DGITechChronicle

DGI TECH CHRONICLE

SIT EDITION

Vol II Issue I (Jul -Dec 2021)

EDITORIAL BOARD

Dr. Aadarsh Malviya

Editor in Chief

In this issue, we delve into a captivating array of topics and developments, all tailored to the inquisitive minds of the future engineers. As an engineering college community, we stand at the forefront of technological breakthroughs, and it is our mission to empower you with the knowledge and insights to not only keep pace but to lead in this ever-accelerating race of innovation.

Ruhi Peter
13536(CSIT)

Co- Editor

Shivanshu Singh
13542(CSIT)

Editor- Design

Akshay Kumar
13493(CSIT)

Editor- Text

DGITechChronicle

C SIT EDITION

Department Vision and Mission

Department PEO, PSO and PO's

My Pen and Me: Students Articles

VISION

Promoting technologists by imparting profound knowledge in information technology, all while instilling ethics through specialized technical education.

MISSION

Delivering comprehensive knowledge in information technology, preparing technologists to excel in a rapidly evolving digital landscape.

Building a culture of honesty and responsibility in tech, promoting smart and ethical leadership.

Empowering individuals with specialized technical skills and ethical values to drive positive change and innovation in the tech industry.

Program Educational Objectives (PEO)

To enable graduates to think logically, pursue lifelong learning and will have the capacity to understand technical issues related to computing systems and to design optimal solutions.

To enable graduates to develop hardware and software systems by understanding the importance of social, business and environmental needs in the human context.

To enable graduates to gain employment in organizations and establish themselves as professionals by applying their technical skills to solve real world problems and meet the diversified needs of industry, academia and research.

Program Specific Outcome (PSO)

To adapt to emerging technologies and develop innovative solutions for existing and newer problems.

To create and apply appropriate techniques IT tools to complex engineering activities with an understanding of the limitations.

To manage complex IT projects with consideration of the human, financial, ethical and environmental factors.

Program Outcome (PO)

Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

Problem analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

Modern tool usage: Create, select, and apply appropriate techniques, resources,& modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

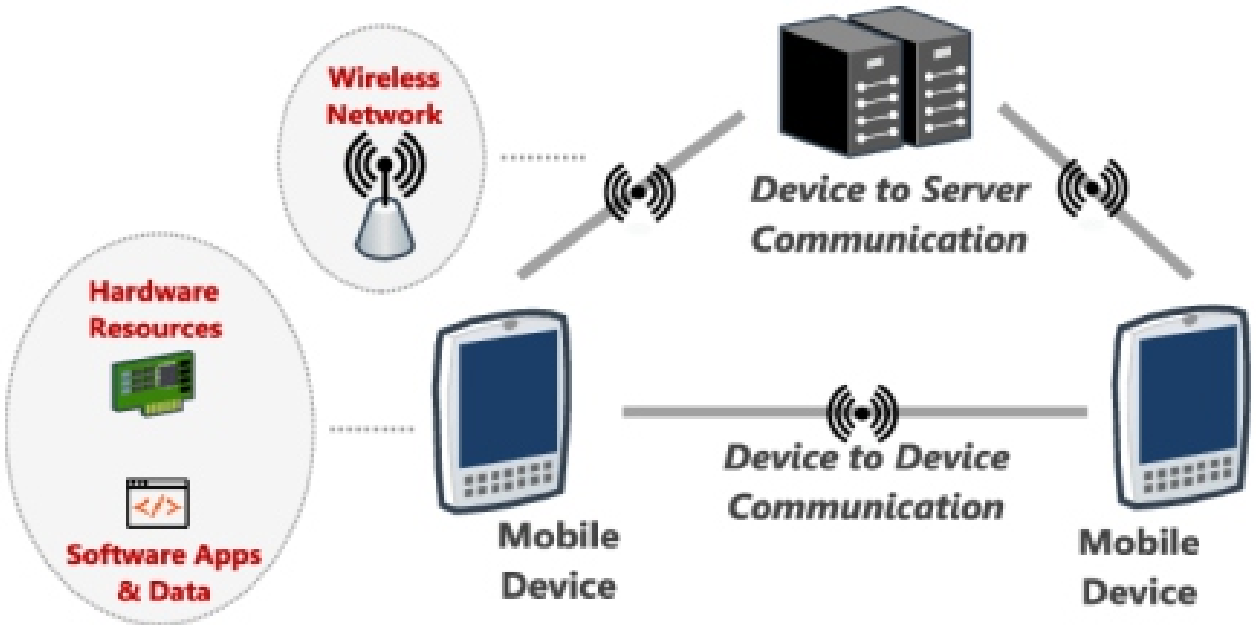
Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Mobile Systems and Computing: Empowering Global Development

Bikram Singh
(13508; CSIT)

STUDENTS ARTICLES

In the digital age, mobile systems and computing have emerged as powerful tools driving global development, particularly in regions where traditional infrastructure may be limited. The ubiquity of mobile devices, coupled with advances in computing technology, is catalyzing positive change by providing innovative solutions to longstanding challenges.

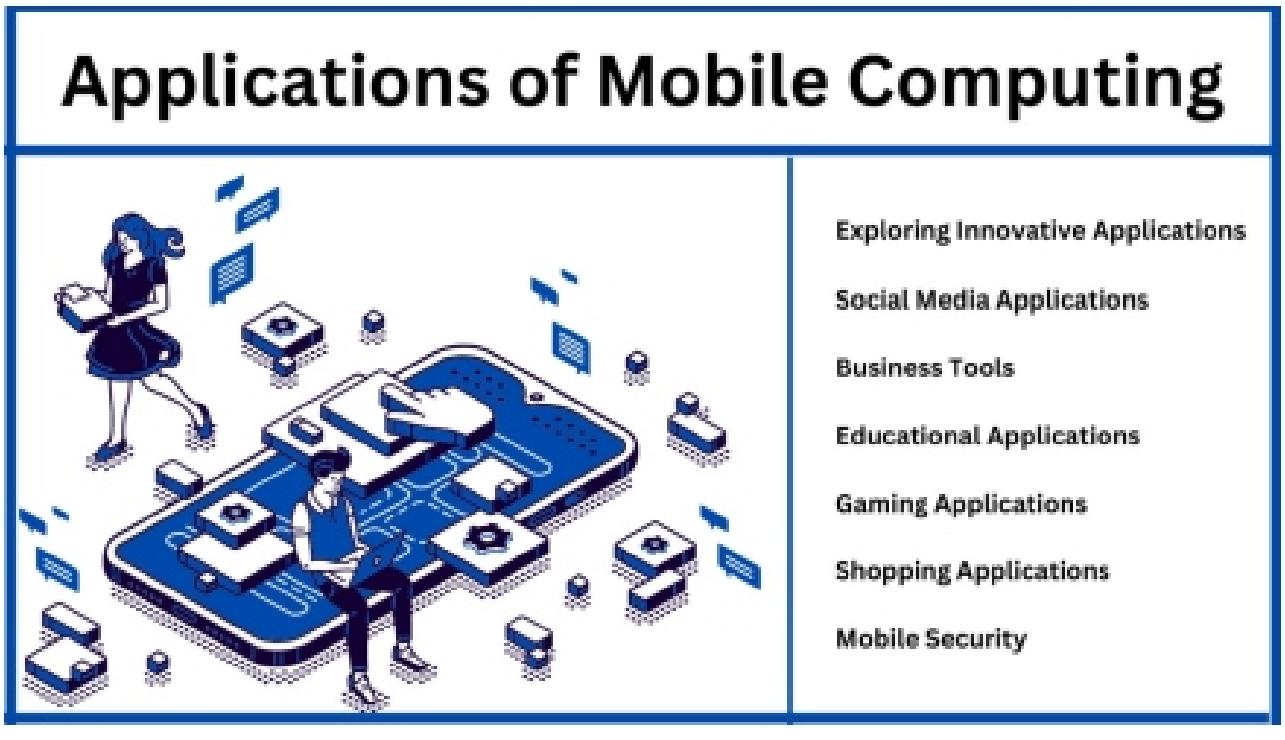


One of the primary ways mobile systems contribute to global development is through improved access to information and communication. Mobile phones have become indispensable tools for individuals in remote and underserved communities, enabling them to connect with the world, access educational resources, and stay informed about health-related information. This connectivity empowers communities with knowledge and opens up new opportunities for education, entrepreneurship, and collaboration.

Mobile computing also plays a pivotal role in financial inclusion, especially in regions with limited access to traditional banking services. Mobile banking applications and digital payment systems allow individuals to manage their finances, transfer money, and access credit seamlessly. This not only fosters economic empowerment at the individual level but also contributes to the growth of local economies by facilitating transactions and promoting financial stability.

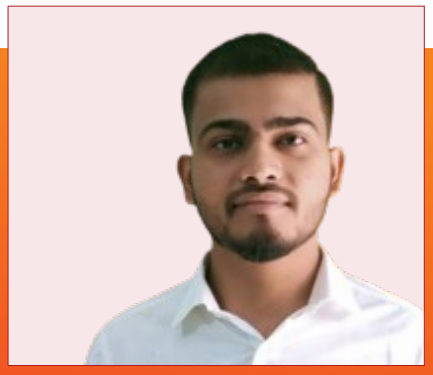
In the realm of healthcare, mobile systems are revolutionizing access to medical information and services. Mobile health applications provide a platform for health monitoring, disease prevention, and even telemedicine consultations. This is particularly impactful in remote areas where traditional healthcare infrastructure is sparse, allowing individuals to receive timely medical advice and interventions.

Furthermore, mobile systems contribute to global development by facilitating data collection and analysis. Researchers and organizations leverage mobile devices to gather real-time data on various issues, ranging from environmental conditions to social indicators. This data-driven approach enables evidence-based decision-making and targeted interventions, ultimately leading to more effective development strategies.



As mobile systems and computing continue to evolve, their role in global development is set to expand further. By harnessing the power of these technologies, we can bridge digital divides, empower marginalized communities, and create a more inclusive and connected world where the benefits of technology are harnessed for the greater good.

Unveiling the Guardians of Cyberspace: Ethical Hacking and White Hat Techniques

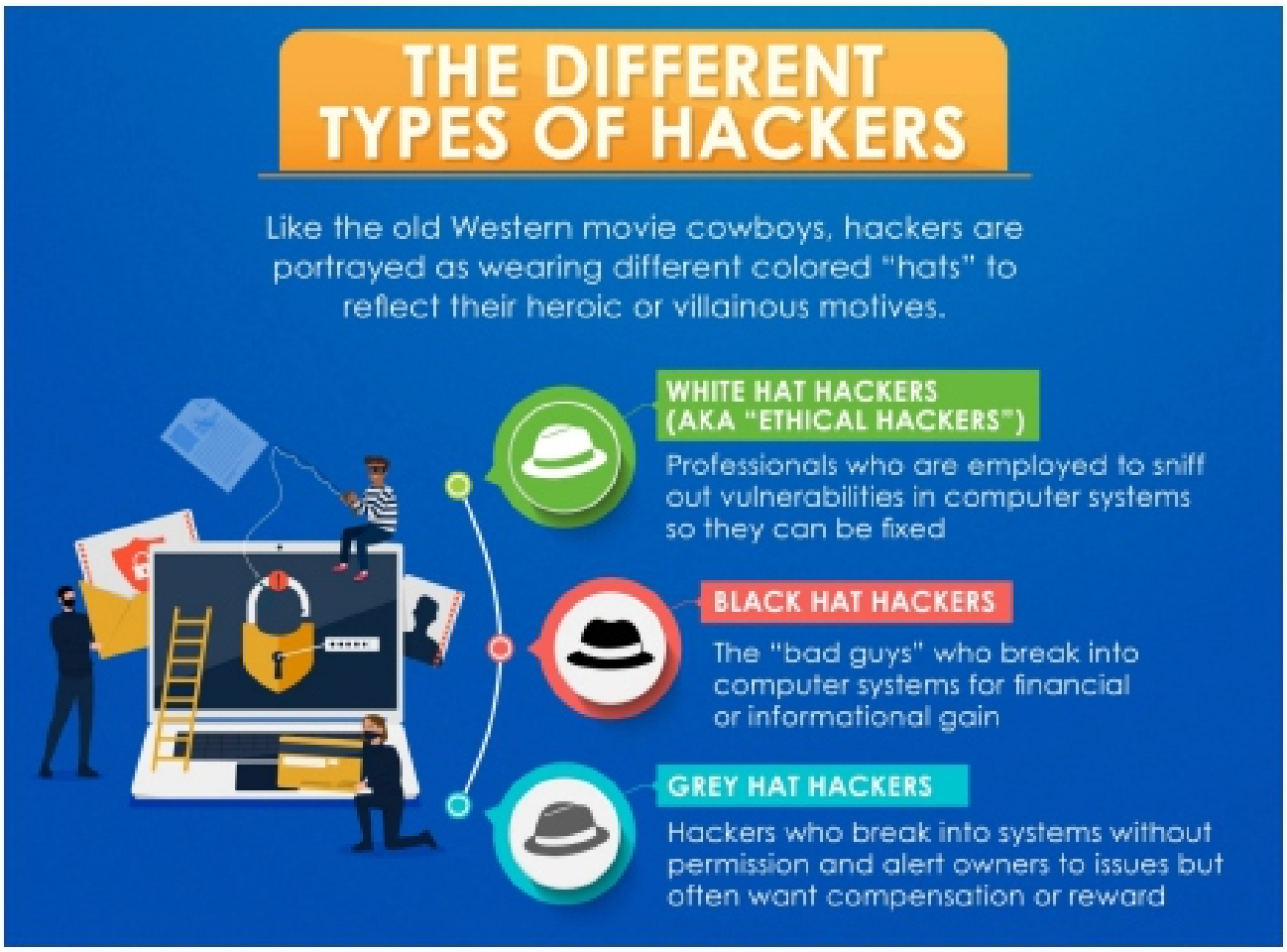


Sazid Khan
(13541; CSIT)

STUDENTS ARTICLES

In the ever-evolving landscape of cybersecurity, ethical hacking, often referred to as white hat hacking, stands as a beacon of defense against malicious cyber threats. Ethical hackers are the unsung heroes who use their expertise to strengthen digital fortresses rather than breach them. Employing a range of white hat techniques, these cyber guardians help organizations identify and rectify vulnerabilities, ensuring a robust defense against potential cyber attacks.

White hat techniques involve a variety of methodologies designed to simulate cyber attacks, enabling ethical hackers to uncover weaknesses before malicious actors exploit them. Penetration testing is a common white hat approach, where professionals systematically probe systems, networks, and applications to identify vulnerabilities. This proactive approach allows organizations to patch security gaps and fortify their digital infrastructure.



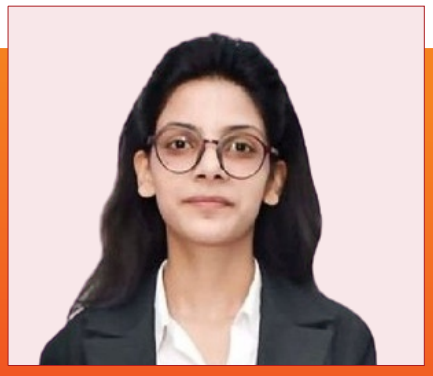
STUDENTS ARTICLES

White hat techniques involve a variety of methodologies designed to simulate cyber attacks, enabling ethical hackers to uncover weaknesses before malicious actors exploit them. Penetration testing is a common white hat approach, where professionals systematically probe systems, networks, and applications to identify vulnerabilities. This proactive approach allows organizations to patch security gaps and fortify their digital infrastructure.

Vulnerability scanning is a white hat technique that involves automated tools to identify potential weaknesses in a system. Ethical hackers utilize these tools to perform regular scans, ensuring that any newly discovered vulnerabilities are promptly addressed. This proactive measure prevents cyber threats from exploiting known weaknesses.

In essence, ethical hacking and white hat techniques play a crucial role in maintaining the integrity and security of digital ecosystems. By staying one step ahead of cybercriminals, ethical hackers contribute to a safer online environment for individuals, businesses, and governments alike. As technology continues to advance, the ethical hacking community remains at the forefront, adapting and innovating to safeguard the digital realm from potential threats.

Behind the Code: Crafting Antivirus Software to Combat Cyber Threats

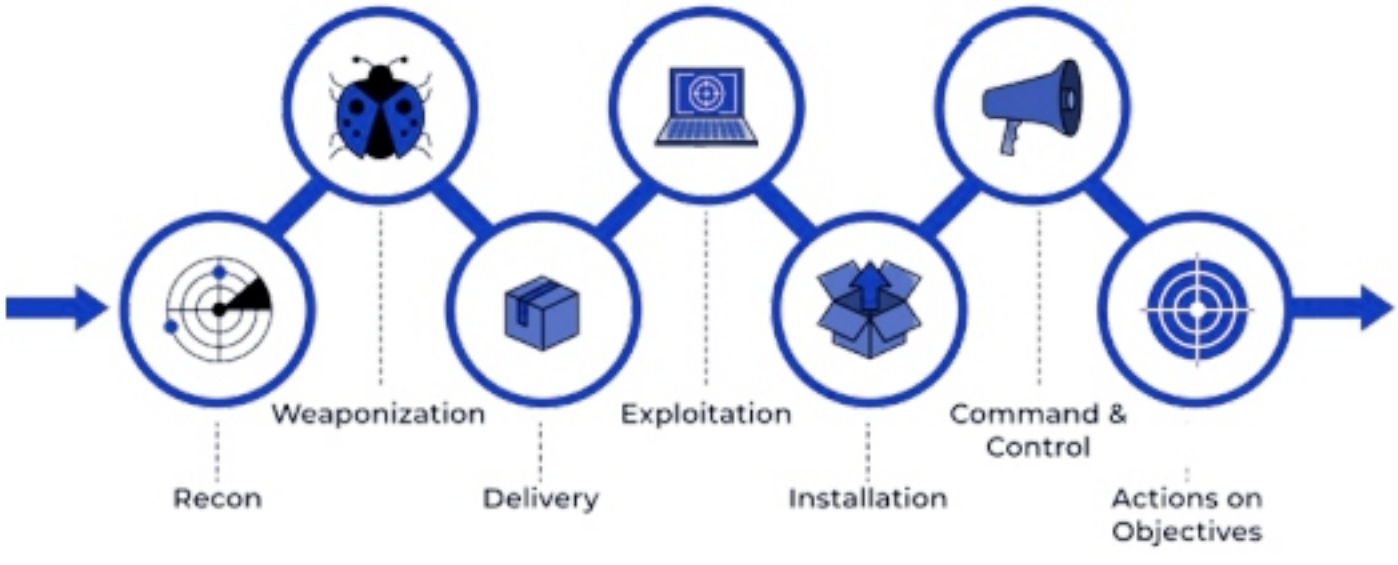


Rashi Saini
(13535; CSIT)

STUDENTS ARTICLES

Antivirus software stands as a digital shield, protecting users from the ever-growing landscape of cyber threats. Crafting these essential tools involves a combination of advanced programming, threat intelligence, and constant adaptation to the dynamic nature of malware. Here's a glimpse into the intricate process of writing antivirus software.

At the core of antivirus software development lies the creation of detection algorithms. Programmers design sophisticated algorithms that analyze the code of files and applications, identifying patterns and behaviors commonly associated with malware.



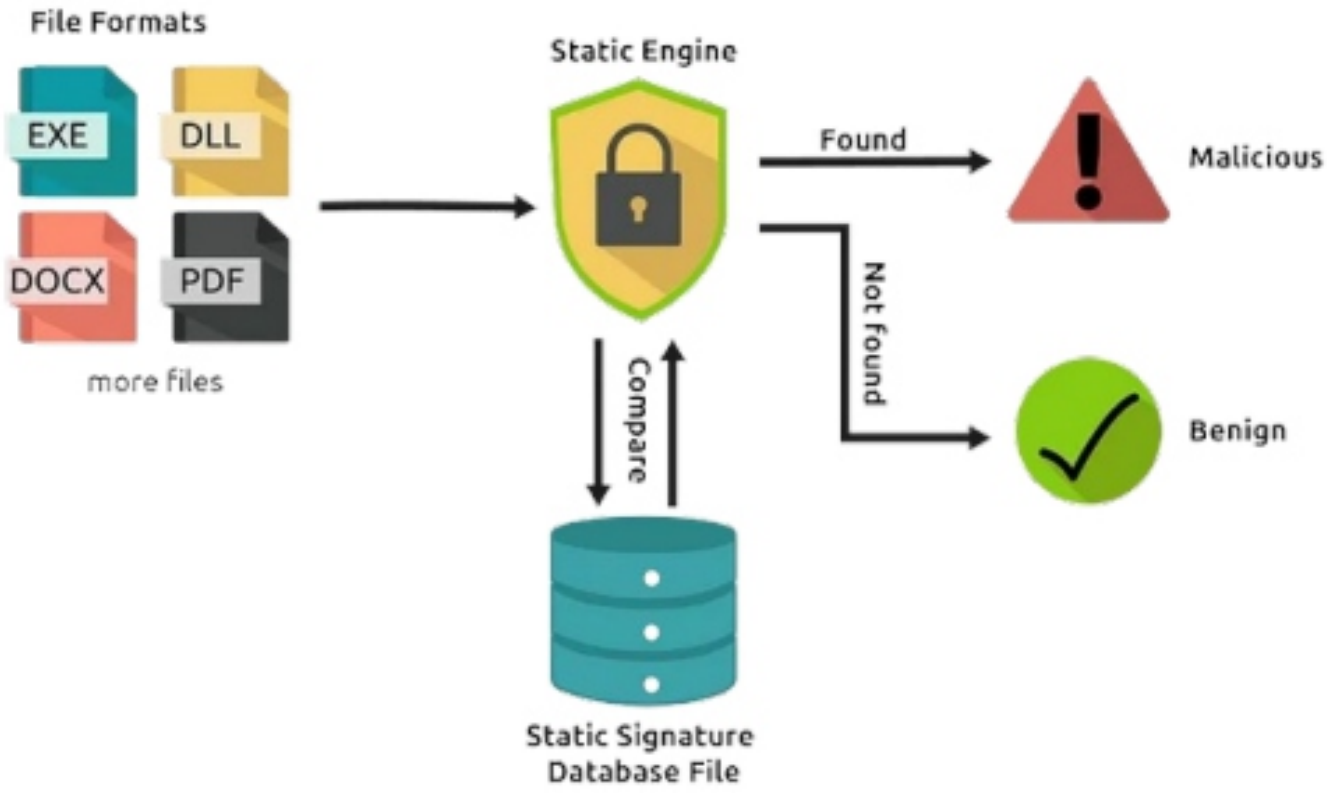
These algorithms are constantly updated to keep pace with emerging threats, making regular updates a crucial aspect of antivirus effectiveness.

Virus signature databases are another vital component. These databases store unique identifiers, or signatures, of known malware. During a scan, the antivirus software compares files against these signatures to identify malicious code. Continuous updates to these databases ensure that the antivirus program can recognize the latest threats circulating in the digital realm.

Heuristic analysis is a proactive technique employed in antivirus software writing. Instead of relying solely on predefined patterns, heuristics allow the software to detect suspicious behaviors or characteristics that may indicate the presence of previously unseen malware. This adaptive approach enables antivirus programs to catch new and evolving threats based on their behaviors rather than just their signatures.

Collaboration with threat intelligence feeds plays a crucial role in enhancing the efficacy of antivirus solutions. Cybersecurity researchers and organizations constantly gather information on new threats and attack vectors. Antivirus developers incorporate this intelligence into their software, enabling it to recognize and neutralize emerging threats before they can cause harm.

In essence, the writing of antivirus software is a dynamic and collaborative process that involves a combination of advanced algorithms, constant updates, and collaboration with the broader cybersecurity community. As cyber threats continue to evolve, antivirus developers remain committed to staying one step ahead, ensuring that users can navigate the digital landscape with confidence and security.



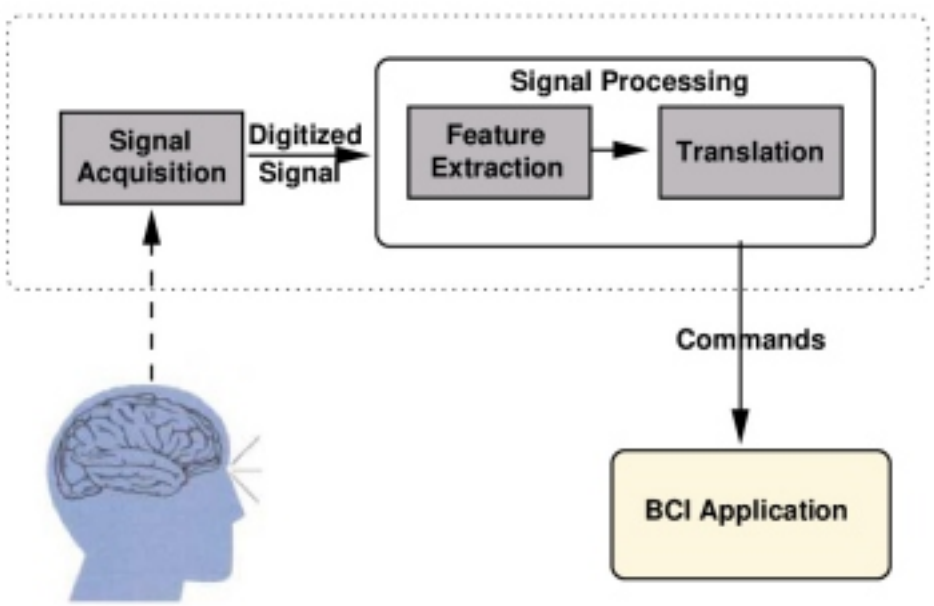
Unlocking the Future: Mind-Controlled Password Systems Redefine Security

Anant Singh
(13500; CSIT)

STUDENTS ARTICLES

In the realm of cybersecurity, the traditional landscape of passwords is undergoing a revolutionary transformation with the advent of mind-controlled password systems. Imagine a world where the power of your thoughts becomes the key to accessing your most sensitive information. This cutting-edge technology, once the stuff of science fiction, is now a tangible reality, paving the way for a more secure and seamless authentication process.

Mind-controlled password systems leverage advancements in brain-computer interface (BCI) technology. These interfaces establish a direct communication channel between the human brain and external devices, creating unprecedented possibilities in the field of cybersecurity. The concept involves users mentally interacting with their devices to authenticate access, eliminating the need for traditional passwords or biometric identifiers.



One of the key advantages of mind-controlled password systems is the uniqueness of brainwave patterns. Just as fingerprints and retinal scans are unique to individuals, the patterns of electrical activity in the brain are distinctive. This uniqueness adds an extra layer of security, making it exceedingly difficult for unauthorized individuals to mimic or replicate the required mental authentication.

The technology operates by recording and analyzing the user's brainwave patterns during the authentication process. This recorded data becomes the user's "mindprint," serving as the digital equivalent of a traditional password. To enhance security further, some systems even incorporate machine learning algorithms that adapt and evolve alongside changes in the user's mental patterns over time.

Beyond the obvious security benefits, mind-controlled password systems also offer a more user-friendly experience. Users are spared the burden of remembering complex passwords or dealing with the inconvenience of fingerprint scanners. Instead, accessing secured information becomes as natural as thinking.

While mind-controlled password systems are still in the early stages of development, they hold tremendous promise for the future of cybersecurity. As technology continues to unlock the mysteries of the human mind, the convergence of neuroscience and information security is poised to reshape how we safeguard our digital lives. The era of mind-controlled passwords heralds a new frontier in security, where the power of thought becomes the ultimate key to unlocking the digital world.