VOL. : 2 ISSUE : 7
November 2017

PANIPAT INSTITUTE OF ENGINEERING & TECHNOLOGY

Approved by: A.I.C.T.E, New Delhi & Affiliated to Kurukshetra University, Kurukshetra

NEWSLETTER

Volume : 2

Issue : 7

PIET
PANIPAT INSTITUTE
OF ENGINEERING & TECHNOLOGY
(Approved by AICTE & Affiliated to Kurukshetra University, Kurukshetra)

VISION

Department of Computer Science and Engineering aspires to be recognized universally as a promoter of computer technology and its applications and socially relevant research pursuits.

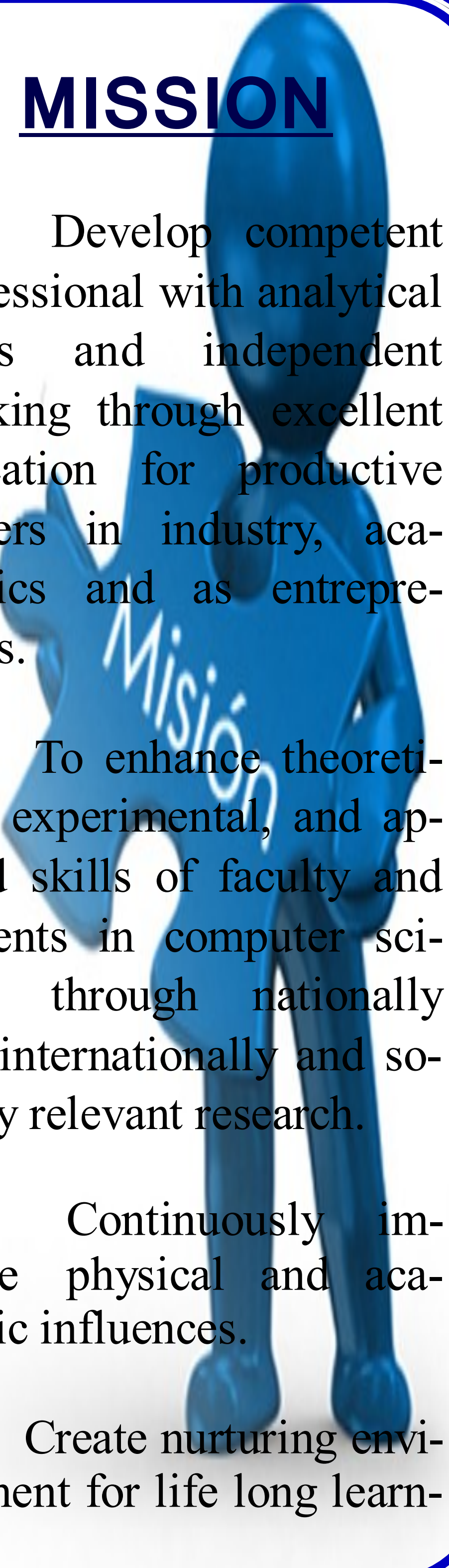
MISSION

M1. Develop competent professional with analytical skills and independent thinking through excellent education for productive careers in industry, academics and as entrepreneurs.

M2. To enhance theoretical, experimental, and applied skills of faculty and students in computer science through nationally and internationally and socially relevant research.

M3. Continuously improve physical and academic influences.

M4. Create nurturing environment for life long learn-



SNEAK PEEK

INSIDE TECHNOMEAL

FROM THE DESK OF CHAIRPERSON.......

The CSE team has been successfully upholding the traditions of the department which is evident from the efforts that have been made in publishing the newsletter.

Dr. S.C Gupta, Chairperson (CSE/IT)

FROM THE DESK OF HEAD OF DEPARTMENT....

I love to facilitate my students so that they can enhance & enrich their skill domains. I wish all the students and faculty a great academic career.

Dr.Vikram Bali, HOD (CSE)

VOL. : 2 ISSUE : 7

November 2017

TECHNOMEAL

FABRICATORS

FROM FACULTY EDITORS:-

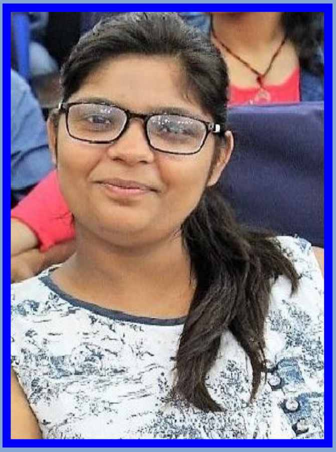
The content in this newsletter is in perfect blend of quality. It is an incredible platform for real, technical, managerial and social insight, hence perfect to convert a raw student into successful one.

AAKANSHA MAHAJAN , CSE

ASSISTANT PROFESSOR

RITU BANGA ,CSE

ASSISTANT PROFESSOR



VRINDA , CSE

ASSISTANT PROFESSOR

FROM STUDENT EDITOR :-

I would like to congratulate our department for a great month. Firstly I would like to thank all the people who have helped us in making the newsletter. It had been an amazing and new experience for me. This month was full of great things. Let's have a look towards them.

MOHIT ROHILLA

CSE , 2nd Year

TECHNATION

AS in PIET we believe in improvising quality and not in quantity, we believe in encouraging spirit of students and always finding ways to exhibit the same. So, we initiated an inter-department level event in our college in which all the departments participated and in which they proved their skills with their projects . There was an immense support under the supervision of the H.O.D of computer science dept, Dr. Vikram Bali and also under the umbrella of knowledge of Chairperson Dr. S.C Gupta . Also the worthy mentors appreciated the efforts of students. Students participated with a great zest and idea of innovation in TECHNATION.

INDUSTRIAL VISIT

Industrial visit has been carried out at MCN Solutions Pvt Ltd. In Nov 2017. This visit has its own importance in a career of a student who is pursuing a professional degree. Objectives of industrial visit is to provide students an insight regarding internal working of companies. Theoretical knowledge is not enough for making a good professional career. With an aim to go beyond academics, industrial visit provides student a practical perspective on the world of work. It provides students with an opportunity to learn practically through working methods and employment practices. It gives them exposure to current work practices as opposed to possibly theoretical knowledge being taught at college. Industrial visits provide an excellent opportunity to interact with industries and know more about industrial environment.

WPA2 Flaw Could Blow WiFi Systems Wide Open

A security flaw in WPA2, the security protocol for most modern WiFi systems, could allow an attacker to steal sensitive data including emails, credit card numbers and passwords, Researchers at Belgian university KU Leuven reported Monday.

Depending on the network configuration, the flaw also could allow an attacker to inject or manipulate information in the system -- for example, inject ransomware or other malware into websites being used.

The weakness is in the WiFi standard itself, not in any particular products or implementations, so this impacts just about any correct implementation of WPA2, explained Mathy VanHoef, a postdoc researcher in the university's imec-DistriNet Research Group, who together with Frank Piessens, a DistriNet professor, discovered the flaw.

Widespread Impact

A series of vulnerabilities were found in Android, Linux, Apple, Windows, OpenBSD, MediaTek, Linksys and other systems, the researchers said. In order to fix the problem, users need to update affected products as soon as patches become available.

The research will be presented at the ACM Conference on Computer and Communication Security, which will take place Oct. 30 to Nov. 3 in Dallas, and at the Black Hat Europe conference in December.

Microsoft released security updates a week ago, and customers who have Windows Update enabled or otherwise have applied the updates are protected.

As a proof of concept, the DistriNet researchers executed a key reinstallation attack (KRACK) against an Android smartphone, noting that Linux and Android 6.0 or higher were particularly vulnerable. Both operating systems can be tricked into reinstalling an all-zero encryption key.

Threat Responses

Users should install recommended updates from end device and network equipment manufacturers, Kevin Robinson, vice president of marketing at theWi-Fi Alliance.

The alliance has taken immediate steps to address the issue, and it now requires testing for the vulnerabilities within its global certification lab network. The alliance has provided a vulnerability detection tool for its members' use.

The vulnerabilities can be lumped into two categories, according to the International Consortium for the Advancement of Cybersecurity on the Internet. In one, attacks would affect wireless endpoints as "supplicants." In the other, attacks would affect wireless infrastructure devices as "authenticators."

Depending on the device configuration, exploiting these vulnerabilities could allow unauthenticated attackers to perform packet relay, decrypt wireless packets, and potentially forge or inject packets into a wireless network, ICASI said.

Members including A10 Networks, Amazon, Cisco Systems, IBM, Intel Corp., Juniper Networks, Microsoft, Oracle and VMWare were notified.

Fundamental flaws that impact all Web users, like KRACK, are "incredibly rare" but not unprecedented, said Rich Campagna, CEO of security firm Bitglass.

The Heartbleed vulnerability, which surfaced in 2014, is another example of a flaw that had widespread impact across the spectrum.

An attack exploiting the WPA2 flaw would require an adversary to be close to the target, noted Gaurav Banga, CEO of Balbix.

PLACEMENTS

PEARLS ADDED IN ROSARY OF PIET

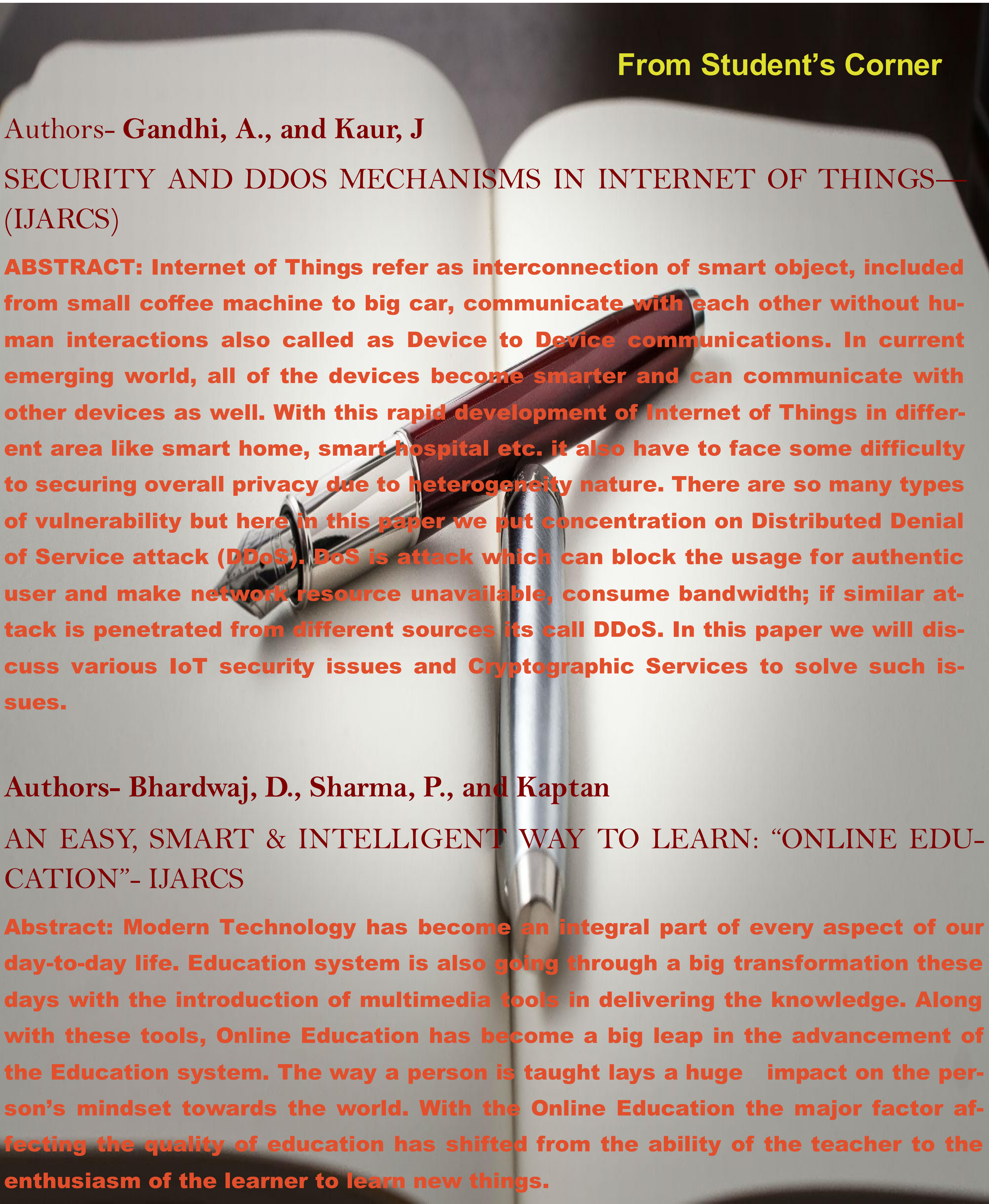
CAPGEMINI

Suraj Saluja
Shefali Garg
Rishabh Khurana
Paras Miglani
Ananya Verma
Saurabh Sakuja
Mughda
Anshul
Shubham Batra
Karanjot
Mohit Charaya
Isha
Neha

VOL. : 2 ISSUE : 7
November 2017

TECHNOMEAL

PUBLICATIONS



From Student's Corner

Authors- **Gandhi, A., and Kaur, J**

SECURITY AND DDOS MECHANISMS IN INTERNET OF THINGS— (IJARCS)

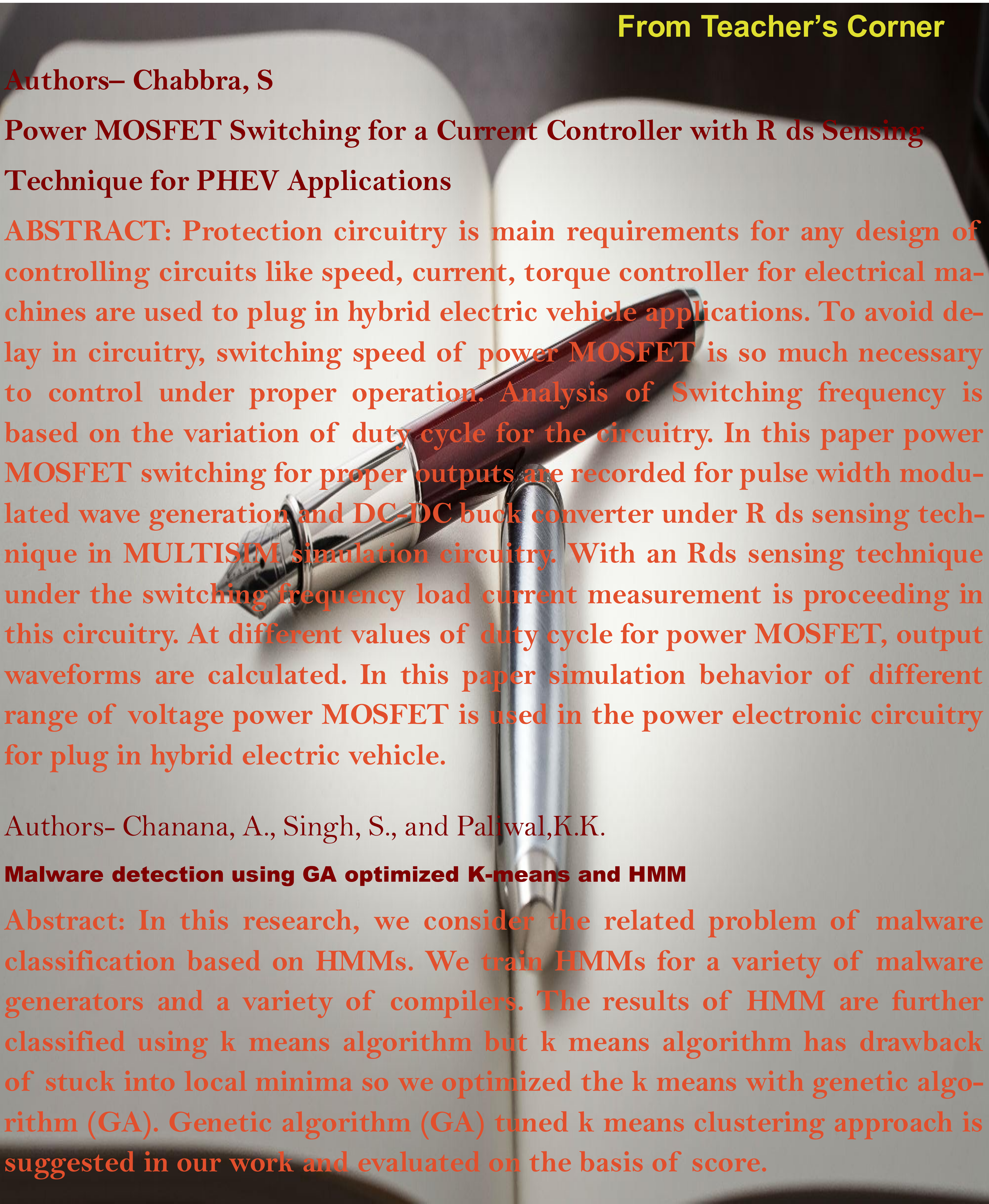
ABSTRACT: Internet of Things refer as interconnection of smart object, included from small coffee machine to big car, communicate with each other without human interactions also called as Device to Device communications. In current emerging world, all of the devices become smarter and can communicate with other devices as well. With this rapid development of Internet of Things in different area like smart home, smart hospital etc. it also have to face some difficulty to securing overall privacy due to heterogeneity nature. There are so many types of vulnerability but here in this paper we put concentration on Distributed Denial of Service attack (DDoS). DoS is attack which can block the usage for authentic user and make network resource unavailable, consume bandwidth; if similar attack is penetrated from different sources its call DDoS. In this paper we will discuss various IoT security issues and Cryptographic Services to solve such issues.

Authors- Bhardwaj, D., Sharma, P., and Kaptan

AN EASY, SMART & INTELLIGENT WAY TO LEARN: "ONLINE EDUCATION"- IJARCS

Abstract: Modern Technology has become an integral part of every aspect of our day-to-day life. Education system is also going through a big transformation these days with the introduction of multimedia tools in delivering the knowledge. Along with these tools, Online Education has become a big leap in the advancement of the Education system. The way a person is taught lays a huge impact on the person's mindset towards the world. With the Online Education the major factor affecting the quality of education has shifted from the ability of the teacher to the enthusiasm of the learner to learn new things.

PUBLICATIONS



From Teacher's Corner

Authors– Chabbra, S

Power MOSFET Switching for a Current Controller with R ds Sensing Technique for PHEV Applications

ABSTRACT: Protection circuitry is main requirements for any design of controlling circuits like speed, current, torque controller for electrical machines are used to plug in hybrid electric vehicle applications. To avoid delay in circuitry, switching speed of power MOSFET is so much necessary to control under proper operation. Analysis of Switching frequency is based on the variation of duty cycle for the circuitry. In this paper power MOSFET switching for proper outputs are recorded for pulse width modulated wave generation and DC-DC buck converter under R ds sensing technique in MULTISIM simulation circuitry. With an Rds sensing technique under the switching frequency load current measurement is proceeding in this circuitry. At different values of duty cycle for power MOSFET, output waveforms are calculated. In this paper simulation behavior of different range of voltage power MOSFET is used in the power electronic circuitry for plug in hybrid electric vehicle.

Authors- Chanana, A., Singh, S., and Paliwal,K.K.

Malware detection using GA optimized K-means and HMM

Abstract: In this research, we consider the related problem of malware classification based on HMMs. We train HMMs for a variety of malware generators and a variety of compilers. The results of HMM are further classified using k means algorithm but k means algorithm has drawback of stuck into local minima so we optimized the k means with genetic algorithm (GA). Genetic algorithm (GA) tuned k means clustering approach is suggested in our work and evaluated on the basis of score.