

Popular research projects on IoT devices in Qatar are illustrated below.

1) **An Intelligent Car Monitoring system** is developed by Jabbar et.al [6] in collaboration with Qatar Foundation and Qatar University, for road safety and traffic control in Qatar. The model is based on the naturalistic driver behavior using existing traffic monitoring systems. The authors have used Deep Learning and Neural

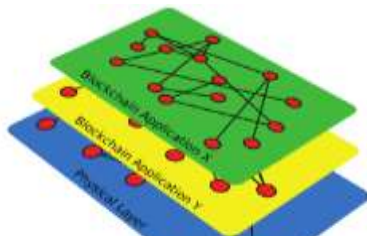


Figure 3 Hierarchical structure of attributes.

Networks to collect and analyze data to provide dynamic information about road conditions, high and low risk locations.



Figure 2 Intelligent Car Monitoring system

## 2) Context aware

**name discovery for block chain based services in IoTs** was proposed by

Roberto Di et. al [7] from HBKU, to easily identify services in IoT devices using universal multi-layer blockchains. The model is based on the existing protocols and uses publicly available information from one block chain to gather meaningful knowledge from the environment.

3) **A Survey on IoTs, Protocols and Applications** by M. Guizani et. al, Qatar University [8]. This work summarizes the technologies, most relevant protocols, and security issues of Internet of Things (IoT). The fundamental concepts of architecture and building blocks are made clear in the beginning to comprehend further deep understanding of protocols. The working of the protocols at each layer is mentioned with graphs and clear illustration. Higher technical terms are used in simple English for the reader to gain insight into terminologies used in IoTs. The paper has covered large details on the standard protocols proposed by IETF, IEEE and EPCglobal. This article helps student and researchers to understand key IoT characteristics and elements without much effort to quick start new research in emerging areas like big data analytics, cloud fog computing.



Figure 4 Horizontal and Vertical market integration of IoTs

4) **A comprehensive survey on application of Deep Learning methods for IoT Security:** by Amr Mohamed et. al., Qatar University [9]. The work explores the issues and challenges in implementing the security measures, such as encryption, authentication, access control, network security and application security for the IoT devices. It highlights how intelligent techniques can be used to enhance the security. The research suggests that intelligent monitoring provides a significant solution to new or zero-day attacks. ML/DL are the robust methods for data exploration, management and for learning 'normal' and 'abnormal' behavior of the network. The authors have enlisted all the recent work done in IoT security using ML/ DL, providing limitations and advantages of each method to trigger new direction of research and implementation of IOT security.