



Gujarat Technological University Graduate School of Engineering and Technology

Report of an Online Research Talk “Investigate AI-based Cyber Security Research”

Date and Day: 11.03.2023, Saturday

Time: 4:00 PM to 6:00 PM

Mode: Online through GMeet

Coordinator: Dr. Seema B. Joshi, Asst. Professor (Cyber Security), GTU-GSET

Resource Person: Mr. Jaideep Kotak, Security Researcher, Ben-Gurion University, Israel.

About Expert Session:

M.E. Computer Engineering Department of GTU-GSET has organized an online research talk on “Investigate AI-based Cyber Security Research” on 11.03.2023. The session was delivered by one of the Alumnus of GTU Mr. Jaideep Kotak, Security Researcher, Ben-Gurion University, Israel.

Expert have covered various topics such as with demonstration:

1. Fundamentals of Machine Learning and Deep Learning
2. Various challenges of AI in Cyber Security Research
3. Cyber Security Domain Use Cases
4. Explainable Artificial Intelligence (XAI) and Adversarial Machine Learning
5. Research Scope in XAI and Adversarial ML

Objective of Research Talk:

The session was organized for the PG Scholars of Cyber Security Program with an objective to explore the AI-based cyber security research. To enhance the knowledge of ML/DL with cyber security domain use cases as well as to explore the various research scope in explainable AI and adversarial machine learning.

Glimpse of the research talk:

GUJARAT TECHNOLOGICAL UNIVERSITY
GRADUATE SCHOOL OF ENGINEERING AND TECHNOLOGY

Online Research Talk

INVESTIGATE AI-BASED CYBER SECURITY RESEARCH

Session Coordinator
 Prof. Seema B. Joshi

11th March 2023
 4:00 to 6:00 PM (IST)

MEETING ID
 meet.google.com/abf-kjqb-syi

Mr. Jaideep Kotak
 Security Researcher,
 Ben-Gurion University, Israel

NAAC Accredited A+ Grade

meet.google.com/abf-kjqb-syi?authuser=0&pli=1

Jaidip Kotak is presenting

Preprocessing/Feature Engineering

	A	B	C	D	E	F	G	H	I
1	Src_IP	Dst_IP	Src_Port	Dst_Port	TotalFram	Duration	Fwd_pkt	Bwd_pkt	Total_pkts
2	192.168.1.104	114.2	43469	443	6641	0.074241	15	11	26
3	192.168.1.104	114.21	56260	80	26057	376.3281	23	27	50
4	192.168.1.104	154.4	33883	443	6833	709.6207	27	31	58
5	192.168.1.104	154.4	34912	443	4469	123.2654	13	17	30
6	192.168.1.104	154.4	36504	443	4372	122.1841	13	16	29
7	192.168.1.104	154.4	38631	443	4452	122.2726	13	15	28
8	192.168.1.104	154.4	38747	443	4452	122.6895	13	15	28
9	192.168.1.104	154.4	41578	443	4143	122.232	12	14	26
10	192.168.1.104	154.4	42724	443	4415	123.2564	13	16	29


4:32 PM | Research Talk on "Investigate AI-based Cyber Secu..."

Participants: Jaidip Kotak, Parth Mistri, Bhavini Patel, Krishani Bhavsar, Janvi Raj, rohullah afzali, 19 others, You

Jaidip Kotak is presenting


Challenges

THE REALITIES OF APPLYING MACHINE LEARNING IN CYBER SECURITY ARE... COMPLICATED




BENIGN NETWORK ACTIVITY IS ALMOST NEVER NORMAL

Finding anomalous activity requires an understanding of what is normal, and network traffic is almost never normal




ADVERSARIES AND THEIR TACTICS ARE MOVING TARGETS

Machine learning assumes future data follow the patterns of past data, but networks and adversaries constantly change



EVERY FALSE POSITIVE COSTS TIME AND MONEY

False positives require analysts to examine an alert only to determine it was triggered by benign activity



INSIGHTS MUST BE BOTH ACCURATE AND ACTIONABLE

SOC operators need to know why a detection occurred, and black-box models can't provide that

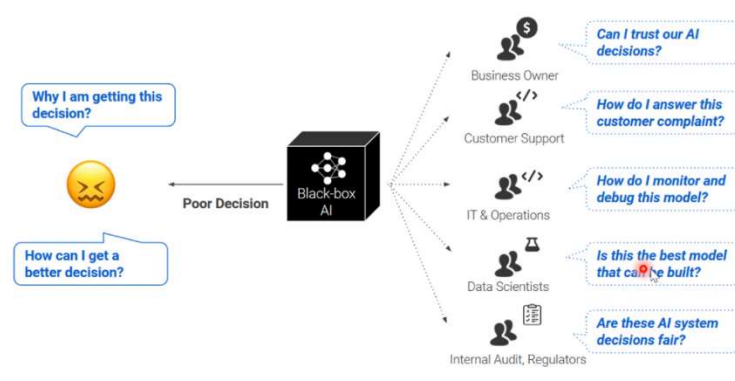
4:35 PM | Research Talk on "Investigate AI-based Cyber Secu..."

Video call participants:

- Jaidip Kotak
- Parth Mistri
- Bhavini Patel
- Krishani Bhavsar
- Janvi Raj
- rohullah afzali
- 19 others
- You

Jaidip Kotak is presenting

Black-box AI creates confusion and doubt



4:54 PM | Research Talk on "Investigate AI-based Cyber Secu..."

Video call participants:

- Jaidip Kotak
- Parth Mistri
- Bhavini Patel
- Vaibhav K Patel
- Maresh Parmar
- rohullah afzali
- 18 others
- You

Gujarat Technological University				
Graduate School of Engineering & Technology				
ME CE (Cyber Security), Semester-2 and 4, AY-2022-23				
Online Research Talk on "Investigate AI-based Cyber Security Research" Dt-11.3.2023, 4:00 to 6:00 PM				
Student Attendance Sheet				
Sr No.	Enrollment No.	Student Name	Semester	Attendance
1	221370759001	BHALALA RONAIBHAI BHARATBHAI	2	Present
2	221370759002	CHAUHAN BRIJESH HANUMANTSINGH	2	Present
3	221370759003	DESAI PRIYAL DHARMESHBHAI	2	Absent
4	221370759004	GALATHARIYA DHARMIKBHAI TRIBHOVANBHAI	2	Absent
5	221370759005	JAGANI DEVIK UMESHBHAI	2	Absent
6	221370759007	MISTRI PARTH RAJESHKUMAR	2	Present
7	221370759008	NAIR RENJINI THULASEEDHARAN	2	Present
8	221370759009	OZA NEEL MANISHKUMAR	2	Present
9	221370759010	PARMAR HIMANIBEN SANJAYKUMAR	2	Absent
10	221370759011	PATEL ABHISHEK PARESHBHAI	2	Absent
11	221370759012	PATEL BHAVINIBAHEN ASHVINBHAI	2	Present
12	221370759013	PATEL DARSH KISHORE	2	Absent
13	221370759014	PATEL MIRAL RAJESHBHAI	2	Present
14	221370759015	PATEL NANDINEE JATINKUMAR	2	Present
15	221370759016	PRANAV PATEL	2	Present
16	221370759017	RAJ JANVI SURESHBHAI	2	Present
17	221370759018	ROHITA REGUNATHAN WARRIER	2	Present
18	221370759019	SAHU GAINDRAM TILAKRAM	2	Absent
19	221370759020	TANK NISHITA CHETANBHAI	2	Absent
20	221370759021	YADAV ANURAG RAMESHKUMAR	2	Absent

21	221370759022	MALICK GAI	2	Absent
22	221370759023	AFZALI MOHAMMAD ALI	2	Present
23	211370759001	MENDAPARA JASHKUMAR MUKESHKUMAR	4	Absent
24	211370759002	LALWANI ASHIMA HARESH	4	Absent
25	211370759003	RAJPUT DIKSHASINGH HIRENDRASINGH	4	Absent
26	211370759004	PATEL BHUMI MUKESHBHAI	4	Present
27	211370759005	BHATEVARA NIHARIKA DEVENDRAKUMAR	4	Present
28	211370759006	PATEL PINAL DILIPKUMAR	4	Absent
29	211370759008	PARMAR ASHASRI ANANDKUMAR	4	Absent
30	211370759009	PARMAR MAHESHKUMAR KUBERBHAI	4	Present
31	211370759010	SURYADEEPSINH	4	Absent
32	211370759011	PATEL JAY BABUBHAI	4	Present
33	211370759012	PATEL KATHAN RAJESHBHAI	4	Absent
34	211370759013	RATHAVA PRITIBEN JANAKBHAI	4	Absent
35	211370759014	PATEL VAIBHAVKUMAR KISHORBHAI	4	Present
36	211370759015	SHILPABEN SODVADIYA	4	Absent
37	211370759016	MEWADA POOJA NIRAVBHAI	4	Present
38	211370759018	AGRAWAL MILI NITESHKUMAR	4	Absent
39	211370759019	BHAVSAR KRISHANI AJITKUMAR	4	Present
40	211370759020	SATHWARA BRIJESHKUMAR YOGESHBHAI	4	Present
41	211370759021	PRAJAPATI RIDDHI BHAVESHKUMAR	4	Present
42	211370759022	RAJPUT VIDHI GORAKHNATH	4	Present
43	211370759023	BHARVAD BHARGAVBHAI BHOPABHAI	4	Present
44	211370759024	LOYA SAFIYA ILIYASBHAI	4	Present
45	211370759025	JYOTI SINGH	4	Present
46	211370759026	ASAD NUR ABDI	4	Present
47	211370759027	TRIVEDI JEEL MANOJKUMAR	4	Absent
48	211370759028	ZAKARIYE OSMAN ABDULLAHI	4	Present