VSIT | Vidyalankar School of Information Technology

V-Tech

Technical Magazine of Information Technology Department

Academic year

2020 - 21

Issue - II

Preface

I am pleased to present the second issue of V-Tech, the technical magazine by the Department of Information Technology of VSIT, for academic year 2020-21. With present COVID-19 pandemic in mind, we have decided following themes for this issue-

1) Data security and security threats in the context of work from home.
2) Role and applications of IOT in context of COVID-19 pandemic.
3) Role of Technology and Innovations in sustaining isolated life during COVID-19 pandemic.

Teachers contributed articles with reference to the above themes and current/upcoming areas which help in expanding the knowledge base of faculty members.

Since last one year, as all of us are working from home, one must focus on data security. Various articles are presented in this issue discussing about security threats and data security in context of WFH. This issue also presents articles based on during COVID-19 pandemic or post the pandemic, what is the role of IOT and how IOT can help us to cope with the same. Last but not the least; it also covers the COVID pandemic and challenges faced in academia, the concept of work from home and Role of Technology and Innovations in sustaining isolated life during COVID-19 pandemic.

I hope you will find this issue as interesting as I did. It will help all the readers in enriching their IT knowledge and hopefully strike a chord in at least one area where they can take a deep dive for their research activities.

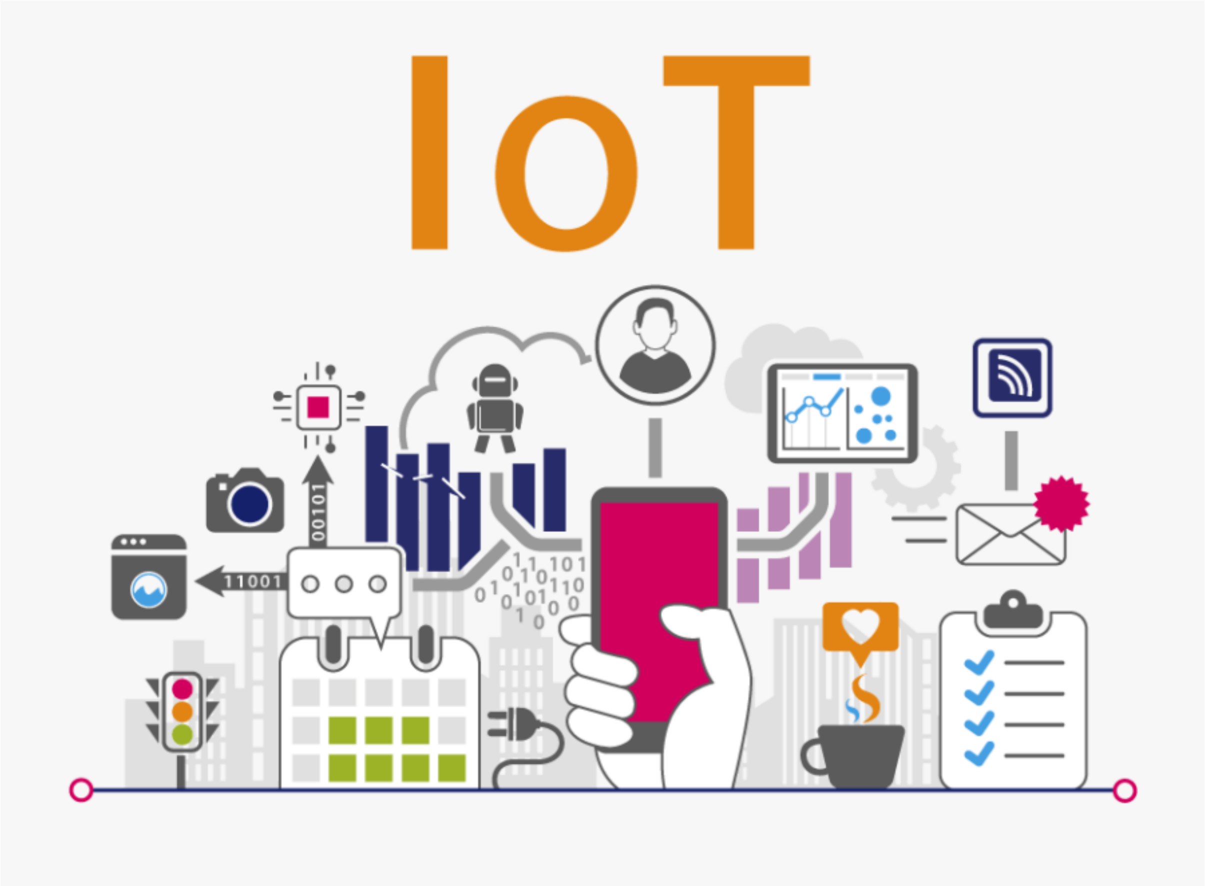
Prof. Makarand Deshpande

Adjunct Faculty

Index

Theme- Role of Technology and Innovations in sustaining isolated life during COVID-19 pandemic.

ROLE AND APPLICATIONS OF IOT IN CONTEXT OF COVID-19 PANDEMIC



Use of IoT in controlling the spread of Covid -19 by avoiding Gathering

India is the second largest populous country in the world. A major part of this population is divided into the metro cities like Mumbai, New Delhi, Bangalore, and Chennai. Apart from that the whole world is suffering from COVID19 global pandemic where the virus is spreading through human interaction. Therefore, the purpose of gathering size estimation cameras is to ensure the minimum mass moment in public places like Railway station, Shopping Complex and many more. Also, people will be aware of the gatherings and not to gather at one place.

Sometimes people at many places gather during the covid19 situation too breaking rules and not taking measures against the virus. Due to this reason too to control situations better and handy making places safer and people also. The capabilities of current intelligent visual surveillance systems to monitor masses and to improve their robustness can be employed in practical situations. In large public places, it is often not possible to monitor every person's individual behaviour due to gathering size. Instead, gathering properties can be monitored, such as the distribution of people throughout the space and the total number of people in the scene. Gathering size may be an indicator of security threats such as fighting, violent protest, mass panic and excitement. Even in peaceful gatherings, size may be an indicator of congestion, delay, or other abnormalities. Other than last few months the whole world is suffering from global pandemic.

In such cases social distancing is the important factor to stop the spread. Hence gathering size estimation plays a vital role. Gathering counting can be done using Raspberry Pi, ThingSpeak and OpenCV system can be implemented in various domains such as libraries, schools, airports, malls. In school and public libraries. Humuan counters are mostly used in the retail industry to gain better insights into how shoppers behave. They are also found in security, event management, and smart city applications. Imagine you manage a large mall: these counters let you know how many people are standing at one place or how many are there. which paths they take, where they stop, and most importantly when it all happens.

Companies like CrowdVision and many other have tried to implement the people Counter system. Also used the image processing algorithms. User friendly and easily available device can be used. It should be applicable in large as well as compact area's. It provides quick and accurate processed data. This device should be the game changer in current global pandemic situation where social distancing is a key factor. In India metro cities like Mumbai, Bangalore, Chennai where mass management is nearly impossible this device will help government agencies to maintain law and order. Monitoring places and movements at places can be done easily via the gathering counting management system. Also, the setup and monitoring are easy on this device a person can monitor all the movements through the screen. ThingSpeak include real-time data collection, data processing, visualizations, apps, and plugins. At the heart of ThingSpeak is a ThingSpeak Channel. A channel is where you send your data to be stored. Python is a dynamic, high level, free open source and interpreted programming language. It is easy to code, free and open source, object-oriented Language. Python is Portable language. ThingSpeak is an IoT analytics platform service that allows you to aggregate, visualize, and analyze live data streams in the cloud. You can send data to ThingSpeak from your devices, create instant visualization of live data, and send alerts devices to ThingSpeak. With the ability to execute MATLAB® code in ThingSpeak you can perform online analysis and processing of the data as it comes in. ThingSpeak is often used for prototyping and proof of concept IoT systems that require analytics.

OpenCV captures and saves videos, process images (filter, transform), perform feature detection, detect specific objects such as faces, eyes, cars, in the videos or images, analyze the video, i.e., estimate the motion in it, subtract the background, and track objects in it. Raspberry Pi is low cost compared to other boards. It provides huge processing power and it also very compact. It provides many interfaces (HDMI, multiple USB, Ethernet, onboard Wi-Fi, and Bluetooth, many GPIOs, USB powered, etc.). It is a minicomputer to help build products faster and better than other boards. So finally I can conclude that using IoT, we can manage gathering automatically and will help in controlling the spread of Covid-19.

Pushpa Susant Mahapatro

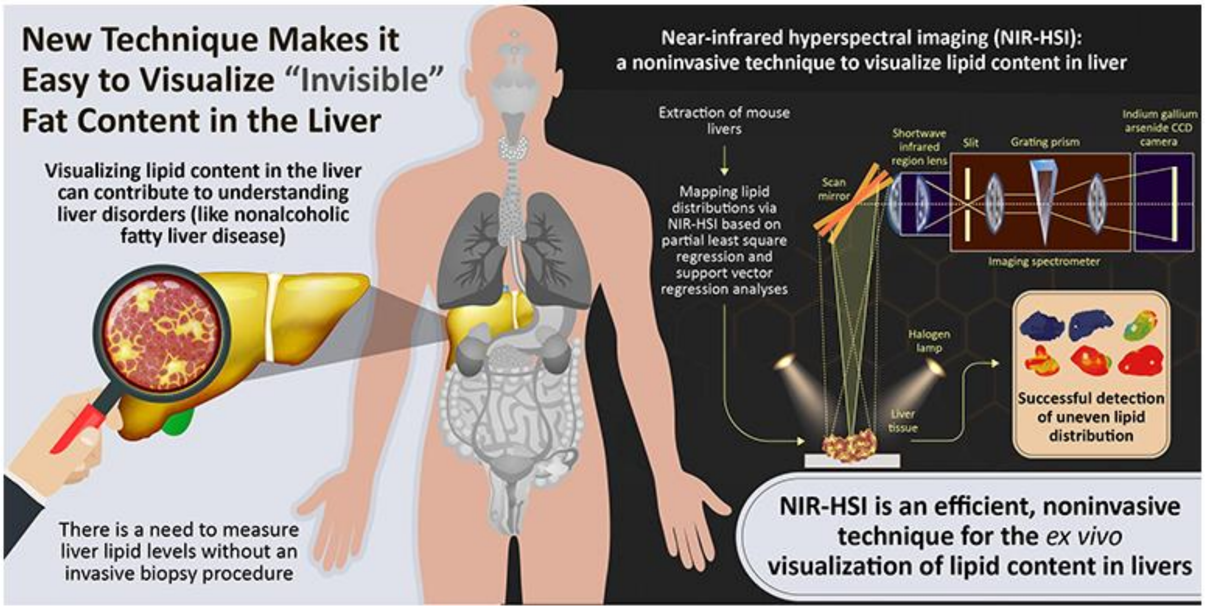
Assistant Professor

Non-invasive Liver Fat Detection

Your liver is the second largest organ in your body. It helps process nutrients from food and drinks and filters harmful substances from your blood. Too much fat in your liver can cause liver inflammation, which can damage your liver and create scarring. In severe cases, this scarring can lead to liver failure.

When fatty liver develops in someone who drinks a lot of alcohol, it's known as alcoholic fatty liver disease (AFLD). In someone who does not drink a lot of alcohol, it's known as non-alcoholic fatty liver disease (NAFLD). NAFLD becomes silent killer as patient remains unaware of his own condition since he does not have background of drinking problem. A liver biopsy is considered the best way to determine the severity of liver disease. During a liver biopsy, a doctor will insert a needle into your liver and remove a piece of tissue for examination. They will give you a local anaesthetic to lessen the pain. This test can help determine if you have fatty liver disease, as well as liver scarring.

NAFLD involves excessive fat deposition in the liver and can lead to liver failure. As the name suggests, this is not caused by alcohol abuse, but risk factors such as type 2 diabetes and high cholesterol play a role. At present, the standard technique to assess the liver for its fat content is to obtain a biopsy. This is not much fun for the patient, so a less invasive approach would be welcome.


New Technique Makes it Easy to Visualize "Invisible" Fat Content in the Liver
Visualizing lipid content in the liver can contribute to understanding liver disorders (like nonalcoholic fatty liver disease)
There is a need to measure liver lipid levels without an invasive biopsy procedure
Near-infrared hyperspectral imaging (NIR-HSI): a noninvasive technique to visualize lipid content in liver
Extraction of mouse livers
Mapping lipid distributions via NIR-HSI based on partial least square regression and support vector regression analyses
Scan mirror
Shortwave infrared region lens
Slit
Grating prism
Indium gallium arsenide CCD camera
Imaging spectrometer
Halogen lamp
Liver tissue
Successful detection of uneven lipid distribution
NIR-HSI is an efficient, noninvasive technique for the *ex vivo* visualization of lipid content in livers

Researchers at the Tokyo University of Science have applied a new imaging technique in a way that may allow clinicians to assess liver fat content without having to take biopsies. This technique is called near-infrared hyperspectral imaging, the method can highlight fat distribution in liver tissue, potentially helping clinicians to diagnose and assess conditions such as Non-Alcoholic Fatty Liver Disease (NAFLD).

According to Kyohei Okubo, a researcher involved in the study, “Lipid distribution in the liver provides crucial information for diagnosing fatty liver-associated liver diseases including cancer, and therefore, a non-invasive, label-free, quantitative modality is needed, This technique is a method to visualize the distribution of lipids in the liver using a near-infrared spectral imaging technique that incorporates machine learning.”

Previously, researchers have used near-infrared hyperspectral imaging to image atherosclerotic plaques in the blood vessels of rabbits, and so these Japanese researchers hypothesized that it might be useful to assess the distribution of fatty acids in the liver.

The team tested the technique with mice that ate a normal diet or a high-fat diet, and were able to visualize the lipid distribution throughout their livers. They could even generate maps that showed the gradients of lipid density. A technique called the Folch extraction method helped the researchers to quantitatively measure the actual lipid content of each liver, and they found that their measurements obtained using near-infrared hyperspectral imaging correlated closely with these values.

The results suggest that the technique may be valuable in assessing suspected fatty liver in human patients, without the need for biopsy.

Amraja K. Shivkar

Assistant Professor

V2X Technology- A journey towards driverless Vehicles

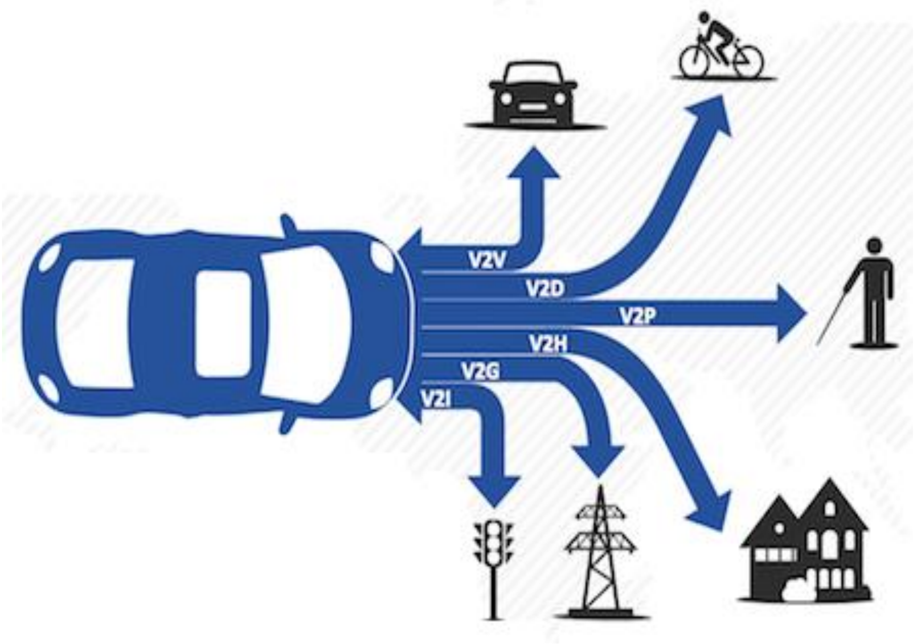
Background

The automotive industry in India is the 4th largest in the world with sales increasing 9.5 per cent year-on-year to 4.02 million unit. As a result of rapid growth of the number of automobiles on the road, the safety factor also arises. Every day lot of accidents happen on the roads due to over speeding, rash driving, hurry to reach the destination, breaking the traffic rules, drink and drive cases, and some other road hazards.

This safety question can be solved by making the automobiles intelligent and less reliant on human operation. The self-driven car or autonomous car can sense its surrounding environment and it is driven by very little human input. The driver-less car can be programmed to be aware of all surroundings in order to help prevent collision. Some additional features can also be added to the system such as information regarding weather, accident detection alarm, alcohol detection system, accidents and road conditions in nearby surroundings.

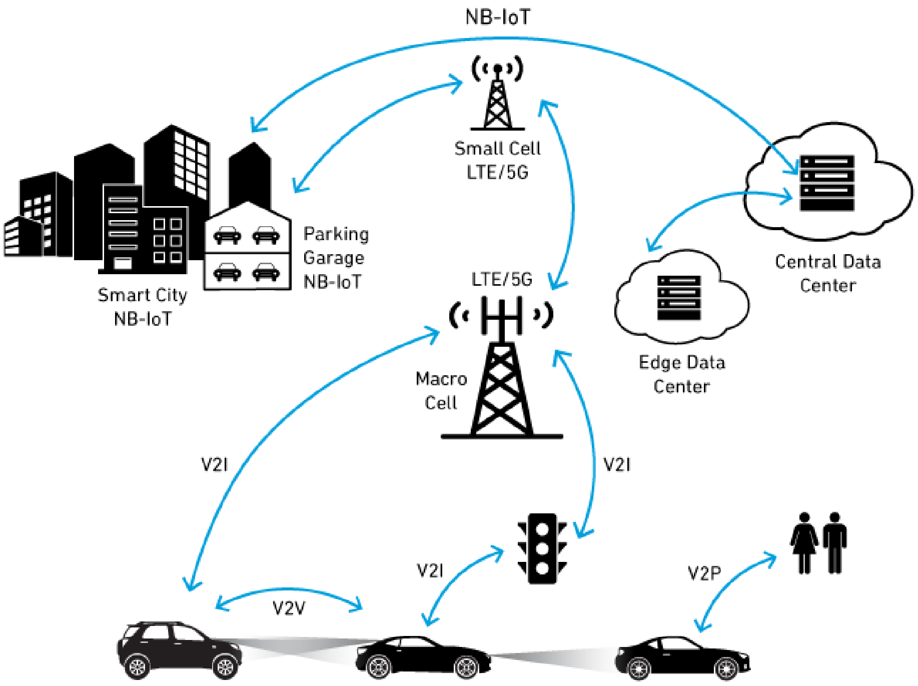
V2X Technology

V2X which stands for Vehicle to everything is an emerging technology for safer, greener and more efficient journeys. V2X allows vehicles to communicate with moving parts of the traffic system around them. With V2X technology, cars can actually "talk" to other vehicles on road, traffic lights, digital road signs, speed-breakers, and pedestrians, even if they're not directly within direct line of sight.



C V2X-

Cellular V2X, the standard is developed to communicate over existing and future cellular networks for improved road safety. It uses two communication modes-



1. Direct Communications- Enables direct communication between the vehicles (V2V), between vehicles to infrastructure (V2I) and between vehicles and other road users (V2P). This mode is independent of cellular networks.

2. Network Communications- Enables vehicle to network communication (V2N) over a licensed cellular network. The LTE networks support reliable real time communication at high speed. Vehicles can broadcast message related to the traffic, nearby accidents, road conditions to other vehicles over the network.

Types of V2X-

Vehicle-to-everything (V2X) communication is the passing of information from a vehicle to any entity that may affect the vehicle, and vice versa. It is a vehicular communication system that has following types.

1. V2V (Vehicle-to-vehicle)-

Vehicle-to-vehicle (V2V) is a dedicated short-range communication (DSRC) over wireless network where vehicles inform each other about their current status/activity. It includes speed, current location, direction of travel, status of brakes and stability of vehicle. systems, and so on. In automobiles and aircraft, paper batteries are used in hybrid vehicles because of their light weight.

2. V2I (Vehicle-to-Infrastructure)-

Vehicle-to-infrastructure is a communication model that allows vehicles in transit to share information with the road systems such as RFID readers and cameras, traffic lights, lane markers, streetlights, signage and parking meters, etc. V2I communication is bi-directional, wireless and uses DSRC channel for data transmission over an ad hoc network.

3. V2P (Vehicle-to-Pedestrian)-

The V2P approach holds in a broad set of road users including people walking, passengers getting on and off from buses and trains, people using wheelchairs, people riding bicycles, etc.

4. V2N (Vehicle-to-network)-

V2N enables both broadcast and unicast communications to take place between vehicles and the V2X management system and the V2X Application Server. This is achieved by making use of the LTE network infrastructure and the E-UTRA (Evolved Universal Terrestrial Radio Access). Vehicles can receive broadcasted alerts regarding accidents nearby, traffic information in the vicinity or weather conditions.

5. V2D (Vehicle-to-device) –

Vehicle-to-device (V2D) communication is a particular type of vehicular communication system that consists in the exchange of information between a vehicle and any electronic device that may be connected to the vehicle itself.

6. V2G (Vehicle-to-grid)-

Vehicle-to-grid (V2G) concept focuses on optimizing the energy needs of vehicles by turning electric cars into “Virtual Power Plants [11]”. Electric vehicles can store and distribute electrical energy stored in networked vehicle batteries, which together acts as one collective battery for sending power back to the grid when demand is high and charging at night when demand is low.

Applications and conclusion-

With the help C- V2X, real-time information beyond the driver’s line of sight is provided. C-V2X can be used in different ways to improve road safety and road traffic management, therefore achieving intelligent transportation system for monitoring and surveillance of road traffic. C-V2X is designed to be fully compatible with 5G technology.

Maitreyi Joglekar

Assistant Professor

Role of IoT during COVID-19

During COVID-19 IoT has played a great role in helping the healthcare system to properly monitor virus-infected patients through intertwined networks and devices. The industry during these times has inevitably chosen to rely on this system of communication to protect people against the spread of the pandemic.

Digital Diagnostics: - Kinsa smart thermometer were able to track the spread of the virus through fever spikes mapped with data from their devices. This centralized data helps people in their own communities to keep a track of where an outbreak may be potentially happening by building a communication network that connects more than a million users with a free app, email alerts, and a connected thermometer. As compared to old-fashioned thermometers without IoT integration, smart versions can collect valuable data to be shared with health providers and keep track of trends across a region to better protect communities.

Remote Monitoring: -

Devices created to keep track of patients from their homes, remote IoT has been able to monitor chronic diseases of elderly patients that increase the risk of dying from the Coronavirus. If data shows a patient is approaching a crisis, they can be quickly transported to a hospital but otherwise they can remain under IoT device monitoring in the safety of their homes.

Robot Assistance: - Robots can be used to disinfect devices, clean hospitals and deliver medicine, all of which give healthcare workers more time to treat their patients. Danish company UVD Robots has started using IoT to make robots that can clean patient rooms and disinfect theatres in hospitals and fighting COVID-19 contamination with a special UV light that effectively kills the virus. Since the light can be harmful to humans, the robot enters the room, the door is closed, then the process is completed. Once finished, the robot alerts workers outside the room that it is safe to open the door again.

IoT continues to protect patients and healthcare workers alike in the face of COVID-19 and will grow even stronger in a post-pandemic world.

Leena Jadhav
Assistant Professor

The role of IoT in Data privacy and protection in Healthcare during Covid-19

The healthcare industry has been making rapid progress in recent years by using new technologies to perform medical services with greater accuracy. In addition to the Covid-19 outbreak that has severely disrupted the daily lives of people around the world, technology has advanced rapidly to help the health care sector.

With the prevalence of the epidemic at its peak, says Yash Mehta, an IoT specialist with Big Data Science, medical professionals are using new methods to treat patients, while avoiding human treatment, unless necessary. Internet of Things (IoT) devices have become a way to make this happen.

Many companies are helping to help the community with the disease, one of which is Ioterra, a marketplace that helps businesses find the right IoT service providers. It has also expanded its services in helping the public fight Covid-19 in partnership with various other companies in providing medical devices and products.

For example, monitoring a patient's temperature was the first and foremost step in determining if he or she was affected. IoT wearable devices such as smartwatches can provide the necessary information about a patient's heart rate, blood sugar level, blood oxygen level, and so on without the need for personal assistance. Apart from this, IoT has provided its services in many ways in the healthcare sector at this unprecedented time.

The integration of IoT devices with intelligent sensors and algorithms in the medical field, connected to the cloud application and other connected devices, has been very helpful in combating this epidemic. Some of the key services provided by IoT in health care include telemedicine, contact tracking, robotic cleaning, and data privacy and protection in the healthcare sector.

Since the health care industry contains a lot of sensitive information about patients, it has been a major target for many hijackers and criminals. Also, customer trust has been a major factor to consider as policies vary across platforms. Since data transactions between physician and patient take place over the cloud, the necessary steps must be taken to protect confidential information.

IoT has been associated with the healthcare sector for a long time by helping with IV status, temperature, and heart rate monitoring. But they were very trapped in the hospital. In recent times, IoT has been expanding its medical services outside of the hospital and helping many people with various ailments. Impact of Covid research in various IoT Industries makes it clear that IoT has been gaining momentum and has been introducing new trends in the medical field. Technological advances in the medical field have brought comfort not only to patients but also to physicians. Compared to conventional therapies in recent years, IoT medical devices have yielded many positive results in this field.

Rohini Desai

Assistant Professor

Offices Post Covid

Covid-19 pandemic started affecting the entire world. Many of the offices had to make a shift to a remote work. Every employee began to adapt to new routines and processes while working from home.

Some companies have announced plans to maintain their remote work format, some companies are planning to shift back to the office routine, and some are planning for a hybrid work pattern.

Post-Covid time has not yet arrived and the time to come back to normal is uncertain.

Many offices are empty, some are used occasionally and few of them are used daily but with limited work force.

Following are some of the technologies for office safety and efficiency.

- IoT access systems and automated door locks enable a safer and more secure office building, and they also allow for keyless, contact-free entrances. Many IoT access systems use biometrics to identify people and automatic doors, thus preventing unauthorized intruders and reducing the need for touch in a typically high-touch area.

- IoT sensors helps to enable lights, control HVAC (Heating, Ventilation and Air Conditioning. A healthy environment is much needed post covid.

- UV-C light with the connectivity of an automated IoT platform should be used. This enables UV disinfection programs to run in unoccupied spaces during off hours. UV disinfection provides employees with peace of mind about being in a cleaner, safer work environment.

- IoT air purification programs should be used that creates safer, more ventilated office environment. So that employee does not face any health issues post covid.

- In offices like public places certain areas like washroom need to be cleaned after certain number of people have visited them. Cleaners can mark a washroom cleaned in their mobile application and all this information can be shown on an info display outside the restroom. This way the users are informed if the washroom is available, and when it has been cleaned thus avoiding unnecessary contacts and feeling safe.

Offices are certainly going to change but will not disappear fully. The business owner should start converting their office in to smart office.

IoT solutions can help us fight against Covid-19 by preventing the spread of disease and ease our concerns of returning back to public spaces and offices safe.

Snehal Tandale

Assistant Professor

Realtime Portable Sensors for Virus Alert-Need of the time

At the end of year 2019, the whole world was affected by a new pandemic, respiratory virus, which causes the coronavirus disease 2019 also known as COVID-19. The disease is proven to be highly contagious. It is also feared to be air-borne; droplets of body fluids can transmit the disease in a matter of hours and has been proven to be fatal in many cases. This calls for an urgent need to formulate fast and reliable tests for the new coronavirus, so it helps to bring the pandemic under control as soon as possible. Most laboratories use a molecular method called, RT-PCR (Reverse Transcription Polymerase Chain Reaction), to detect viruses in respiratory infections. This is well established and can detect even small number of viruses, but at the same time it can be time consuming and not every person can go and do the testing without having any symptoms or justifiable reasons for infection.

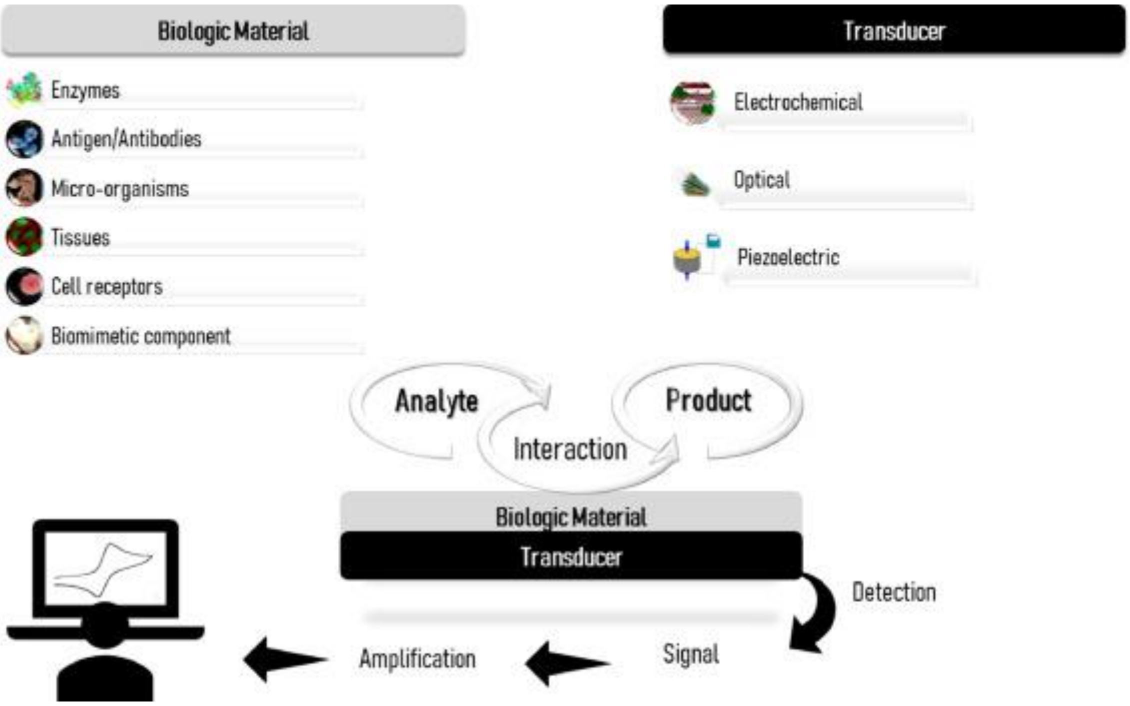


Image Credit: https://www.sciencedirect.com/science/article

Biosensors are analytical devices that convert biological reactions into measurable signals. The biological material such as enzymes, tissues, microorganisms, antibodies, cell receptors, is immobilized over a transducer, and interacts with the analyte in the solution, producing a biochemical response. The transducer, in turn, converts this biochemical response into a quantifiable signal measured by the digital detector module.

A team of researchers from Empa, ETH Zurich and Zurich University Hospital has succeeded in developing a novel sensor for detecting the new coronavirus. In future, it could be used to measure the concentration of the virus in the environment. Jing Wang and his team at Empa and ETH Zurich usually work on measuring, analysing and reducing airborne pollutants such as aerosols and artificially produced nanoparticles. Even before the COVID-19 began to spread, Wang and his colleagues were researching sensors that could detect bacteria and viruses in the air. Jing Wang and his team have developed an alternative test method in the form of an optical biosensor. The sensor combines two different effects to detect the virus safely and reliably: an optical and a thermal one.

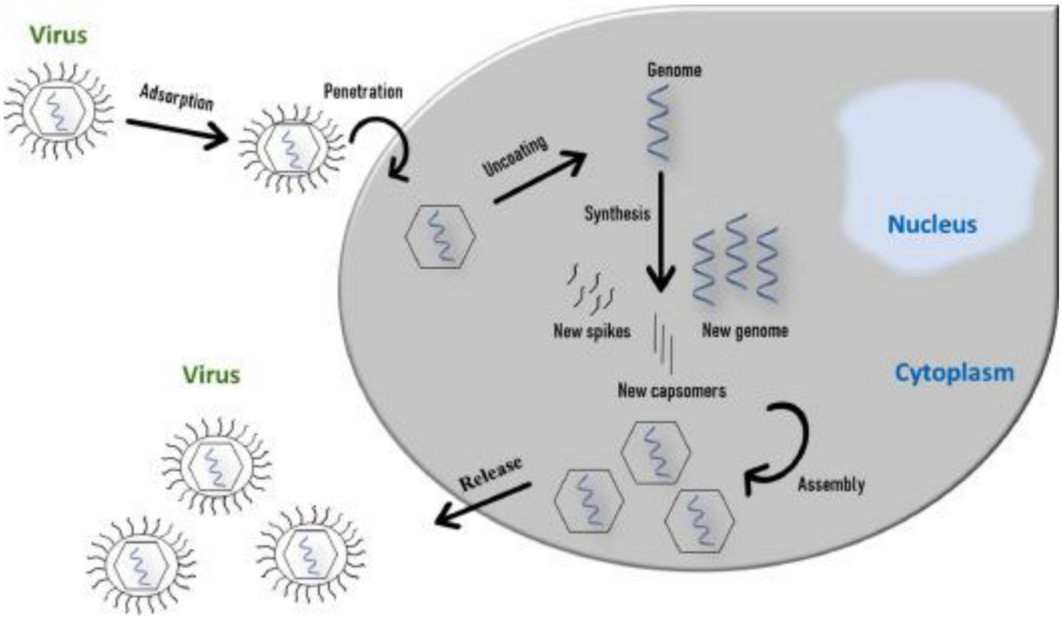


Image Credit: https://www.sciencedirect.com/science/article

The coronavirus is an RNA virus. The receptors on the sensor are therefore the complementary sequences to the virus' unique RNA sequences, which can reliably identify the virus. The technology used for detection is called LSPR, (Localized Surface Plasmon Resonance). An optical sensor located on the back of the sensor can be used to measure this change and thus determine whether the sample contains the RNA strands in question. However, the sensor is not yet ready to measure the corona virus concentration in the air

Several companies are selling devices that detect the novel coronavirus, but none give instant readings. These devices suck in large quantities of air and trap aerosolized virus particles and anything else that is present. The contents are then tested for the presence of the novel coronavirus, which causes COVID-19. But these devices are not able to deliver results in real time. Instead, the collected samples must be sent to a lab to be analysed, typically by PCR. This process takes hours.

In present time what we need is a device that can detect the virus and provide alert in real time. This device should beep to alert people nearby that the virus has been detected. Scientists at Tohoku University have been studying materials that can change mechanical into electrical or magnetic energy, and vice versa, for decades. They published a review about the most recent endeavours into using these materials to fabricate functional biosensors. Piezoelectric materials convert mechanical into electrical energy. Antibodies that interact with a specific virus can be placed on an electrode incorporated onto a piezoelectric material. When the target virus interacts with the antibodies, it causes an increase in mass that decreases the frequency of the electric current moving through the material, signalling its presence. This type of sensor is being investigated for detecting several viruses, including Human Papilloma Virus, HIV, Influenza, Ebola and Hepatitis B.

Scientists still need to develop more effective and reliable sensors for virus detection, with higher sensitivity and accuracy, smaller size and weight, and better affordability. The future could hold portable and wearable sensors for detecting viruses and bacteria in the surrounding environment in real time and not just in laboratory. But we are not there yet.

Amraja K. Shivkar

Assistant Professor

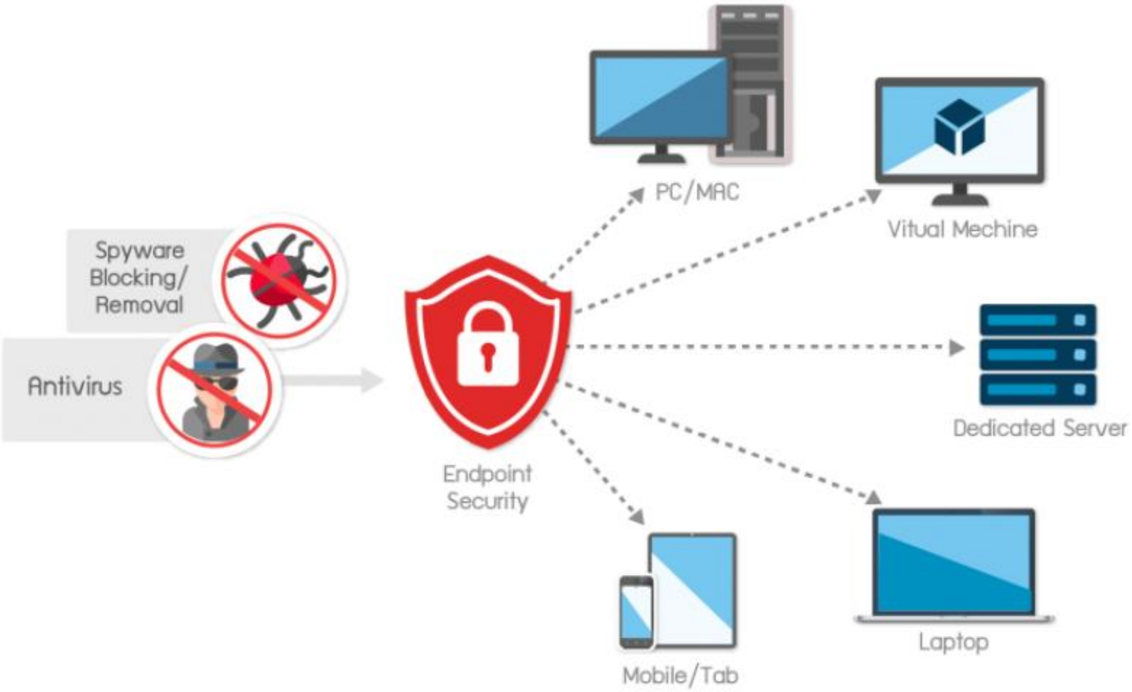
DATA SECURITY AND SECURITY THREATS IN THE CONTEXT OF WORK FROM HOME

Endpoint Security: Blind Spot for Remote Work

World is facing and suffering from the impact of Covid-19 and it is spreading in all countries and in all industries. Don't know how long it will take and how much it will inpact on the global economy.

From last year ,almost all companies , all enterprises experience challenges in acquiring new clients, renegotiating existing contracts, and generating revenues. This is a challenege because no one knows how to face this challenge as a result it will put pressure on cash flows forcing enterprises to think about the new and different business models to reduce costs and generate revenue.

During the lockdown, In Indian also, all IT industry companies made their employees to do "Work from Home" (WFH) in order to support government's instructions.



Numbers of people are working from home, accepting the trend of "New Normal". Our homes have become our offices, we're using new systems . Majority of the employees use their own devices rather than standard issue machines to connect to the corporate network , now they are not following any IT policies . It means in this " New Normal" trends security is affecting. There are many ways through our security is effecting during work from home environment. Endpoint Security is one of them.

What are Endpoint devices?

Any device which are connected to the network are referred as Endpoint such as desktop computers, laptops, smartphones, tablets, printers, or other specialized hardware like POS terminals.

Endpoint Device Weaknesses

Security policies, especially as they relate to BYOD protections, are an essential part of protecting endpoint devices from being exposed to attack. But the largest contributor to vulnerability is the quality of training and awareness given to employees. Bad habits can have a serious effect on the integrity of a secure network:

1. **Lost or improperly** decommissioned devices: Employees who lose devices that are connected to the company network may expose that network to attacks.

2. **Poor adoption of security updates**: Out-of-date operating systems and applications can lead to any number of vulnerabilities within a device that has been given access to sensitive company information.

3. **Employees switching encryption off/on:** people are more likely to adjust the security controls on devices they own and will rework settings to suit their needs. This can lead to unwanted access points.

What are the problems?

Unsecured Wireless Access Point (WAP)

Nowadays every employee use their own network it means either they are working from their home, hotels ,café etc . All are using their public network, public means that it is open for everyone. If we conduct a survey we come to know that all these remote workers are using unmanaged, insecure endpoint devices to connect to the corporate systems which is very dangerous.

Data Breach

Most of the time employees upload companies data over the public cloud. This will be an open invitation foe the attacker to get access over it, manipulate it or harm the company’s profile.

Malware and Phishing

Everything is unsecured now ,data is flowing through the unprotected channel. It makes attacker’s work very easy. Attacker just need to designed one attack like when employee click on the link for opening documents result in malware and ransomware attacks.

What can we do now?

- Companies need to check the security setting of the devices, protecting capability of the network. After checking , only device are able to connect to the companies network. Incase of any unauthourized device there is a need to remove it from the network.
- Delete all unnecessary data and unwanted application from the devices, as these are the first point where security can be attacked.
- All the device access port shoud be disabled , All the device control must be a mandatory administrative policy for a company’s cybersecure environment.
- Make use of standalone virtual machine. VDIs live within virtual machines (VMs) on a centralized server and are accessed over a network with an endpoint device

Today’s need is to build a secure endpoint ecosystem. Hackers want to compromise any and every device because cybercrime is a booming business nowadays. As wireless endpoint devices inch closer to acting as corporate infrastructure in the current remote work scenario, debunking the myth that wireless hijacking cannot be done across remote geographic locations becomes more critical.

More recently, with the increasing adoption of software as a service platforms (SaaS), the program and host server are both managed remotely by the SaaS provider. This business model gives organizations a chance to lower costs while ensuring constant updates to security parameters.

Spruha More

Assistant Professor

Extended Detection and Response

Extended Detection and Response (XDR) is a SaaS-based (method of software delivery that allows data to be accessed from any device with an internet connection and a web browser), vendor-specific, security threat detection and incident response tool that natively integrates multiple security products into a cohesive security operations system that unifies all licensed components. XDR enables an enterprise to go beyond typical detective controls by providing a holistic and yet simpler view of threats across the entire technology landscape. XDR delivers real-time information needed to deliver threats to business operations for better, faster outcomes.

Extended Detection and Response (XDR) primary advantages are:

- Improved protection, detection, and response capabilities
- Improved productivity of operational security personnel
- Lower total cost of ownership for effective detection and response of security threats

XDR consolidates multiple products into a cohesive, unified security incident detection and response platform. XDR is a logical evolution of endpoint detection and response (EDR) solutions into a primary incident response tool. Current systems need a platform that brings together all relevant security data and reveals advanced enemies. As enemies use more complex techniques, to exploit traditional security controls, organizations are scrambling to secure increasing numbers of vulnerable digital assets. Enterprises need unified and proactive security measures to defend the technological assets, mobile, and cloud workloads without overburdening staff and in-house management resources.

With all types of attackers, hacking groups, nation states and even potentially malicious insiders constantly circling, enterprise security and risk managers are left to overcome too many disconnected security tools and data sets from too many vendors. Security staff struggle with a large amount of overload and too small amount of security. Enterprise security and risk management leaders should consider the security advantages and productivity value of an XDR solution.

The primary value propositions of XDR products or capabilities include improving security operations productivity by enhancing detection and response capabilities by unifying visibility and control across endpoints, network, and cloud. XDR ingests and distils multiple streams of telemetry. XDR can also analyse various threats to make complex security operations capabilities more accessible to security teams that do not have the resources for more custom-made point solutions. XDR removes the intimidating detection and investigation cycles and offers threat centric and business context to move more quickly to a response to the threat.

Extended Detection and Response (XDR) security provides advanced threat detection and response capabilities including:

- Detection and response to targeted attacks
- Native support for behaviour analysis of users and technology assets
- Threat intelligence including shared local threat intelligence coupled with externally acquired threat intelligence sources.

- Reducing the need to chase false positives by correlating and confirming alerts automatically.
- Integrating relevant data for faster, more accurate incident triage
- Centralized configuration and hardening capability with weighted guidance to help prioritize activities.
- Comprehensive analytics

XDR products add value by consolidating multiple security products into a cohesive, unified security incident detection and response platform. Detecting today's advanced threats requires more than a collection of point solutions. XDR can optimize response with advanced context. XDR security provides advanced threat detection and response capabilities including:

- Converting a large stream of alerts into a much smaller number of incidents that can be focused on for manual investigation.
- Providing integrated incident response options that have necessary context from all security components to resolve alerts quickly.
- Providing response options that go beyond infrastructure control points, including network and endpoints.
- Providing automation capabilities for repetitive tasks
- Reducing training and up-levelling Tier 1 support by providing a common management and workflow experience across security components
- Providing usable and high-quality detection content with little-to-no tuning required

XDR improves critical functions when they are reacting to an attack in their environment:

- Detection - Identify more and meaningful threats by combining endpoint telemetry with a growing list of security controls providers as well security events collected and analysed by security information and analytic platforms.
- Investigation - Human-machine teaming correlates all relevant threat information and applies situational security context to more quickly reduce signal from noise and assist with the identification of root cause.
- Recommendations - Provide analysts with prescriptive recommendations to further an investigation through additional queries as well as offer relevant response actions that would most effectively improve the containment or remediation of a detected risk or threat.
- Hunting - Provide a common query capability across a data repository containing multi-vendor sensor telemetry in search of suspicious threat behaviours, allowing threat hunters to locate and act based on recommendations.

A comprehensive XDR platform requires a vendor that can deliver a product portfolio and a partner ecosystem with breadth, depth, and market maturity to seamlessly and meaningfully interconnect and correlate detections across multiple alerts.

Hrishikesh Tendulkar
Assistant Professor

Cyber Security Risks: Best Practices for Working from Home and Remotely

Since the pandemic, working from home has become much more widespread worldwide. Even once the pandemic fades, many predict that remote working will remain prevalent across multiple sectors. While working from home is convenient and has many benefits, it also exposes both individuals and businesses to a range of cyber security risks. That’s why it is essential to give serious consideration to home cyber security. By following best practices, you can mitigate most cyber security work from home threats quite easily.

How to stay safe when working from home

With the rise in remote working, certain cyber security threats – in particular, phishing – have become more prevalent. A key issue is that, in most workplaces, an IT team will take care of cyber security within the office. With a distributed workforce working remotely, staff have to pay more attention to cyber security threats themselves. Here are the top remote working security tips to ensure you and your staff are working from home safely.

1. Make sure your passwords are strong and secure

One of the simplest yet often overlooked ways to protect yourself when working from home is to strengthen your passwords and ensure that you have maximized password protection across your devices.

The US Federal Trade Commission offers this advice,

“Use passwords on all your devices and apps. Make sure the passwords are long, strong, and unique: at least 12 characters that are a mix of numbers, symbols, and capital and lower-case letters."

They also recommend adding a password screen every time you access your laptop and other devices so that if your device is breached or falls into the wrong hands, it will be harder for a third-party to access your sensitive files. We recommend using a password manager tool to help keep all your passwords secure.

2. Use antivirus and internet security software at home

One of the most effective security tips for working from home is to invest in a comprehensive antivirus suite for you and your employees.

According to sources, the estimated global damage to businesses due to cybercrime is around $1.5 billion per annum. This figure is only likely to increase as hackers look to exploit people's home internet networks and business VPNs to gain access to sensitive files.

Antivirus suites take the hard work off your hands by offering automatic remote work security against a host of threats, including:

- Zero-day attacks (viruses taking advantage of security flaws before they are patched)
- Malware, spyware, and viruses
- Trojans and worms
- Phishing scams, including those sent via email

It also runs discreetly in the background of your other operations, so you won’t even notice the hard work its doing.

3. Invest in a sliding webcam cover

Working from home usually means taking part in teleconferences and video calls which require the use of your webcam. Unfortunately, savvy hackers can easily access your webcam without permission, compromising your privacy. Worse still, if you have sensitive documents around your physical workspace, hackers may be able to view these by hijacking your webcam.

If your webcam is separate from your device, you should unplug it whenever you are not using it. If your webcam is built-in, you should take extra measures to protect yourself – there’s no telling when a webcam attack could occur.

Sliding webcam covers are easy to find online in all shapes, sizes, and colors to suit your needs. They are typically easy to install, too, as most come with an adhesive layer that fits around your webcam.

While using videoconferencing software, you may also want to use functions such as the "blur background" feature if your platform has it. This can prevent people in your conferences from spying on objects in the background of your home, which can often include sensitive data about you or your clients.

4. Use a VPN

Remote working often means connecting your computer to the company's Virtual Private Network (VPN connection) – but this, in turn, creates new home office safety 'back doors' that hackers could potentially expose.

First and foremost, it’s essential to provide employees with work from home security tips and guidance or policies on being a secure remote worker. Companies should look for ways to make their VPN more secure.

VPN security can be enhanced by using the most robust possible authentication method. Many VPNs use a username and password, but you may want to think about upgrading to the use of smart cards. You can also enhance your encryption method for VPN access, for example, by upgrading from a Point-to-Point Tunneling Protocol to a Layer Two Tunneling Protocol (L2TP).

5. Secure your home Wi-Fi

One of the simplest ways to ensure cyber security for remote workers is to strengthen your home Wi-Fi network's security. You can achieve this through some straightforward steps.

Create a strong, unique password, rather than relying on the automatic password your router came with. You can access your router’s settings page by typing “192.168.1.1” into your browser and change the password there. Make sure to choose a password that would be difficult for anyone to guess. You can also change your SSID, the name of your wireless network, on the same settings page to make it more difficult for third parties to identify and access your home Wi-Fi network. Do not use your name, home address, or anything that could be used to identify you.

Aasha Chavan

Assistant Professor

SECURE Work, while work from HOME.

The COVID-19 pandemic shows little sign of slowing down, and for many businesses, employees are still working remotely and from home offices. As a result, there has been an influx of employees signing in remotely to corporate networks and using cloud-based applications. But this shift could also open doors to security risks and cyberthreats.
While some companies are gearing towards reopening their standard office spaces in the coming months and have all the challenges associated with how to do so safely to face, they may also be facing repercussions of the rapid shift to remote working models in the cybersecurity space.
In the clamour to ensure employees could do their jobs from home, the enterprise needed to make sure members of staff had the right equipment as well as network and resource access. However, according to Malwarebytes, the rushed response to COVID-19 in the business arena has created massive gaps in cybersecurity and security incidents have increased as a result.

In Information Security threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.
Working from home has specific cyber security risks, including targeted cybercrime. When compromised, unauthorised access to your stored information can have a devastating effect on your emotional, financial, and working life.

As technology such as the Internet, computers and mobile devices become ubiquitous throughout society, the need to ensure our information remains secure is imperative.
Unfortunately, it has long been understood that good security cannot be achieved through technical means alone and a solid understanding of the issues and how to protect yourself is required from users.
Whilst many initiatives, programs and strategies have been proposed to improve the level of information security awareness, most have been directed at organizations, with a few national programs focused upon home users. Given people’s use of technology is primarily focused upon those two areas: the workplace and home, this paper seeks to understand the knowledge and practice relationship between these environments.
Information security awareness has been given an increasingly important focus within both academic and commercial communities. Organizations are gradually understanding the importance of their information assets and developing strategies to improve awareness throughout the company.

Context-aware security requires knowledge of who the user is, what the user is requesting, how the user is connected, when the user is requesting information and where the user is located. The goal is to prevent unauthorized end users or insecure computing devices from being able to access corporate data. Such an approach might allow an end user to browse the network from inside the office, for example, but deny access if the end user is trying to connect with public Wi-Fi.

One analogy that is often used to explain context-aware security is a door with a lock. A standard security door would simply require a key to open the door's lock. By comparison, a context-aware security door would behave differently in different scenarios. For example, a man in the United States might require a key to open the door, while a man in the United Kingdom would only need to know a secret password.

Some of the security policies need to follow to securely transitioning to work from home.

Be aware that the COVID-19 pandemic will be used by cybercriminals to try to scam people out of their money, data and to gain access to systems. While working from home you should:

- Exercise critical thinking and vigilance when you receive phone calls, messages, and emails.
- Exercise caution in opening messages, attachments, or clicking on links from unknown senders.
- Be wary of any requests for personal details, passwords, or bank details, particularly if the message conveys a sense of urgency.
- If in any doubt of the communicator's identity, delay any immediate action. Re-establish communication later using contact methods that you have sourced yourself.

Passwords are obsolete! Strong passphrases are your first line of defence. Enable a strong and unique passphrase on portable devices such as laptops, mobile phones, and tablets. Use a different passphrase for each website and app, particularly those that store your credit card details or personal information. To use the same username (such as an email address) and passphrase for multiple accounts means that if one is compromised, they are all at risk.

Multi-factor authentication is one of the most effective controls you can implement to prevent unauthorised access to computers, applications, and online services. Using multiple layers of authentication makes it much harder to access your systems. Criminals might manage to steal one type of proof of identity (for example, your PIN) but it is very difficult to steal the correct combination of several proofs for any given account.

It is important to allow automatic updates on your devices and systems like your computers, laptops, tablets, and mobile phones. Often, software updates (for operating systems and applications, for example) are developed to address security issues. Updates also often include new security features that protect your data and device.

Virtual Private Network (VPN) connections are a popular method to connect portable devices to a work network. VPNs secure your web browsing and remote network access.

Using free wireless internet may be tempting; it can also put your information at risk. Free Wi-Fi by its very nature is insecure and can expose your browsing activity to cybercriminals. Cybercriminals have also been known to set up rogue Wi-Fi hotspots with names that look legitimate and can intercept communications, steal your banking credentials, account passwords, and other valuable information. Use trusted connections when working from home, such as your home internet or mobile internet service from your telecommunications provider.

It is much easier to access your information if other people have access to your devices. Do not leave your device unattended and lock your computer when not in use, even if it is only for a short period of time.

You should also carefully consider who has access to your devices. Do not lend laptops to children or other members of the household using your work profile or account. They could unintentionally share or delete important information or introduce malicious software to your device.

If you do share your computers or devices with family or your household, have separate profiles so that each person logs in with a unique username and passphrase.

When transporting work from the office or shop to home, portable storage devices like USB drives and cards are easily misplaced and, if access is not properly controlled, can harm your computer systems with malware. If possible, transfer files in more secure ways, such as your organisation's cloud storage or collaboration solutions. When using USBs and external drives, make sure they are protected with encryption and passphrases.

Cybercriminals and other malicious actors use popular and trending topics such as COVID-19 to spread disinformation or scam people. Impersonating, cloning, or creating websites to look genuine is one way to do this (see 'Beware of scams' above). Producing and sharing false information on social media is another.

Be sure to only use trusted and verified information from government and research institution’s websites. Think critically about the sources of information that you use and balance all evidence before believing what people share.

Setting up a secure remote-working environment is not an overnight job. It requires considerable effort from all people involved, especially in the case of those who are new to telecommuting. The measures laid out here should help employees ease the burden and effectively protect work-from-home setups from cyberthreats.

Rajendra Ramesh Patole
Assistant Professor

How COVID-19 Pandemic has restructured Cyber Security Attacks in work from home environment?

World Health Organization (WHO) declared the COVID-19 as a pandemic in January 2020. COVID-19 has not only threatened our survival but also has damaged our daily lives, induced stress, and anxiety among people. It has destabilized businesses and damaged global economy. To limit the spread of this infection, governments have imposed restrictions, and encouraged lock down protocols, and social distancing measures. Many institutions, corporations and companies have closed their offices and initiated work from home (WFH) for its employees. In this situation, Information Technology departments of company's has played a very important role in ensuring that employees continue to work from their home environments and connect to companies' networks and continue to work using online platforms and tools. Online traffic on the internet has increased moving the physical workplace to an online virtual workplace. The demand for getting online medicines, groceries, food deliveries have increased.

A year after the transition to remote working, many organizations continue to grapple with security issues and weaknesses. Cyberattacks has seen an increase in healthcare institutions, financial institutions, government, and media institutions. These attacks have created an unpleasant situation by providing misleading information and instilling hype and fear among public. This pandemic scenario has been an advantage for malicious attackers to launch various cyberattacks and disrupt services for financial gains.

The following is a quick summary of few cyber security attacks that have and could take place during this pandemic.

- **DDoS Attacks:** Distributed Denial of Service (DDoS) attacks have affected the normal functioning of government and healthcare institutions by crashing their websites and thus, interrupting their communication channels.
- **Spam Emails (Phishing Schemes):** Scammers and hackers have sent corona virus related emails containing malicious attachments for financial gains and to promote their evil intents. They pretend that the email is from organizations like WHO and ask them to donate or provide personal information in awake of the pandemic.
- **Malware:** In this current pandemic situation, a user wants to know the spread of the virus in his/her locality/district/state/country. Interactive corona virus maps and websites can be embedded with malwares, spywares and trojans which when clicked can take control of the users' device. These devices then can be used for DDoS attacks, spam campaigns, malware spreading and other malicious activities.
- **Ransomware:** Institutions in healthcare and education, financial institutions, and government organizations cannot afford to be locked out of their systems. Cyber criminals launch ransomware attacks via phishing emails, malicious websites, or already infected or compromised systems with the aim of holding them at a ransom.

This malware or ransomware once installed can not only encrypt the user’s data but also steal information and passwords and lock the user out of their own systems.

- **Malicious Social Media Messaging and Browsing Apps:** Almost every individual uses the social media platform and downloads apps to gain quick access to information. Hackers use scams like free subscriptions and phishing tactics to redirect users to malicious links, or websites asking them to share their credentials or personal information or install malware or infected apps in their devices.

With work from home procedures in place, institutions face an increase in attacks which has generally been caused by employee negligence. Human errors lead to cyber security risks which in turn cause the above-mentioned cyber security attacks.

- Weak passwords or repeated passwords across personal and business accounts are easier to exploit for cyber criminals. Proper password policies, using passphrases, banning repeat passwords, using password managers can help.
- Information or file sharing becomes very important in a work from home scenario. Sensitive information when intercepted can lead to identity theft, ransomware attacks and much more. Encrypting the data, using digital signatures, using secure platforms can help.
- Home Wi-Fi networks are also at a risk as software updates are often ignored, firewalls are not installed. Updating the software regularly and installing a hybrid router firewall will help to overcome this risk.
- Personal devices like smartphones, home printers, personal desktops have security gaps which can be exploited by hackers. Encrypting the data, using an appropriate antivirus can help secure these personal devices.

The most important element of effective security in a time of change is to realize that while you can do anything, you cannot do everything. Security is never "finished" because the opponent is never finished; cyber criminals are endlessly innovative and adaptive. In the words of Winston Churchill, "Never let a good crisis go to waste." Use this as the chance to start a new, ongoing security dialogue within your business.

Bhavesh D. Shah

Asst. Professor

ROLE OF TECHNOLOGY AND INNOVATIONS IN SUSTAINING ISOLATED LIFE DURING COVID-19 PANDEMIC

Self-Isolation using technology

As the world is dealing with the most devastating situation of pandemic with great valour, people who are suffering from this disease also have to deal with lot of devastation mentally as well as physically, in the self-isolation phase. The article is written by having an interaction with people who had gone through this mode. Self-isolation time is the most difficult time which demands love and care from the loved ones, which is not possible since the disease is contagious.

The article talks about dealing with such depressive state in the self-isolation situation using technology. The article is influenced by two ideas. Firstly, a mobile based application which can be implemented for younger crowds, who are physically strong to perform their routine activities but needs motivation to deal with the stress of remaining isolated from the loved ones. The mobile based application for self-isolation will be configured with features like medicine reminders, meal and water drinking notification, timely motivational messages and also would have options for playing meditating music. The app will also have an appointment with the counsellors so that the patience should not go into stress or depression while recovering. It will have features for reviewing the conditions of the patient with a daily feedback which will help the doctors to track the recovering state of the person in self isolation. This is an idea which needs a dedicated implementation for sustaining healthy mental life in isolation phase.

Secondly the IOT based system can be a robot which will perform all household task and would also be a companion for the person in isolation. Amazon’s Alexa or google assistance would listens to the instructions given by the person and give search results accordingly but robots will give a feeling of some human to be around for taking care and listening. The sale of robots has increased drastically in the logistics as well as in medical sectors during pandemic, but this can also be a good option when it comes to dealing with patients in self-isolation. If a patient is not taken care properly in self isolation, there are changes that he might develop some other severe mental issues or would take longer to recover. A companion is needed in this stage of pandemic, which can be tackled using robots. Hospitals, in Italy, are making use of Robots to disinfect patients’ rooms, using ultraviolet-C light to kill the virus, a robots from a company named TIAGo have been designed to deliver food to the patience on timely manner. These features can be combined together in a compact robot, which will be very helpful for people who are lonely and need some motivation in this difficult time for sustaining their life. Robots will perform the daily household task, would also be a counsellor and a motivator for the patient when the actual human counsellor could not reach out to them in isolation stage.

Seema Vishwakarma

Assistant Professor

Digital Twins- A Dynamic Digital Representation

Introduction:

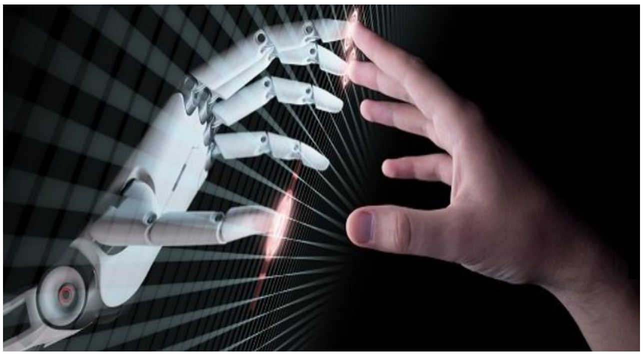
Digital Twin Technology is one among the strategic technology trends named by Gartner Inc. in 2017. Digital Twin concept represents the convergence of the physical and the virtual world where every industrial product will get a dynamic digital representation. Throughout the product development life cycle, right from the design phase to the deployment phase, organizations can have a complete digital footprint of their products. These “connected digital things” generate data in real time, and this helps businesses in better analyse and predict the problems in advance or give early warnings, prevent downtime, develop new opportunities, and even plan better products for the future at lower costs by using simulations. All these will have a greater impact on delivering a better customer experience in business as well.

Digital twins in the industry

The fourth industrial revolution or Industry which embraces automation, data exchange and manufacturing technologies is at the talking point of the business world. Digital Twins is at the core of this new industrial revolution bringing in unlimited possibilities. It changes the traditional approach of ‘the first build and then tweak’ in the industrial world and brings in a more virtual system-based design process that brings in the much more efficient role out of any equipment or system by understanding its unique features, performance, and potential issues if any. With Digital Twin, an operator can get trained on a virtual machine without spending for a dedicated trainer or simulator. With the further evolution of Machine Learning and Artificial Intelligence, the future is not too far for the machines to take the autonomy to the next level. In such an autonomous world of industrial machines, the role of Digital Twin will evolve, and we can witness increasing self-awareness in the machines. Such machines will be capable of optimizing its performance, coordinating with other machines, doing self-diagnosis, and self-repairing the faults if any, with minimal intervention from a manual operator. No doubt, there is an exciting future to get unfolded in the world of Manufacturing and Engineering and Digital Twins is a significant step to it.

How Digital Twins work

Digital Twins, the virtual counterparts of the physical assets are created as digitalized duplicates of machines/ equipment or physical sites using sensors. These digital assets can be created even before an asset is built physically. To create a digital twin of any physical asset, the engineers collect and synthesize data from various sources including physical data, manufacturing data, operational data, and insights from analytics software. All this information along with AI algorithms is integrated into a physics-based virtual model and by applying Analytics into these models we get the relevant insights regarding the physical asset. The consistent flow of data helps in getting the best possible analysis and insights regarding the asset which helps in optimizing the business outcome. Thus, the digital twin will act as a live model of the physical equipment.



Source: https://www.happiestminds.com/insights/digital-twins/

Applications of Digital Twins

Digital Twin concept is the next big thing in most of the business sectors, which helps in accurately predicting the current state and future of physical assets by analyzing their digital counter parts. By implementing Digital Twins, organizations can gain better insights on product performance, improve customer service, and make better operational and strategic decisions based on these insights. We have started seeing the major applications of Digital Twins in the following sectors.

- **Manufacturing**: Digital Twin is poised to change the current face of manufacturing sector. Digital Twins have a significant impact on the way products are designed manufactured and maintained. It makes manufacturing more efficient and optimized while reducing the throughput times.
- **Automobile**: Digital Twins can be used in the automobile sector for creating the virtual model of a connected vehicle. It captures the behavioural and operational data of the vehicle and helps in analyzing the overall vehicle performance as well as the connected features. It also helps in delivering a truly personalized/ customized service for the customers.
- **Retail:** Appealing customer experience is key in the retail sector. Digital twin implementation can play a key role in augmenting the retail customer experience by creating virtual twins for customers and modelling fashions for them on it. Digital Twins also helps in better instore planning, security implementation and energy management in an optimized manner.
- **Healthcare**: Digital Twins along with data from IoT can play a key role in the health care sector from cost savings to patient monitoring, preventative maintenance and providing personalized health care.
- **Smart Cities**: The smart city planning and implementation with Digital Twins and IoT data helps enhancing economic development, efficient management of resources, reduction of ecological footprint and increase the overall quality of a citizen's life. The

digital twin model can help city planners and policymakers in the smart city planning by gaining the insights from various sensor networks and intelligent systems.

- **Industrial IoT**: Industrial firms with digital twin implementation can now monitor, track and control industrial systems digitally. Apart from the operational data, the digital twins capture environmental data such as location, configuration, financial models etc. which helps in predicting the future operations and anomalies.

Conclusion:

Digital Twins which incorporate Big Data, Artificial Intelligence (AI), Machine Learning (ML) and Internet of Things are key in Industry and are predominantly used in the Industrial Internet of Things, engineering, and manufacturing business space. The widespread reach and usage of the Internet of Things have made the Digital Twins more cost-effective and accessible for the business world.

Geeta Sahu
Assistant Professor

Role of Technology and Innovations in sustaining isolated life during COVID-19 pandemic

Isolation a depressing word to overcome sadness or environmental pressure or state of suppressed health by a human being. But we humans never thought a regular day of our life would suddenly go for a state of isolation with unknown time clause as well as unplanned vision. A prediction says that the number of over 50s experiencing loneliness will reach 2m by 2025/26[1] certainly a bad value and when we are talking of physically impaired people to sum it up, we are still a long way to go to overcome isolation techniques. When we feel lonely as well as rejected, brain regions associated with distress and rumination are activated instead. Lonely people also have a even greater negative focus and anxiously to examine people's intentions. Sometimes this can become so strong that it makes us feel even more lonely – creating a brutal cycle.

In this article we are talking about the current trends of technology already adopted by people while work which in under research.

The foremost to top the chart are.

Robot Companion: The future does not long too long and having a robo as a family member is no more distinct thought. Countries like Japan have instated this practice to help the age-old group.

Home care kit: It's a mechanism of monitoring the daily routine of loved ones by making use of sensors and plugs, extracting data from this devices analyse the data and verify the day-to-day moment of individual.

Having a customer support team: This team really needs to be on toes as a person with isolation would certainly face any other disorder so keeping a trace of the calls placed by them also the frequency at which they are been placed is what a customer support team needs to do.

Smart speakers: Smart speakers such as Google Home and Amazon's Alexa are powerful tools. These voice-activated devices act as a bridge to the fountain of knowledge on the internet. The voice interface means for those who might be socially isolated; they get to hear their voice in the room and to get a response creating a sense of dialogue.

Being active on various platforms: Technology has shaped emotions and habits long before Instagram likes and Twitter retweets. A study has shown that Users on the internet are 38% less likely to rely exclusively on their spouses/partners as discussion confidants. Those who use instant messaging are even less likely, 36% less likely than more internet users, or 59% less likely than non-internet users to rely exclusively on their spouses/partners for important matters. People who are using the internet to upload pictures to share online are 61% more likely to have discussion partners that cross political lines. Maintaining a blog is associated with a 95% higher likelihood of having a cross-race discussion confidant. Most Common at home users on the internet are also 53% more likely to have a confidant of a different race.

Immersive Technology: Making use of the concept of virtual reality which withholds families to playing games, watch videos, and forge memories. The platform utilizes neuroscience to offer activities for cognitive stimulation, socialization, and therapy, even helping users recreate meaningful memories.

Building accessible devices: Those less attuned to new-the-state of art technology can also benefit from anti-loneliness tech. The end user while using these devices only make use of single button to share or communicate with the other party.

Reference:

1. https://abilitynet.org.uk/news-blogs/how-use-technology-reduce-social-isolation
2. https://theconversation.com/the-neuroscience-of-loneliness-and-how-technology-is-helping-us-136093

Mithila Chavan

Assistant Professor

The Role of Telehealth during COVID-19

Telehealth is the use of digital information and communication technologies, such as computers and mobile devices, to access health care services remotely. Telehealth services helps in preventing, diagnosing, treating, and controlling diseases during COVID-19 outbreak. The World Health Organization (WHO), after the large expansion of SARS-CoV-2 virus, declared the state of pandemic by coronavirus 2019 disease (COVID-19) on March 11, 2020. The COVID-19 outbreak has triggered the lockdown of populations worldwide, strongly affecting daily life, as well as most health systems, which have been faced with the management of patients.

During the Lock down time the telehealth process helped to reduce the risk of exposure to the patients. The utilisation of telemedicine has had positive impacts in the public health emergency beyond facilitating triage, including allowing the rapid deployment of large numbers of healthcare providers and the providing of services when local hospitals and healthcare centres are unable to meet demand. Telemedicine has been a means of providing healthcare information not only to infected people but also to non-infected people during this infectious pandemic.

Various Telehealth apps are

1.Doctor on Demand

Doctor on Demand is a popular telemedicine software that believes in supporting healthcare wherever you are. They have an experienced panel of certified physicians and psychiatrists who are available on your schedule. Accessible 24 x 7, this application connects with the doctors via a live video. It investigates a variety of health categories like behavioural health, urgent care, preventive health, and chronic care. It reduces the waiting time provides quick access to doctors on pre-defined time schedules.

2.Amwell

Amwell is one of the applications that facilitates patient’s connection with the desired doctors, from the comfort of your home, not compromising on any health benefit. It is said to have reduced the patient’s waiting time by almost 70%. This app offers a variety of health plans and nursing facilities that can be availed online, covering from urgent care to acute care.

The Telehealth process expands access to care and reaches more patients and improves patient satisfaction.

Akshatha Jain

Assistant Professor

Advent of advanced wearable device for self-quarantine

India’s war against the deadly second wave of COVID-19 continues, and both governments and civic bodies are working tirelessly to ensure resources reach on time. However, loopholes and lapses seem unavoidable, posing a risk to citizens’ safety. The corona virus and this amid pandemic situation have made people highly health conscious. Wearing masks and social distancing is the new normal. One of the key gadgets’ doctors are recommending is an oximeter that can measure blood oxygen saturation or SpO2 levels to understand each COVID-19 patient’s condition.

The situation before pandemic where early mornings and cool evenings are when people used to step out of their homes to exercise – walk, run or jog. And to achieve their fitness goals technology rather smart wearables came in picture. With changing lifestyles and habits, the demands of consumers from their fitness trackers have changed. While earlier fitness trackers could only serve the purpose of keeping count of steps taken by the user, the latest ones can do much more. Many offer advanced health features such as heart-rate monitors, oxygen-saturation (SpO2) monitors, calorie counters, and sleep monitoring to ensure that the users always keep track of their health.

As per government advisory, SpO_2 is an important indicator for pneumonia symptoms. During the self-isolation period it is difficult for an individual to keep the details of the Oxygen level time-to-time. Using this smart band one can easily track the oxygen level, heart rates without any hesitation. This also can help big isolation centres to track the oxygen levels of majority of the patients instead of visiting each patient individually. Looking at the sudden increase in number of Patients in March 2021, its difficult for doctors and nurses to handle and record their condition individually. Smart wearables can help the doctors & nurses to get the data of number of records on the go. And can give right treatment as soon as possible.

The data collected will also help Covid Centres to estimate the number of Oxygen cylinders required the next day or may next week. And can make the provisions accordingly. They are some cases where the symptoms are common like in case of Severe cases. Serious symptoms are difficulty breathing or shortness of breath, chest pain or pressure, loss of speech or movement. If the bands are designed in such a way that if they focus on measuring these 3 areas, then it will be of great help to the Medical Officials to give treatment right at that time.

We can use this wearable health bands in two scenarios. 1. Self-isolation 2. Covid Centres. In Self-isolation case, this band will keep on updating their family members regarding their health condition such as heart rate, Oxygen level & body movements. So, a person who is away from this patient can have detail information about whoever kept in self-isolation. Also, can call Doctors during emergency. In the Covid centres we can make these wearables available for the patients.

Following are the expected challenges to implement the same:

1. Making it available at low cost.
2. If we reuse the same band, how to sanitize it before reusing it?

Therefore, implementing such technology during such situations can be helpful to give right treatment at the right time. But the cost involved as well as the maintenance required to buy such devices is high.

References:

1. https://www.who.int/emergencies/diseases/novel-coronavirus-2019
2. Frontoersin.org
3. Sage journals
4. News18.com/news/tech/oximeter
5. Financial times

Madhavi Amondkar

Assistant Professor

- ***Editorial Team :***

Mr. Makarand Deshpande
Ms. Maitreyi Joglekar

VSIT | Vidyalankar School of Information Technology

Vidyalankar Educational Campus, Vidyalankar Marg, Wadala (East), Mumbai - 400 037 Maharashtra, India.
Telefax: +91 22 2416 1126 | Email: principal@vsit.edu.in

Follow Us:

www.facebook.com/Vidyalankar.VSIT twitter.com/VSITCollege www.instagram.com/vsitinsta