BYTE QUEST

Vasavi College of Engineering

Department of Computer Science and Engineering

September 15, 2017
Volume 43

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

T.NISHITHA(ASST. PROFESSOR)

M.SUNDARI(ASST. PROFESSOR)

STUDENT COORDINATORS

M. ADARSH (4/4 CSE-A)	RAHUL (4/4 CSE-B)
NIKITHA (3/4 CSE-A)	ABHINAV (3/4 CSE-B)
ESHWAR (2/4 CES-A)	SREEJA(2/4 CSE-B)

SPY TECHNOLOGIES

Spying is the act of obtaining secret or confidential information without the permission of the holder of the information.

Spy-Fi can be defined as media that centres around the adventures of a protagonist working as a secret agent or a spy. The spy protagonist may discover in his or her investigation that a mad scientist or evil genius and his secret organization are using futuristic technology to further their schemes.

Surveillance is the monitoring of behaviour, activities, or other changing information for the purpose of influencing, managing, directing, or protecting people.

Support:

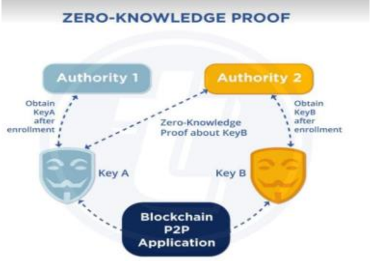
Supporters of surveillance systems believe that these tools can help protect society from terrorists and criminals. They argue that surveillance can reduce crime by three means: by deterrence, by observation, and by reconstruction.

Opposition:

In December 2017, the Government of China took steps to oppose widespread surveillance by security-company cameras, webcams, and IP Cameras after tens-of-thousands were made accessible for internet viewing by IT company Qihoo.

B. CHANDANA REDDY (CSE-B 2/4)

ZERO KNOWLEDGE PROOF

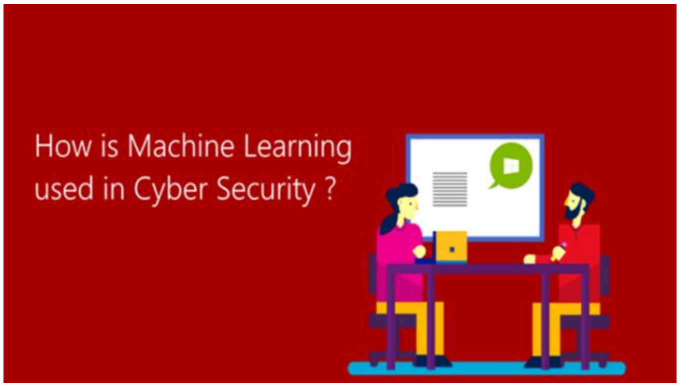

ZERO-KNOWLEDGE PROOF
Authority 1
Authority 2
Obtain KeyA after enrollment
Zero-Knowledge Proof about KeyB
Obtain KeyB after enrollment
Key A
Key B
Blockchain P2P Application

All new technologies, platforms and services gobble up massive amounts of data and more often than not, this data is not very well protected. Fortunately, there is a way to protect privacy. With the hype around blockchain, start-ups are also working on a new technology called Zero Knowledge Proof (ZKP). Zero Knowledge Protocol (or Zero Knowledge Password Proof, ZKP) is a way of doing authentication where no passwords are exchanged, which means they cannot be stolen. nobody else can find out what you're communicating about or what files you are sharing. ZKP allows you proving that you know some secret (or many secrets) to somebody at the other "end" of communication without actually revealing it. The very term "zero knowledge" originates from the fact that no ("zero") information about the secret is revealed, but the second party (called "Verifier") is (rightfully) convinced that the first party (called "Prover") knows the secret in question. Why would you need to prove you know the secret without telling it? When you don't trust the other person, but still need to persuade them that you know it.

AYUSH NOEL (CSE-B 2/4)

MACHINE LEARNING AND DEEP LEARNING METHODS FOR CYBERSECURITY

With the increasingly in-depth integration of the Internet and social life, the Internet is changing how people learn and work, but it also exposes us to increasingly serious security threats. A network security system consists of a network security system and a computer security system. Each of these systems includes firewalls, antivirus software, and intrusion detection systems (IDS). There are three main types of network analysis for IDSs: misuse-based, also known as signature-based, anomaly-based, and hybrid. Misuse-based detection techniques aim to detect known attacks by using the signatures of these attacks. New (zero-day) attacks cannot be detected based on misused technologies. Anomaly-based techniques study the normal network and system behaviour and identify anomalies as deviations from normal behaviour. This article presents a literature review of machine learning (ML) and deep learning (DL) methods for cybersecurity applications. ML/DL methods and some applications of each method in network intrusion detection are described. It focuses on ML and DL technologies for network security, ML/DL methods and their descriptions. The research aims on standards-compliant publications that use ‘‘machine learning’’, ‘‘deep learning’’ and cyber as keywords to search on Google Scholar. In particular, the new hot papers are used because they describe the popular techniques. The purpose of this article is for those who want to study network intrusion detection in ML/DL.



Thus, great emphasis is placed on a thorough description of the ML/DL methods, and references to seminal works for each ML and DL method are provided. Examples are provided concerning how the techniques were used in cyber security. This article does not describe all of the different techniques of network anomaly detection; instead, it concentrates only on ML and DL techniques. However, in addition to anomaly detection, signature-based and hybrid methods are depicted. Patch and Park [5] discuss technological trends in anomaly detection and identify open problems and challenges in anomaly detection systems and hybrid intrusion detection systems. However, their survey only covers papers published from 2002 to 2006, whereas this article includes more recent papers. This also covers the application of ML/DL in various areas of intrusion detection and is not limited to cloud security.

CH.ABHILASH (CSE-B 2/4)