BYTE QUEST

Vasavi College Of Engineering

Department Of Computer Science and Engineering

March 15, 2016

Volume 19

CONTENTS

- ♦ AUGMENTED REALITY

- ♦ SMARTPHONE WITH SCREEN ALWAYS ON

- ♦ HACK-PROOF RFID CHIPS

.

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 COORDINATORS
DIVYA (ASST. PROFESSOR)
T.NISHITHA (ASST. PROFESSOR)

STUDENT COORDINATORS	
R NIKITHA(4/4 CSE-A)	K ABHINAY(4/4 CSE-B)
AMREEN KOUSAR(3/4 CSE-A)	KRISHNA CHAITHANYA(3/4 CSE-B)
T AISHWARYA(2/4 CSE-A)	RAHUL(2/4 CSE-B)

AUGMENTED REALITY

The emerging augmented reality technology superimposes computer-generated images on the real world, courtesy of a cell phone camera or special video glasses. With AR you might aim a phone's camera at a restaurant, and on the screen you'll see not just the venue but also a review hovering above it.

The U.S. Marine Corps is testing AR technology. They don headgear that projects animated 3-D computer graphics onto the equipment under repair, labeling parts and giving step-by-step guidance.

Early adopters can test out the world's first AR glasses from Vuzix. They look like wraparound sunglasses, except you can't see directly through the lenses. Instead, small cameras centered on the outside of each lens feed continuous video through a mobile computer to an LCD screen

mounted inside each lens. The price for the glasses with cameras is about $600.

The next stage in the evolution of AR is taking shape in the lab of Babak Parviz who has made a contact lens etched with a tiny, transparent electronic circuit that contains a single LED which might allow it to display text and images that would appear to hover in space at a readable distance in front of the eye.

- I.Amulya Sai (CSE-A 2/4)

SMARTPHONES WITH SCREEN ALWAYS ON
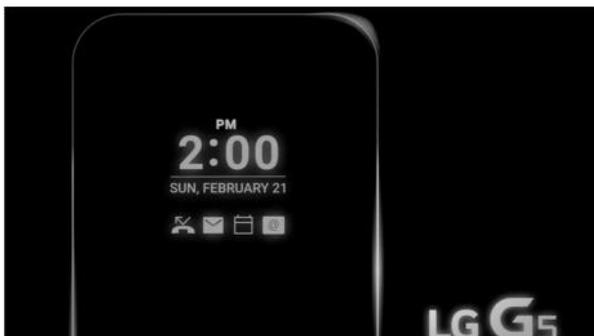
Constantly turning on phone's screen to check the time or for missed calls, new texts or recent social-media interactions not only takes time, but also drains your battery. So, the two new devices coming to market soon look to address this issue. Smartphone maker LG's soon-to-be-released G5 and Samsung's upcoming G7 will introduce an "Always ON" display feature, in which the time, date and

notifications will remain visible on a darkened screen and the company has filed to trademark the phrase "Always on Display.". Engadget points out that the G5 will supposedly be operating the always-on feature as a full-screen version of the LG V10's smaller second screen, with icons arranged in a line at the top of the screen. It also suggests that Samsung is using more powerful batteries in the Galaxy S7 model to ensure that standby time won't be too affected by the change.The G5 is expected to hit the market on Feb. 21, the same day Samsung will release more details about the Galaxy S7.

- Navya (CSE-B 4/4)

HACK-PROOF RFID CHIPS

Researchers at MIT and Texas Instruments have developed a new type of radio frequency identification (RFID) chip that is virtually impossible to hack.

According to a graduate student at MIT, the chip is designed to prevent so-called side-channel attacks which analyze patterns of memory access or fluctuations in power usage when a device is performing a cryptographic operation.

The RFID chip would run a random-number generator that would spit out a new secret key after each transaction. A central server would run the same generator, and every time an RFID scanner queried the tag, it would relay the results to the server, to see if the current key was valid.

Such a system would still be vulnerable to a "power glitch" attack i.e., the RFID chip's power would be repeatedly cut right before it changed its secret key. Two design innovations allow the MIT researchers' chip to thwart power-glitch attacks: One is an on-chip power supply whose connection to the chip circuitry
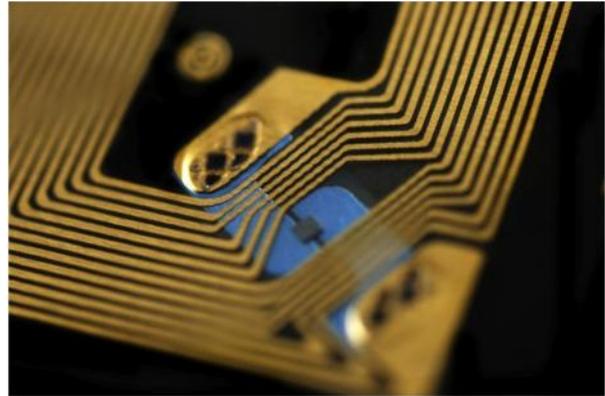
would be virtually impossible to cut, and the other is a set of "nonvolatile" memory cells that can store whatever data the chip is working on when it begins to lose power.

Both of these features use a special type of material known as a ferroelectric crystals. A ferroelectric crystal can also be thought of as a capacitor, an electrical component that separates charges and is characterized by the voltage between its negative and positive poles. This research is an important step toward the goal of a robust, low-cost, low-power authentication protocol for the industrial Internet.

- Afifa Iram (CSE-B 2/4)