacker id
hacking
name
HACKING TRACKER
Informs
ph. no.
department
awareness
details
methods

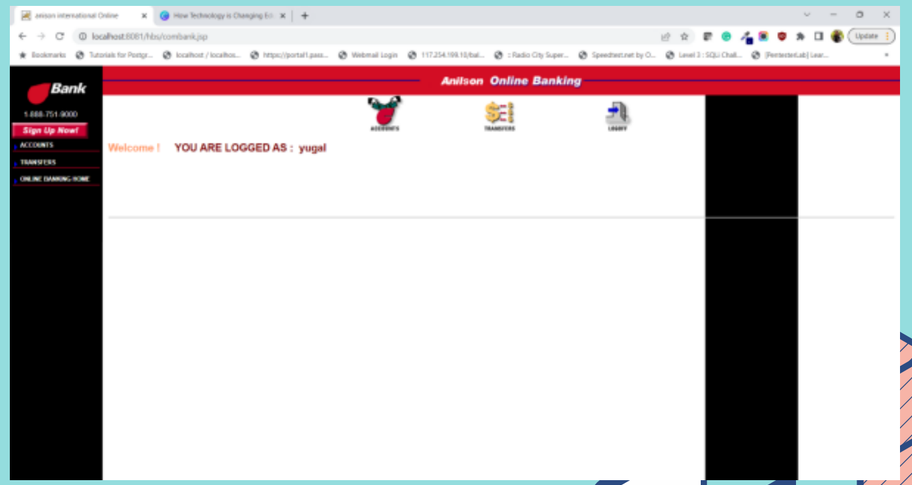
FEATURES

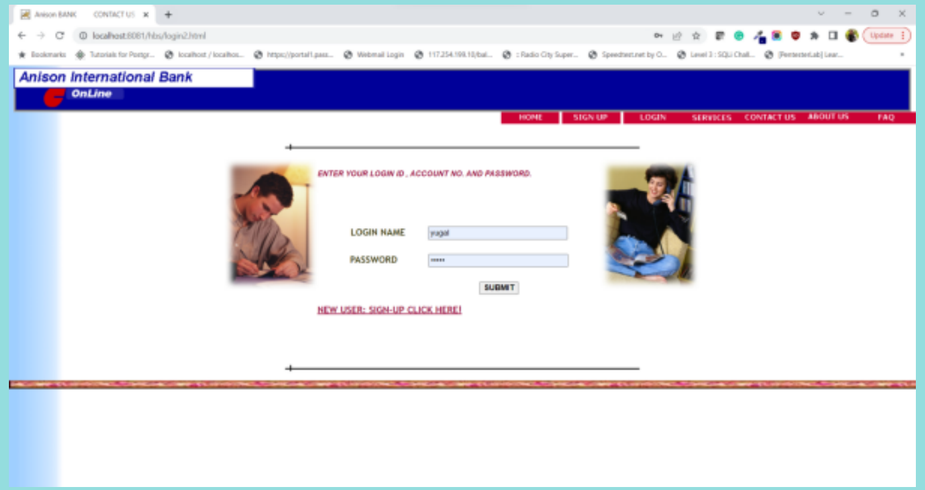
- Our project provides secure access of confidential data.
- It becomes Easy to manage the records.
- Provide managed authority control.
- Removes cost of consultation.
- Availability of data on a click.

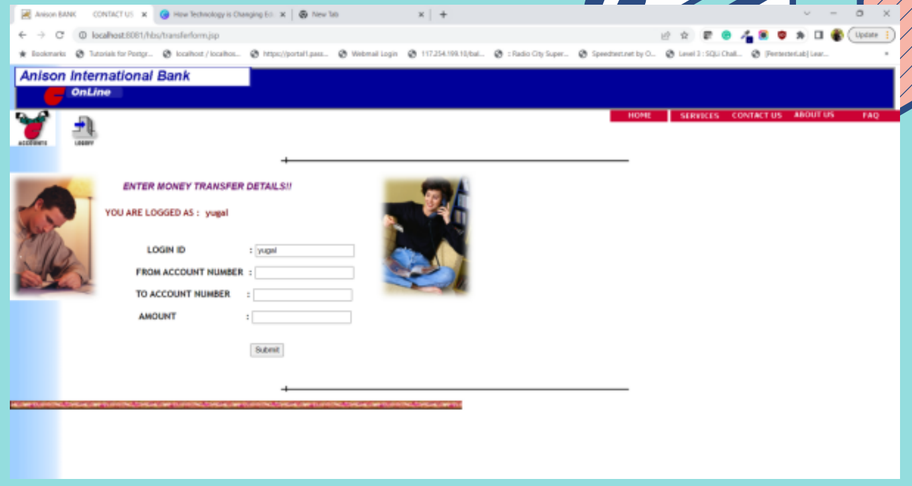


PROJECT SNAPSHOTS



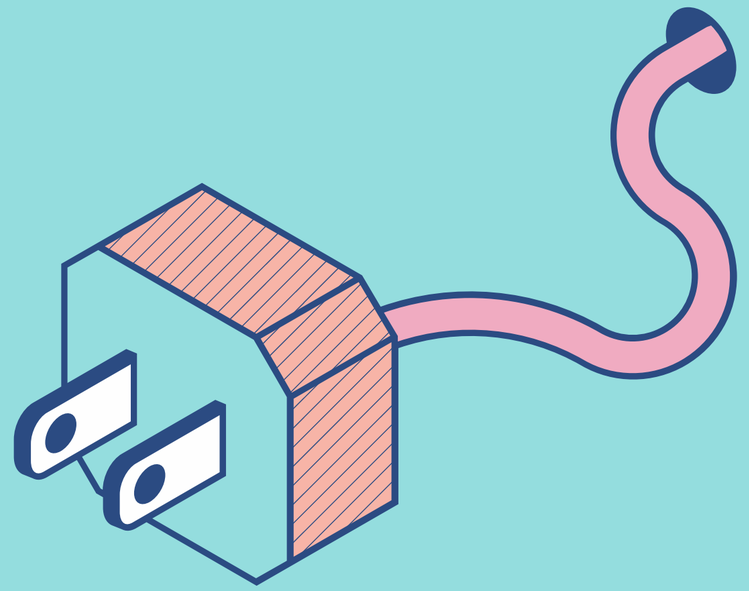






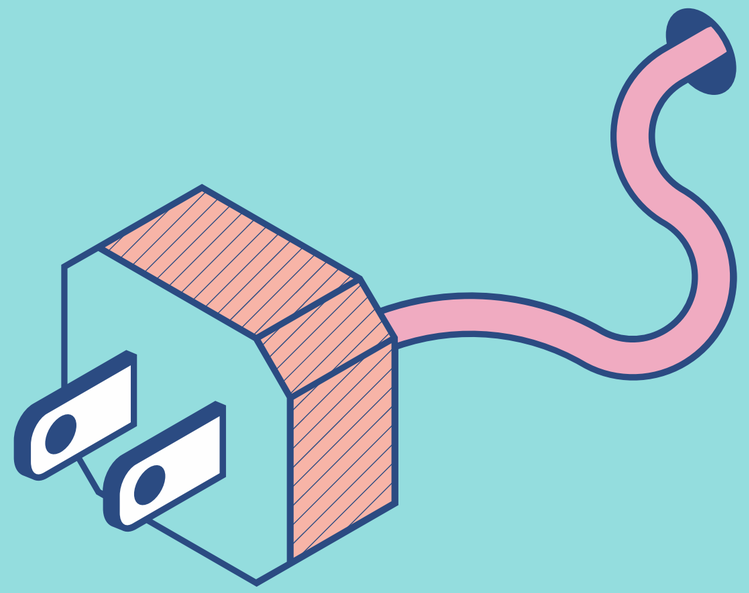
LIMITATIONS

- False Sense of Security.
- Resource Intensive.
- Legality and Ethics.
- Network Complexity.
- Maintenance and Updates.
- Potential Impact on Legitimate Users



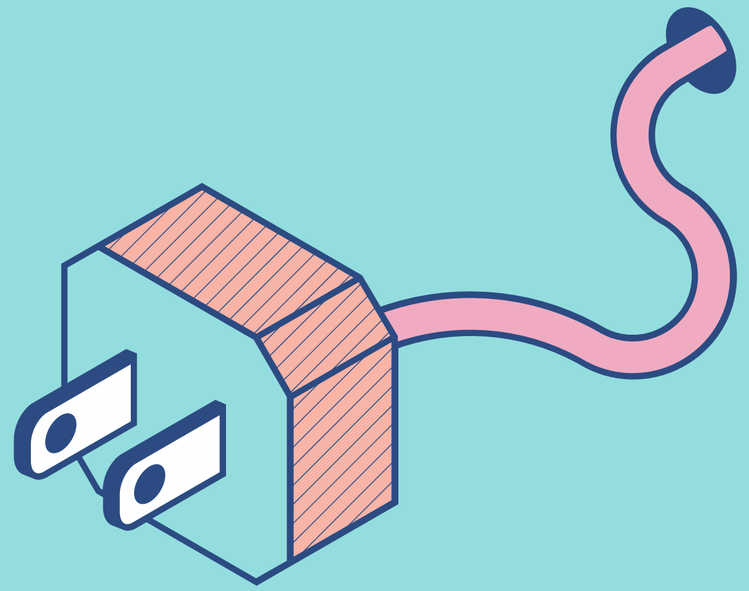
FUTURE SCOPE

- Advanced Threat Detection.
- Deception Technology.
- Internet of Things (IoT) Security.
- Threat Intelligence.
- Cloud-Based Honeypots.
- Machine Learning and Artificial Intelligence.
- Collaboration and Information Sharing.
- Industrial Control Systems (ICS) Security.



CONCLUSION

In conclusion, honeypots are an effective tool for tracking hackers and identifying potential security threats. By emulating vulnerable systems and services, honeypots can attract attackers and gather valuable information about their techniques, motivations, and objectives. This information can then be used to strengthen an organization's security posture, improve incident response, and develop proactive measures to prevent future attacks.



Literature Survey

Research Paper	Author, Year	Methodology
Honeypot for Cyber security Threat Intelligence	Ren Rui Tan, Simon Eng, Kiam Cheng How, Yongqing Zhu and Paul Wu Horng Jyh 2022	SME, Cybersecurity Threat Intelligence, Web Honeypot; Threat Intelligence Dashboard First Section
Honeypot Software and Data Analysis	Marcin Nawrocki, Matthias Wahlisch, Thomas C. Schmidt 2016	Extensive overview on honeypots. This includes not only honeypot software but also methodologies to analyse honeypot data.

REFERENCES

[1] Honeypot for Cybersecurity Threat Intelligence https://www.researchgate.net/publication/365300476_Honeypot_for_Cybersecurity_Threat_Intelligence, Aug 2022

[2] Honeypot: A Trap for Attackers https://ijarcce.com/upload/2017/march-17/IJARCCE%20197.pdf, Mar 2017

THANK YOU