BYTE QUEST

Vasavi College of Engineering

Department of Computer Science and Engineering

March 30th, 2020
Volume 82

Contents:

Byte Quest is the article published by the CSE dept of Vasavi College of Engineering regarding the latest innovative Technologies and Software that have been emerged in the competitive world. The motto of this article is to update the people regarding the improvement in technology. The article is designed by the active participation of students under the guidance of faculty coordinators.

 Good, bad or indifferent if you are not investing in new technology, you are going to be left behind.

-Philip Green

 Once a new technology rolls over you, if you’re not part of the steamroller, you’re part of the road.

-Stewart Brand

FACULTY CO-ORDINATORS

K B BINI (ASST. PROFESSOR)

KOMAL KAUR (ASST. PROFESSOR)

STUDENT COORDINATORS

CAROL (4/4 CSE-A)	D.APARNA (4/4 CSE-B)
ABHINAV (3/4 CSE-A)	K.ANISHA (3/4 CSE-B)
AKASH VORA (2/4 CSE-C)	IMRAN (2/4 CSE-A)

HOME WIRELESS SECURITY

In the digital era, when cyber-attacks are increasing day by day, ensuring home wireless security plays an important role in maintaining one’s own privacy. To ensure Home wireless security, certain steps Can be followed.

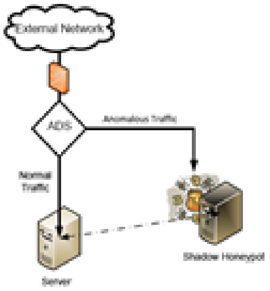
One of the best practices is to Change the Name (SSID) and Password of your default home network. Also, one can increase wi-fi security by activating network encryption. Using a strong network administrator password to increase Wi-Fi security is also of great help in ensuring home wireless security. To set up your wireless router, you usually need to access an online platform or site, where you can make several changes to your network settings. Most Wi-Fi routers come with default credentials such as “admin” and “password” which are such an easy for malicious hackers to break into. One can ensure that their wi-fi is secure by following all these measures.

P.GAUTHAM(3/4 CSE- B)

HONEYPOT

Global communication is getting more important every day. At the same time, computer crimes are increasing. Counter measures are developed to detect or prevent attacks most of these measures are based on known facts, known attack patterns. It is important to know, what kind of strategy an attacker uses, what tools he utilizes and his intention. By knowing attack strategies, counter measures can be improved and vulnerabilities can be fixed. To gather such information is one main goal of a honeypot. A honeypot is primarily an instrument for information gathering and learning. Its purpose is not to be an ambush for the black hat community to catch them in action.

Honeypots only collect data when someone or something is interacting with them. Organizations that may log thousands of alerts a day may only log a hundred alerts with honeypots. This makes the data honeypots collect much easier to manage and analyse. Honeypots are a new field in the sector of network security.

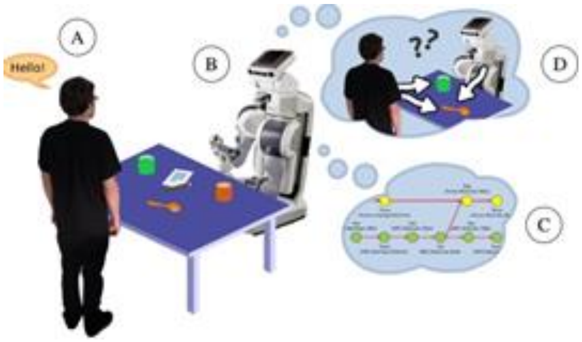


G.MEGHANA (3/4CSE-B)

ARTIFICIAL COGNITION FOR HUMAN ROBOT INTERACTION

Human–Robot Interaction represents a challenge for Artificial Intelligence (AI). It lays at the crossroad of many subdomains of AI and, in effect, it calls for their integration: modelling humans and human cognition. Many AI techniques are mandated, from visual processing to symbolic reasoning, from task planning to theory of mind building, from reactive control to action recognition and learning.

We do not claim to address here the issue as a whole. This article attempts however to organise it into a coherent challenge for Artificial Intelligence, and to explain and illustrate some of the paths that we have investigated the robots, that result in a set of deliberative, knowledge-oriented, software components designed for human–robot interaction.



We focus on a specific class of interactions: human–robot collaborative task achievement supported by multi-modal and situated communication. Figure illustrates this context: the human and the robot share a common space and exchange information through multiple modalities (we specifically consider verbal communication, deictic gestures and social gaze), and the robot is expected to achieve interactive object manipulation, fetch and carry tasks and other similar chores by taking into account, at every stage, the intentions, beliefs, perspectives, skills of its human partner. Namely, the robot must be able to recognise, understand and participate in communication situations, both explicit (e.g. the human addresses verbally the robot) and implicit (e.g. the human points to an object); the robot must be able to take part in joint actions, both pro-actively (by planning and proposing resulting plans to the human) and reactively; the robot must be able to move and act in a safe, efficient and legible way, taking into account social rules like proxemics.

PREETHAM REDDY (3/4 CSE-B)