International Journal of Multidisciplinary Sciences and Arts

E-ISSN : 2962-1658
Volume 3, Number 4 , October, 2024
https://doi.org/10.47709/ijmdsa.vxix.xxxx

# Ensuring Information Integrity in a Mobile-Connected World

**Nahid Neoaz[1], Mohammad Hasan Amin[2]**
[1]Wilmington University, USA
[2]Kettering University, Michigan
[1]nahidneoaz@yahoo.com, [2] amin3672@kettering.edu

***Corresponding Author**
**Nahid Neoaz**
nahidneoaz@yahoo.com

**Article History:**
Submitted: 11-01-2025
Accepted: 11-01-2025
**Published: 11-01-2025**

**Key words:** MDM, mobile security, cloud, data protection, mobile info assurance, encryption, multiple factor authentication, mobile device management, DR, data mirroring, VPN, types of mobile threats, compliancy, data access, security measures.

**Brilliance: Research of Artificial Intelligence** is licensed under a Creative Commons Attribution-Noncommercial 4.0 International (CC BY-NC 4.0).

## ABSTRACT

The sunlight adoption of portable devices in individual and business activity has made a higher urgency of appropriate mobile information assurance policies. This article explores key approaches to securing mobile devices and sensitive information, focusing on three major components: Mobile Device Management (MDM), mobile security best practices, mobile cloud computing. MDM solutions are ways through which organizations can gain control in mobile devices with secure policies, distant management, and compliance checks. In addition, best practices for the physical security of mobiles, which include the use of non-disclosed passwords, the enabling of the encrypt or and the use of virtual private networks or other such security tools go further in safeguarding mobile environments against elements like malware and intrusion. Besides, cloud computing supports portable information assurance by providing backup, recovery, and security measures like encryption, and ID confirmation. Solutions based on cloud technology allow to implement effective data sharing and processing, as well as to control data security and compliance with the requirements of existing legislation. Altogether, these measures constitute an integrated security strategy of mobile, it provides protection to sensitive data, makes them accessible, and help in managing or eradicating threats in the connected environment.

## INTRODUCTION

Presently, using mobile connectivity has become a crucial part of life for both, individuals and companies. A number of people in the society own mobile devices such as smartphones, tablets, laptops and other portable devices that have changed ways that people deliver information and execute tasks. Smartphones are no longer single instruments of communication, but access points to numerous service alternatives, including cloud services and banking, social networks, and corporate applications. With the arithmetic progression of mobile technology, knowledge assurance the necessity of assuring integrity, confidentiality and accessibility of the information has turned into a higher obligation [1]. Given the new possibilities offered by the mobile connectivity the problem of protection of the private data is rather complicated. As the users go mobile, data is moved across open networks, reside on devices with some degree of security, and is utilized by a growing field of applications and services. Laptops and smart phones for example, can easily be lost, stolen, or hacked; and the threat of such attacks have recently become more advanced making it even harder to contain them on mobile devices. In this regards information assurance emerges as a critical component to safeguard data integrity throughout the exchange while at the same time while also guarding the transmitted information from third party interceptions, particularly where the data is being transferred through less secure networks [2].

I agree with this statement as more firms integrate their companies into mobile platforms it becomes critical to protect these and their data. Using such devices as smartphones, tablets, or laptops, people receive and process data all over the place: in their homes, during business trips, or in offices that are isolated from the central office. The COVID-19 pandemic has amplified a new trend of working remotely, decreasing the earlier methodologies of security's efficiency. Firewalls, on premise security tools and solutions are unable to sufficiently protect enterprises, given the mobile working model that employees follow [3]. Therefore, businesses need to extend the concept of information assurance to include emerging realities of mobility connected world. Mobile devices as you know are among the most vulnerable to cyber criminals attack because they contain and retrieve so much of personal, financial and business related information. Different categories of cyber threats including phishing, malware and ransom ware are frequently implemented to target gaps in mobile operating systems, applications and networks. Moreover, mobile platforms dependent on cloud services are more integrated with other services where there are higher risks associated with multiple platforms, devices sharing and users. This in turn creates the necessity of establishing secure methods that are able to prevent unauthorized access, alteration or deletion of this data, as well as to guarantee the trust, necessary for turning to the potential of mobile technologies for

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

E-ISSN : 2962-1658
Volume 3, Number 4 , October, 2024
https://doi.org/10.47709/ijmdsa.vxix.xxxx

individuals and businesses [4].
However, these and several other regulatory and compliance needs pose yet another challenge in mobile security. Thanks for sharing such a useful information; many industries like healthcare industry, finance industry and government industries have laws and policies when it comes to collecting, storing and using data information. For instance, GDPR across the European Union and HIPAA across the United States include certain standard practices to preserve privacy across server data and anything that is in transit, including being accessed on or relayed through a mobile device. Such regulations have to be obeyed by organizations, otherwise, sanctions involve high penalties, loss of reputation, and customer trust [5]. Additional changes in the uses of mobility, cloud technology, and IoT add pressure to the task of achieving information reliability. Because of mobile interactions with cloud services, remote servers, and other devices, this threat vector is growing. Protecting information in this scenario requires different approaches that incorporate encryption, mobile devise management and multi factor authentication in order to protect the information when in transit. An evolution towards information assurance throughout a mobile-connected environment is due to the mobile usage in accessing, storing, and sending sensitive information [6]. How mobile technology develops, the same way, the tactics and technologies developed for defending such info must progress. Mobile security embraced by effective information assurance practices should be employed to protect the private and integrality of data as much as possible as threats continue to emerge. The exciting opportunities available in mobile technologies provide individuals and organizations with the means to effectively enter the world of mobile confidently, even with the existence of threat that accompanies mobile data [7].

## MOBILE SECURITY THREATS AND WEAKNESSES

Since mobile devices have become an essential point of person and business processes and events, mobile threats and exposure have also increased greatly. Whereas, Mobile technology that creates ease and more efficiency, is also one of the greatest concern in information assurance. The parameters that define mobile connectivity, such as constant connection, portability, and usage in unfamiliar networks, make a constant threat vector to sensitive data. It is necessary to learn more about those risks and threats as these insights enable the planning of the most effective security measures which would address the problem of data protection both for an individual and an organization in the context of mobile-connectivity [8]. This paper identifies data leakage attacks as one of the main threats as related to mobile devices, it refers to a situation in which confidential information is stolen by unauthorized parties in the course of the manufacturing, enhancing, selling, purchasing, utilizing, or disposing of the gadget. As for the mobile category, smartphones, tablets and laptops are creating, storing and processing personal and business information, which makes them particularly attractive to hackers. Phishing, MITM attacks and malware some of which have lately affected even reputable organizations threaten devices and make confidential information easily vulnerable. They may target even the mobile operating system, the set applications, or the network connectivity [9].




Figure: 1 showing top mobile security threats

In mobile security there is one more important problem associated with exposure to malware contingency. Virus, Trojan and ransom ware are a type of program malicious software can and is transferred by apps, links and downloading. This we find out due to the prevalence of the mobile operating system software's such as Android and IOs which make hackers most engaged on how they could penetrate into the operating systems. For example, on intrusive applications which target

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

E-ISSN : 2962-1658
Volume 3, Number 4 , October, 2024
https://doi.org/10.47709/ijmdsa.vxix.xxxx

at embezzling data, spying the phone's users, or even introducing ransom ware on the phone, it will appear as an original looking application [10]. Later such programs fully take control of watching the user's actions, reading or writing data, or even locking files and demanding a cash amount for the files decryption. Yet another weakness arise from cases where insecure networks have been employed. There are two particular examples of Internet on portable devices; Wireless fidelity and cellular network data. Despite the usefulness of the wireless networks, they are insecure, and wireless internet connection in an airport, café or other public place or hotspot for instance is insecure. These open network can easily be tapped and a common man in the middle attack is carried out by the attacker to monitor all the communication that goes on between the device and the network. Things such as password like Google, emails, any other significances things and even financial transactions can easily be hacked if the connection isn't encrypted [11].

The other regularly detected fluid security threat that is being found in operating systems is the operating system vulnerabilities. There are several problems that occur specifically and uniquely with two most common mobile platforms: Android and iOS. You just know hackers are always out there, sometimes using an older version of the software which means you are aware that it has certain holes which hackers can poke [12]. However, Google and Apple, who provide the above operating systems, regularly generate releases targeting the issues in question, while the users of the devices/ operating systems in question, habitually postpone, or often, outright ignore the updates that these companies regularly provide, which fix the holes above with fair frequency. The case is that the Android ecosystem is divided into many vendors, every one of which issues updates at different paces that causes issues with maintaining the safety of the devices.

Mobile application usage also has a number of risks namely [13]. In this case there is high tendency to find out that many of applications contain security flaws, for instances those with free downloads or downloaded from the third-party software. Some of these apps may require many privileges which may otherwise collect information not needed by the application or which may be misused. However, bad apps may not have sufficient lack of security measures such as, encryption or the password, and thus can lead to unauthorized use [14].

Other loss which may not be overlooked is loss or theft of mobile devices. These devices are in most times portable, and therefore, can easily be lost or even stolen more often than, for instance, conventional computers which are not moved most of the times. If a corresponding mobile device holds certain information and it is left without powerful passwords, encryption or other protective means, the issue on how various other people can enter the information stored in it becomes quite critical. Also, lost device could be lost irretrievably, which makes them have a higher likelihood of leakage or the third party using it [15]. What is more, there are some new opportunities to be opened with app-based and cloud-based integration. This becomes a challenge when people and companies store data on the cloud and store, retrieve from, and work on information on their phone. A violation in one app or a cloud service equals violated all the data linked through the devices and the services [16].

The vulnerabilities of mobile devices can indeed be viral and network and originating from the os weaknesses, and physical loss. This is an overview of potential risks and an important first step towards establishing sound security policies for the often complicated aspects of personal and business security threats. Mobile threats can be rounded with good high level of encryption, use of secure networks, and frequent update of the software and abeyance of the mobile security policies [17]. By the same token – due to the dynamics typical for the mobile environment – what has been described above will not be the last problem of how to protect data from unauthorized access.

## THE BASIC PREMISES AND STRATEGIES ON MAINSTAY OF DATA COMPLETENESS

Thus and hence, its? Admissibility in mobile settings depends on familiarization with inherent Information assurance or security principles as well as applied security methodology. The responsibility for the control of data is important for guaranteeing that data are absolutely correct and have not undergone alteration from the time of the data collection up to the time it will be used [18]. In the context of mobile devices this means the set of measures aimed at protection of stored information both from unauthorized and unwanted access/interference and changes, and from accidental damage or loss, as well as on the possibility of the above-mentioned information use as necessary. Thus, IA principles have to be applied by organizations and individual users and then specified IA strategies should be used to mitigate a threat and to ensure information protection [19].

### IA Fundamentals, or the ten Principles of Information Assurance

The core principles of information assurance, often referred to as the CIA Triad, are critical to maintaining the integrity of data:

**Confidentiality:** This principle takes special effort to ensure that information is only allowed to be accessed by allowed users or systems only. It defines the way of protecting information from those who are allowed or actually not allowed to access that information. Among them, confidentiality is the most widely needed security characteristic, which is intended to protect data stored in mobile devices or distributed over a network, the solution to which involves the use of encryption methods. In situations where data is encrypted then for example if an attacker gets to the data he will not be able to use the data or understand it [20].

**Integrity:** According to its life cycle, integrated data can fairly simply be described as the quality and consistency of data. It also ensures data consistency that is in storage and during the transfer process. To do this it is essential to exclude damaging from lowering the quality of a database, in general it is important to prevent or protect data from being changed. Some common techniques which are used in an effort to promote integrity of information include hashing, checksums,

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

E-ISSN : 2962-1658
Volume 3, Number 4 , October, 2024
https://doi.org/10.47709/ijmdsa.vxix.xxxx

and Digital signatures. These methods also allow a user to find out whether or not the data has been corrupted and it can also ensure that data obtained in the mobile device is not corrupted [21].

**Availability:** Availability provides certainty that data will be available and accessible at call without any disturbance. Regarding mobile devices it means being able to arrive at the data at any time and from any location without facing unnecessary downtimes. It is commonly supported by a number of solutions for redundancy, backup services for the data as well as services connected with cloud computing. However, the problem that relates to mobile context only, like network coverage, battery capacity, host device capabilities must also be handled so that it allows the steady connectivity to requisite data [22].

## SOME INITIAL APPROACHES FOR KEEPING DATA AUTHENTICITY IN A MOBILE ENVIRONMENT

Beyond these core principles, several strategies can be employed to ensure the integrity of data in mobile environments:

**Data Encryption:** That will be why confidentiality and integrity are probably two of the most central types of security needed when storing or processing data, and also the clearest ways to achieve that are encryption. Mobile devices it should incorporate encryption for data that is embedded locally in the device (local data) and when a device is sending data over a network (switching hosts) that are intended for use. End to end encryption makes it harder for any means in between to be intercepting the data without the consent of the sender and the receiver. For example, iOS and Android mobile operating systems both with pre-installed encryption utility able to encrypt the device data on its own [23].

**Multi-Factor Authentication (MFA):** Security of mobile devices involves the use of authentication. Since mobile devices can be lost or stolen easily unlike other static devices like PCs, there is high likelihood that those engaging in operations need to be verified through multi-factor authentication (MFA). MFA uses what the user knows such as a password, what the user has such as a mobile phone or token and what the user is such as finger prints or facial identification. When people chose complicated password, or use two-factor authentication, it will be harder for the people with intend of intrusion to do it [24].

**Mobile Device Management (MDM):** Companies would simply use the Mobile Device Management (MDM) system to control and secure the mobile devices that connect to the Company's data. Through MDM, organization policies can be set to guarantee that the devices are secure and any data that got into the wrong hands can easily be wiped away from lost or stolen gadgets, further, all gadgets and devices should conform to the business security policies and protocols. Another reason that MDM is beneficial for organization is the ability to check health status of the device and modify security settings; this becomes crucial, if the organization needs to protect its data from invasion and assure the integrity of the information stored on devices [25].

**Secure Mobile Application Development:** Data integrity is also maintained through protecting those applications that the users use on their mobile device. Since most applications are used publicly it is always open to attack if not coded well or frequently upgraded. Engineering for secure code, updating and vulnerability testing are some of the exercises that must be done while developing apps that do not compromise data to other risks. To ensure there is no leakage of sensitive information to the unauthorized the developers should also incorporate right authorization and authentication module in the mobile apps, so that the users are able to use only the data or the parts of the apps which he or she is allowed to use [26].

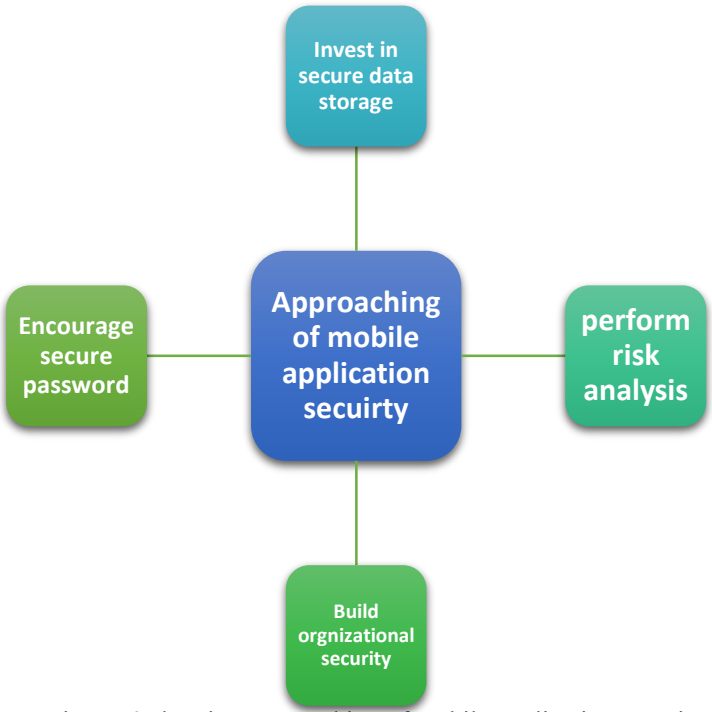



Figure: 2 showing approaching of mobile application security

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

E-ISSN : 2962-1658
Volume 3, Number 4 , October, 2024
https://doi.org/10.47709/ijmdsa.vxix.xxxx

**Data Backup and Redundancy**: This means, data integrity is not only securing unauthorized access or change to data but also to assure the availability of the data in the occurrence of its loss or damage. Availability and data integrity call for periodic backups and data backup systems as well as having standby systems. In environments where mobility is inherent, it means utilizing services in cloud or remote servers that can make backups. Backups provide safeguard in the situation when any device fails, or when a user accidentally loses certain data as frequently we do, consistent backups reduce time wastage and chances of experiencing a loss of data [27].

**Regular Software Updates and Patches:** Arguably, one of the least glamorous but most effective best practices for accomplishing integrity and avoiding compromising its loss through mobile use is basic;

Ensuring that the mobile devices on the network are running the latest software. Operating mobile systems, applications and security tools invariably generate new editions to counter the emergent vulnerabilities and enhance the effectiveness. The constant update of software mitigates the exposure to risks from the identified open doors to compromise; making the device and data safe from new threats [28]. Thus, addressing the challenges and requirements of a mobile-connected world need to involve both the set of guidelines for information assurance and specific security measures. Essential principles of safeguarding include confidentiality, integrity, and availability of data, while relevant countermeasures are, inter alia, encryption, multi-factor authentication, and regular updating of software commonly use in mobile surrounding. That is why, today, much can be done to ensure that mobile security poses no threats to data and, at the same time, data may stay secure, trustworthy, and easy to access if necessary [29].

## EXPLOITING THE PROSPECT OF MOBILE DEVICE MANAGEMENT (MDM) FOR BETTER SECURITY

MDM has emerged to be a critical solution for Mobile Device Management in securing adopted mobile devices especially for business entities. It is becoming even more complex as many organizations embrace the use of mobile devices such as Smartphones, tables and laptops among others. MDM solutions offer a mechanism of keeping track and controlling the mobile devices operated by the employees, contractors, or other users of an organization's facility. With policies, ability to oversee devices from remote location and allowing for deletions in case of lost or stolen devices, it has become critical, especially in mobile-connected scenarios to deploy MDM solutions for the safety of corporate data [30].

**MDM stands for Mobile Device Management, but what really is it?**

MDM is a vernacular for a comprehensive set of technologies and instruments deployed to track, manage, and protect portable devices in business or organizational context. It helps IT executives to create policies and guarantee that company-owned or employees' (BYOD –Bring Your Own Device) mobile gadgets meet certain safety requirements. MDM can comprise management of settings, resident applications and data and vigilance on the security state on the devices to avoid accessibility by unauthorized individuals, compromise of data or invasion by malware [31].

**Key Features of MDM Solutions**

**Remote Device Management:** Another positive aspect of the MDM tool is a possibility to manage and control mobile devices from a distance. From the management console administrators can modify the security to the desired settings, set up VPNs, add or delete applications, and view health status of the device. This implies there would be a centralized management of security and standards to meet on all those devices without having to touch the physical versions [32].

**Enforcing Security Policies:** Through MDM, it becomes easy for an organization to enforce policies on the mobile devices in question; this includes password complexity, encryption and use restrictions including camera and app installations. Through these policies, MDM guarantees that such devices meet the required security required to safeguard such information. For example, through MDM, it is possible to set a device to encrypt before connecting to the corporate network, or to allow some apps on the device [33].

**Relocation and Tracking:** Mobile device management tools sometimes come equipped with filters that help administrators detect the location of devices physically. It can be handy in the search for stolen devices and for better performance of device search operations, as well as prevent unauthorized access to certain material. Geofencing can also be applied to restrict or possibly supervise the device usage whenever the device enters or exits some region [34].

**Remote Wipe and Lock:** Perhaps the most important aspect of MDM is the utmost control over lost or stolen device erasure of all relevant data. If for example a device is lost or stolen the administrator is capable of wiping all the corporate data and locking the device to avoid misuse. It is useful especially in scenario where physical device itself is stolen, data encrypted cannot be obtained by unauthorized person [35].

**Application Management:** Mobile device management solutions can be applied to manage and all Apps on the mobile devices. This also comprises elements such as, having the right to permit or block the applications which should be or should not be used on the company assets. Furthermore, MDM can enable it so that apps are automatically updated and eliminate any app that is stale or possesses security flaws [36].

**Compliance Monitoring:** The measurability of security is a major concern for organizations that are in regulated industries as there is a lot of concern with whether or not organizations are meeting the security standards as well as security regulations that are in place. MDM tools give a capability of being capable of tracking whether devices are complaint with various types of legal requirements like GDPR, HIPAA or PCI-DSS in that they should be configured in certain manner and that they should have certain forms of security applied to them. This can allow administrators to create alert when a device is out of compliance and this makes organizations reduce on the cases of noncompliance [37]. MDM for Mobile Security With the help of mobile device management, businesses can experience several advantages among

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

International Journal of Multidisciplinary Sciences and Arts
E-ISSN : 2962-1658
Volume 3, Number 4 , October, 2024
https://doi.org/10.47709/ijmdsa.vxix.xxxx

which it is necessary to distinguish the following:

**Enhanced Data Protection:** Through using encryption, password protection, and wiping of device content remotely, MDM makes certain that corporate data is secure in the event that the device is lost or stolen. These features keep the information which is stored in the device and which is on the move safe and secure, in addition to protecting the data and making certain data has not been altered in a bad way [38].

**Improved Device Visibility:** MDM helps to provide an exclusive overview of the status and the health of mobile devices at the organization level for the administrators of IT. By being visible, organizations can check patterns of usage throughout the devices and also review the security positions throughout the devices, thereby being able to identify any weaknesses to be addressed before the problem deteriorates into other cases of security breaches [39].

**Streamlined IT Operations:** With MDM, the IT teams are able to control a large number of devices at once, yet without having to touch each device individually. This helps IT administrators in avoiding more efforts and time that is required in enforcing mobile device management policies and at the same time they get to guarantee that mobile devices in the business are both secure and adheres to company standards [40].

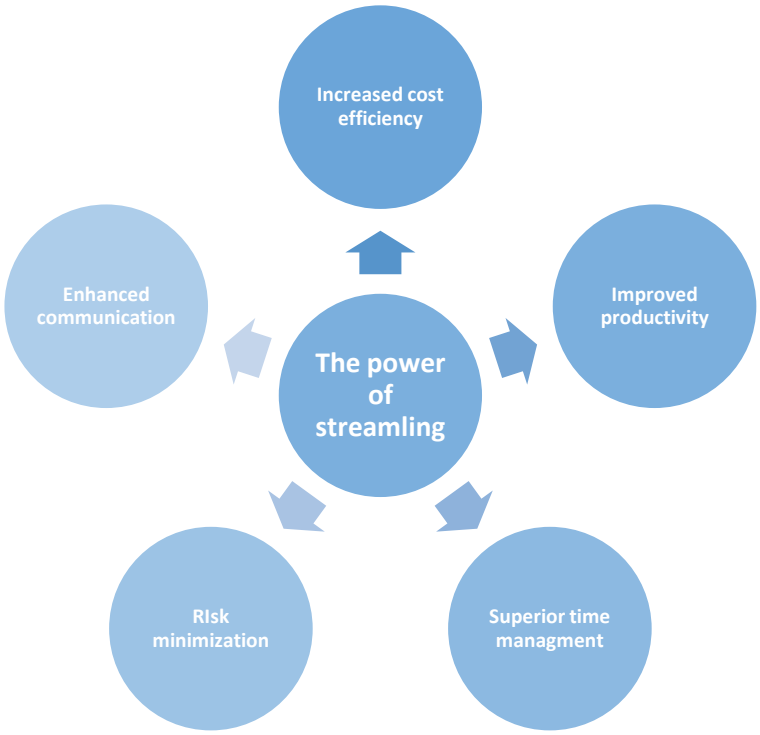



Figure: 3 showing the power of streaming

**Support for BYOD Policies:** Since more organizations allow their employees to use their personal devices for work, MDM is necessary to ensure that these devices complied with corporate security policies. MDM enables businesses integrate personally owned devices in their networks while at the same time maintaining security policies that do not encroach on the rights of the users. This creates a balance between security and user autonomy, which is the major point of having the system in the first place [41].

**Reduced Risk of Data Breaches:** Since MDM allows management of devices from a distance, controlling security measures, and possible leakage of data through lost or stolen or tampered with devices is minimized. The option for data deletion in the event of loss or theft is the major contribution that minimizes losses from unsecured items. From the discussions above it is quite clear that MDM solutions are crucial components in managing the mobile security in today's world. MDM strengthens data protection since it offers the administrators means of enforcing security polices, tracking down devices, and remotely managing mobile devices [42]. This feature allows tracking of the devices, installation or removal of applications as well as wiping of data reduces risks posed by the devices. MDM is a solution that helps manage, control and secure mobile environment and corporate data especially considering that threats of mobile security are developing rapidly and the usage of mobile devices involves serious risks for a company [43].

**To ensure that personal information is protected through the use of mobile devices the following are recommended;-**

With the usage of mobile devices and portable gadgets increasing day-by-day, it is high time to pay specific attention to security and safe protection of the unwanted transmission of important personal or business-related information. Most of these devices contain and share important data which includes social information, financial information and other important business information. But they are also exposed to different sorts of risks, such as data leakage, virus, and

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

E-ISSN : 2962-1658
Volume 3, Number 4 , October, 2024
https://doi.org/10.47709/ijmdsa.vxix.xxxx

hacker attacks [44]. However, in order to protect such information, there is need to implement a number of mobile security best practices that offer good protection. These best practices protect the confidentiality, integrity and availability of data; thus minimizing the probabilities of data compromise.

**Use Strong Passwords and Authentication:** In a way, one of the most fundamental and fundamental measures of mobile devices and sensitive information that is stored in them is the use of passwords as strong and different as possible. It is also obvious that passwords that cannot be classified as strong can be easily cracked opening the device to unauthorized access. However, users should use strong passwords with letters in both upper and lower cases, numbers, dollar signs and periods etc. Additionally, to manage passwords sometimes a person has to use different passwords for different accounts or services, and for this reason, it is recommended to use passwords and to generate them with the help of a password manager [45]. Nevertheless, passwords should be strong, and in today's world, there should be emphasis on the use of Multi Factor Authentication. MFA entails the submission of two or more pieces of identification details to access a device or application; for instance, a password and a code, which is sent to the user's phone, or a biometric factor like finger print or face recognition among others.. This greatly minimizes the likelihood of vulnerabilities that allow an attacker past the password barrier [46].

**Enable Device Encryption:** Mobile security is probably one of the most demanding issues nowadays and encryption is considered one of the most efficient methods of protecting data on portable devices. Device encryption simply converts any data on a mobile device into an encrypted form that cannot be understood by anyone else apart from the owner. And especially important for data that needs to be protected in case that the device is lost or stolen. Android and iOS enable their operating systems with basic encryption attributes that can be toggled for the protection of this data. This means that even if a hand held device is lost or stolen, the information on it cannot be accessed by anyone who is unauthorized to do so [47].

**Install Security Software and Keep It Updated:** Personal computer security tools like antivirus and anti –malware application for mobiles can help safeguard such gadgets against other strands of dangerous software including ransom, spy, and adware. The anti-malware programs can help in real-time through a scan for threats on apps as well as files. The other important thing that users should do is to update their security programs to the latest version they provide for the programs to deal with the latest threats. Android, iOS and other mobile operating systems can have some level of automatic security update but the user must also allow the update of third-party apps to be safe [48].

**Be Cautious with App Permissions and Sources:** Mobile applications many time require permissions on the device to use some of the features which include a camera, microphone, location and contact list among others. As much as these permissions can be useful to enhance the functionality of the app, users caution should be applied when granting permission to the app since some may have undue effects. People should only agree to permissions that are important to an application and should not allow an application to get information that they do not want to share. For instance, a photo editing is not required to access your contact list as a weather app does not require access to your camera [49]. Moreover, there is keen importance to get apps only from authorized sources for instance, Apple App Store, Google Play Store. Apart from infamous Android apps, malware and data stealing possibilities are potentially higher in apps downloaded from third-party websites. Users should take their time also to look at reviews and ratings of the apps they wish to download to avoid downloading fake and vulnerable apps [50].

**Use Virtual Private Networks (VPNs)**: Naturally, man-in-the-middle attacks can occur in open Access Point (AP) networks which people employ in coffee shops, airports and hotels with different levels of security. Connecting with Public Wi-Fi: When connected on Public Wi-Fi, the hackers also get a Benefit of spying on the information exchange that happens on the connection of that particular Wi-Fi network. This would imply that for security of data on these networks, the users should employ use of a VPN [51]. A VPN will secure the linked connection to the internet and so it will be safe from hacker's malicious activity. Everyone who tries to use his or her social media account at work or anyone who uses his or her social media account while being on working place or spends his or her time on any public Wi-Fi networks because it supplements a powerful shield for information transfer [52].

**Regularly Update Operating Systems and Apps:** This is done by having the new mobile operating systems update that has some features and up and which is normally in the market comprising of fixes to new vulnerabilities. Such operating systems still contain threats that could be acted on by hackers provided that these updates are not installed. Therefore, updates of both OS and installed apps should be enabled in order to protect the device from various types of threats. Moreover, properties imply that applications change often and the users should expect them in particular if the new versions contain security fix and have enhanced performance. The previous versions of the apps have those vulnerabilities which the attackers can exploit, and so, it is necessary that the devices should update the apps [53].

**Implement Remote Wipe and Device Tracking:** In the case of a lost or a stolen gadget the desired capabilities are to be able to securely erase data in case the gadget is regained and to also find out where the gadget is. All of the most demanded kinds of portable terminals currently produced are equipped with tracking options for the user to trace his/her phone in case it has been stolen. In case the device is lost and cannot be retrieved to wipe it the user will perform a remote wipe that will delete all what is personal such as emails, photos and documents to ensure that they do not get into wrong hands. For instance, all of the Apple's find my iPhone, and Google's Find My Device offerings offer these options [54].

**Back up Data Regularly:** However, to ensure that loss of valuable data due to stealing of device, or system failure is prevented, the user regularly makes copies of valuable data. The option to backup to other external storage such as Google

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

E-ISSN : 2962-1658
Volume 3, Number 4 , October, 2024
https://doi.org/10.47709/ijmdsa.vxix.xxxx

Drive or iCloud or any third party application can also back up, contacts, photos and documents respectively. This means users must make sure that their backup solutions are encrypted to mean their data will always be safe [55].

**Be Wary of Phishing and Social Engineering Attacks:** Smart phone are also equally prone to phishing and social engineering where by the attacker aims at making the users part with their identity information such as login information and credit card information. This fraud is mainly done through emails, text or calls that are so real they appear to be genuine with the person you know the attacker. Before replying any kind of personal information to the sender of the message, one should confirm whether the sender is real, or open any links or attachments received from unknown senders [56]. Mobile security is not about using a number of tools individually, but about managing the devices used, the applications run, the network connections accessed and data encrypted. Adhering to the mobile security best practices described above is helpful in eradicating most of the risks occasioned by the use of mobile devices and securing user and or enterprise data. In this case therefore, there is need for developers to continuously learn about such threats and trends in mobile technology as well as other new security measures in order to ensure privacy and security of such information in the future [57].

## A CASE OF EXPLORING ON THE CHAIR CLOUD COMPUTING ON THE IMPROVEMENT OF INFORMATION ASSURANCE IN MOBILE ENVIRONMENT

Cloud computing is one of the aspects that constitutes current mobile Information Assurance planning. Since mobility device has become an important part of individuals and organizations daily working strategies, it is important to protect and ensure confidentiality of information that may be contained or may be getting through these devices. As researched, others have discovered that cloud computing has various aspects and importance in details including storing the data, in supporting the applications' access among other benefits and features that enhance security. This paper explores the following literatures that outlines various ways in which cloud technologies enhances mobile information assurance- the provision of protection, availability and solidity of organizations information against the contenders into the future [58].

**Cloud-Based Data Storage and Accessibility:** Mobile information assurance beneficiaries, which is the main focus of this paper, can learn from the following conventions of the cloud computing system: The safety that is associated with central storage of data. In the past, the information that a person contented on his or her mobile devices was fully stored on the gadgets and therefore, in case a person misplaced or XYZ lost their gadget then their information would also be lost. However, with Google Drive, Apple iCloud or Microsoft OneDrive storage, data can be stored in offsite servers and such data can be protected [59]. Therefore, it creates an opportunity for the person to work on the data from a different device, in case the mobile gadget is lost, stolen, or even destroyed. Cloud storage also establishes a chance to get information at any time as well as any place in case the individual has access to the internet connection. This level of accessibility makes the work more mobile and reduces the demand of the physical infrastructure in getting to business or personal information. Some of the many clouds services are typically developed with additional security measures for data including encryption and authentication [60].

**Data Redundancy and Disaster Recovery:** Cloud computing distinctive in that it incorporates backup of other information and has characteristics of disaster recovery adds advantage to mobile information assurance. The type of data many cloud providers use, is spread across many different servers and locations making it so that there is not one single point of failure. This redundancy means that in case one or more of the servers and data center is offline, the data is is stored in other servers. In order words mobile users especially have to make disaster recovery as a primary criteria for their social sites [61]. The cloud solutions also enable easy restoration in the case when there are failed or lost or corrupted devices. There is no loss of time if all data is synchronized to the cloud as such, if a user loses data or transfers data to a new device, then, there is usually little or no problem. This capability is likely to turn out to be most useful in those zones of business which point of reference for functionality is availability and continuance of data [62].

**Scalability and Flexibility:** The other advantage of cloud computing in increasing mobile information assurance is flexibility. Cloud service providers offer Hire storage services in the organization and if at some given time the demand for storage in the organization changes then hire can change the storage capacity being used to reflect this change in demand in the organization. Cloud also operates as a mediator for its users; a single user or a large enterprise prospect storing in cloud can in any one time change his or her storage quota based on demand and without the need for hardware installation [63]. It assists in making certain that whichever detail is kept as datum can be stored safely without having to worry where the future storage area will be or the capabilities of the storing hardware. In this case of security, the cloud addresses the utilization issue for the businesses since the organization can expand the security apparatus as the rest of the business. As more and more mobility gets incorporated in the workplace, IT administrators are well placed to increase security measures as well as control mobile accesses and oversee the different devices deployed in different places. This scalability is very useful when managing many numbers of mobile devices to a fleet that is needed for security and regulatory purposes [64].

**Enhanced Security Features:** Mobile information assurance is also well supported by cloud computing because it provides somewhat higher qualitative degrees of security that cannot be reached on any given single mobile device. Cloud vendors deputize with the software and technology including encryption, IDS and MFA. All these security measures provide a level of security that cannot probably be achieved on any of the mobile devices singly [65].

**Encryption:** Cloud services use cryptographic methods to apply data encryption before the data over the network and at the same time encrypt data that is being stored in the cloud servers hoping that the data exchanged between mobile devices

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

E-ISSN : 2962-1658
Volume 3, Number 4 , October, 2024
https://doi.org/10.47709/ijmdsa.vxix.xxxx

and cloud interfaces offers only secret and is secured from third parties. Most necessary have to do with more important data including account details, individual identity data and unique business data [66].

**Multi-Factor Authentication (MFA):** To this end, MFA can be provided for users who desire access to data that resides in the cloud services. As a result, if there was an infiltration into the mobile device then the details held on sever would still be behind an extra layer of security which is often in form of fingerprint or a one use code [67].




Figure: 4 showing benefits of multi-factor authentication

**Intrusion Detection and Monitoring:** The cloud service provider often combines the service with such heavy security measures to notify the user any fraudulent activities, intrusion or hackers and the likes among other related evils. These tools enable and facilitate blocking of more attacks and prompt responses to security threats in a manner that ensuring mobile data is secure at any given time [68].

**Collaboration and Controlled Access:** cloud based systems ensures real-time working on documents and projects needed by involved persons and at the same time ensures only authorized individuals are allowed to alter details. Cloud services also offer organizations opportunities for applying stringent access controls where only approved personnel accesses organizational information. For instance, using the case of roles, a business can set different user permissions; the read-only option or the editing option [69]. These access control mechanisms assist in minimizing occasions when data is accessed and or modified by unauthorized persons only, personnel with the right clearance level should only be allowed access to particular data. Mobile users in remote or Camp Offices or in any location can collaborate on Cloud such as Google Workspace or Microsoft 365 to ensure productivity is not comprising while the relevant security measures are in place [70].

**Regulatory Compliance and Auditing:** Compliance is a major issue for numerous companies especially when operating in fields that are highly regulated for instance healthcare, finance and the legal practice. For specific compliance regulation, the cloud providers do provide certain tools/ features like GDPR, HIPAA, or PCI DSS. Many of these cloud services also have audit trails integrated within them to help businesses know who has gotten into particular information, when, and what was done. Thus, this level of monitoring does not only guarantee legal complicity but also guarantees additional safeguard for mobile users who deal with sensitive information [71].

Mobile information assurance is therefore significantly impacted through cloud computing by way of assured data storage, data replication and business continuity, scalability and advanced security service provision. Incorporation of the cloud feature into mobile security is important because it will enable people and organizations to protect their valuable data, as well as make it readily retrievable when the need arises, and at the same time stand a better and more efficient chance against the several odds of threats that the sophisticated world presents today [72]. With increasing advancements in mobile technologies and a growing use of mobile gadgets across the globe the role of cloud computing in protecting data has become incredibly crucial. It provides a rich, adaptive, and safe means of handling information in the liberalized and globalized setting that is emerging in the twenty-first century.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

E-ISSN : 2962-1658
Volume 3, Number 4 , October, 2024
https://doi.org/10.47709/ijmdsa.vxix.xxxx

## CONCLUSION

Today, with mobile devices becoming the core of our lives and compact creation that are a smartphone or tablets being the focal point of our life and work mobile security can't be overemphasized. With much more progression opening up in the actual arena of portable security, it was noted that mobile device management or MDM together with security unparalleled measures, and computing and storage in clouds will go down in history as a very efficacious solution in information assurance. Mobile device management helps organizations to enforce a security policy, to manage devices at a distance and to respond to threats that may originate from the use of these devices. Some of the benefits that comes with MDM solutions includes managed password to improve security of the devices, ability to encrypt data, ability to wipe a device remotely, and ability to control what application runs on a specific device, as well as ability to monitor for compliance and track devices to prevent data leakage.

Mobile Security Best Practices to securing information on Mobile Devices are containing information like choosing strong security codes, enabling device encryption, frequently updating applications, and using VPNs for connection. Through the above best practices, users can minimize potential risks of getting infected with malware or having their information stolen, or accessed by unauthorized parties, for both personal and business purposes. Cloud Computing plays an important role in current mobile information assurance schemes. It provides data backup, data duplication, back up in case of an eventuality and enhanced features of security including data encryption and use of password. Cloud services enable mobile users to share data, access data from any location instantly and flexibly, and deploy storage and protection solutions according to their organization's requirements. Cloud computing is also significant to compliance with regulatory environments for business continuity as a strategy towards protection of data and assets in a mobile economy. In combination these technologies and practices offer a sound investment protection against the growing risks of mobile security threats to confidential data. For personal users or enterprise employees, and companies, integrated use of MDM, cloud technology and general mobile security best practice guarantees the safety, availability and reliability of data in the event of any breach. With consumer mobility experienced to be an ever increasing pivotal component of modern society, these strategies are imperative in addressing confidentiality, integrity, and regulatory requirements within a connected environment.

## REFERENCES

1. Dery, K., & MacCormick, J. (2012). Managing mobile technology: the shift from mobility to connectivity. *MIS Quarterly Executive*, *11*(4).
2. Chan, C. Y. (2011, April). Connected vehicles in a connected world. In *Proceedings of 2011 International Symposium on VLSI Technology, Systems and Applications* (pp. 1-4). IEEE.
3. M. Application, S. Threats, "Mobile Application Security Threats and Vulnerabilities 2019: Mobile Device Security - Attacks Research," pp. 1–19, 2019, Accessed: Apr. 19, 2021. [Online]. Available: https://www.ptsecurity.com/ww-en/analytics/mobileapplication-security-threats-and-vulnerabilities-2019
4. Can 5G make you more vulnerable to cyberattacks? - Help Net Security." 16 March 2020. [Online]. Available: https://www.helpnetsecurity.com/2020/03/16/5gsecurity-vulnerabilities/ . [Accessed Apr. 19, 2021].
5. Singla, S. R. Hussain, O. Chowdhury, E. Bertino, N. Li, "Protecting the 4G and 5G Cellular Paging Protocols against Security and Privacy Attacks," Proc. Priv. Enhancing Technol., vol. 2020, no. 1, pp. 126– 142, Jan. 2020, doi: 10.2478/popets-2020-0008.
6. Z. Whittaker, New Flaws in 4G, 5G Allow Attackers to Intercept Calls and Track Phone Locations, Tech Crunch, 24 February 2019. [Online]. Available: https://techcrunch.com/2019/02/24/new-4g5gsecurity-flaws/ . [Accessed 19 April 2021].
7. L. Whitney, How 4G and 5G Networks are Vulnerable to Denial of Service Attacks, Tech Republic, 26 March 2020. [Online]. Available: https://www.techrepublic.com/article/how-4g-and-5gnetworks-are-vulnerable-to-denial-of-service-attacks/ . [Accessed 2 April 2020].
8. 3GPP TS 22.261 ETSI, "5G; Service requirements for next generation new services and markets (Release 15)," vol. TS 22.261, pp. 0–52, 2018, Accessed: Apr. 19, 2021. [Online]. Available: https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx.
9. C. Annual, I. Report, "Cisco Annual Internet Report," p. 2023, 2018, Accessed: Apr. 19, 2021. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/whitepaper-c11-741490.html.
10. Md Minhaz Chowdhury, Kendall Nygard, "Machine Learning within a Con Resistant Trust Model", The 33rd International Conference on Computers and Their Applications (CATA 2018), March 19-21, 2018, Flamingo Hotel, Las Vegas, Nevada, USA.
11. Sowjanya Param, Md Minhaz Chowdhury, Damian Lampl, Pranav Dass, Kendall E. Nygard, "Energy Demand Prediction Using Neural Networks", The 28th International Conference on Computer Applications in Industry and Engineering, October 2015, San Diego, California, USA.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

E-ISSN : 2962-1658
Volume 3, Number 4 , October, 2024
https://doi.org/10.47709/ijmdsa.vxix.xxxx

12. Damian Lampl, Md Minhaz Chowdhury, Pranav Dass, Kendall E. Nygard, Vahid Khiabani, "Optimization Modeling in a Smart Grid", The 15th International Conference on Wireless Networks, 2015, Athens, Greece.
13. Kendall E. Nygard, Md. Minhaz Chowdhury, Pratap Kotala, "Trust and Purpose in Computing", The 32nd International Conference on Computers and Their Applications, March 2017, Honolulu, Hawaii, USA.
14. Posey, C., Bennett, R.J. and Roberts, T.L. (2011), "Understanding the mindset of the abusive insider: an examination of insiders' causal reasoning following internal security changes", Computers and Security, Vol. 30 No. 6e7, p. 486e97.
15. Purtschert, R. (2001), marketing fu¨r Verba¨nde und weitere Nonprofit-Organisationen, Haupt, Bern. Ramireddy, S., Chakraborthy, S., Raghu, R. and Raghav Rao, H. (2010), "Privacy and security practices in the arena of cloud computing – a research in progress", AMCIS 2010 Proceedings, Paper 574.
16. Reppy, J. (2012), International School on Disarmament and Research on Conflicts, available at: www.isodarco.it/courses/andalo12/paper/ISO12_ReppyCyber.pdf Roth, G. (2004), "Lessons from the desert: integrating managerial expertise and learning for organizational transformation", The Learning Organization, Vol. 11 No. 3, pp. 194-208.
17. Sasse, M.A., Brostoff, S. and Weirich, D. (2001), "Transforming the 'weakest link' e a human/computer interaction approach to usable and effective security", BT Technology Journal, Vol. 19 No. 3, p. 122e31.
18. Scarfo, A. (2012), "New Security Perspectives around BYODApplications (BWCCA)", 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA), 12-14 November, pp. 446-451.
19. Schlienger, T. and Teufel, S. (2003), "Information security culture – from analysis to change", Proceedings of ISSA 2003, Johannesburg, South Africa, 9-11 July 2003.
20. Schwarzwalder, R. (1999), "Intranet security", Database and Network Journal, Vol. 22 No. 2, pp. 58-62.
21. Serewicz, L.W. (2010), "Do we need bigger buckets of better search engines? The challenge of unlimited storage and semantic web search for records management", Records Management Journal, Vol. 20 No. 2, pp. 172-181.
22. Spears, J.L. (2005), "A holistic risk analysis method for identifying information security risks", Security Management, Integrity, and Internal Control in Information Systems, Springer, New York, NY, pp. 185-202
23. Stuart, K. and Bromage, D. (2010), "Current state of play: records management and the cloud", Records Management Journal, Vol. 20 No. 2, pp. 217-225.
24. Sweeney, S. and Crestani, F. (2006), "Effective search results summary size and device screen size: Is there a relationship?", Information Processing and Management, Vol. 42, pp. 1056-1074. Von Solms, B. (2000), "Information security – the third wave?", Computers and Security, Vol. 19 No. 7, pp. 615-620.
25. Von Solms, S.H. (2006), "Information security – the fourth wave", Computers and Security, Vol. 25 No. 2006, pp. 165-168. Webb, W. (2010), "Being mobile", Engineering and Technology, Vol. 5 No. 15, pp. 64-65.
26. Willis, A. (2005), "Corporate governance and management of information and records", Records Management Journal, Vol. 15 No. 2, pp. 86-97.
27. Young, R. and Kamffmeyer, U. (2002), Availability and Preservation: Long-term Availability and Preservation of Digital Information (AIIM Industry White Paper on Records, Document and Enterprise Content Management for the Public Sector), AIIM International Europe: Stephens and George Print Group.
28. Amatuni L, Ottelin J, Steubing B, Mogollón JM. 2020. Does car sharing reduce greenhouse gas emissions? Assessing the modal shift and lifetime shift rebound effects from a life cycle perspective.
29. J. Clean. Prod. 266:21869 27. Bi H, Ye Z, Zhu H. 2022. Examining the nonlinear impacts of built environment on ridesourcing usage: focus on the critical urban sub-regions. J. Clean. Prod. 350:131314
30. Ward JW, Michalek JJ, Samaras C. 2021. Air pollution, greenhouse gas, and traffic externality benefits and costs of shifting private vehicle travel to ridesourcing services. Environ. Sci. Technol. 55(19):13174–85
31. Cohen A, Shaheen S. 2016. Planning for shared mobility. Rep. 583, Plan. Advis. Serv., Am. Plan. Assoc., Chicago 30. Wenzel T, Rames C, Kontou E, Henao A. 2019. Travel and energy implications of ridesourcing service in Austin, Texas. Transp. Res. D 70:18–34
32. Hulkkonen M, Mielonen T, Prisle NL. 2020. The atmospheric impacts of initiatives advancing shifts towards low-emission mobility: a scoping review. Sci. Total Environ. 713:136133
33. Moreau H, de Jamblinne de Meux L, Zeller V, D'Ans P, Ruwet C, Achten WMJ. 2020. Dockless e-scooter: a green solution for mobility? Comparative case study between dockless e-scooters, displaced transport, and personal e-scooters. Sustainability 12(5):1803
34. Severengiz S, Finke S, Schelte N, Forrister H. 2020. Assessing the environmental impact of novel mobility services using shared electric scooters as an example. Proc. Manuf. 43:80–87
35. McQueen M, MacArthur J, Cherry C. 2020. The e-bike potential: estimating regional e-bike impacts on greenhouse gas emissions. Transp. Res. D 87:102482

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

E-ISSN : 2962-1658
Volume 3, Number 4 , October, 2024
https://doi.org/10.47709/ijmdsa.vxix.xxxx

36. Hu S, Chen P, Lin H, Xie C, Chen X. 2018. Promoting carsharing attractiveness and efficiency: an exploratory analysis. Transp. Res. D 65:229–43
37. Meng L, Somenahalli S, Berry S. 2020. Policy implementation of multi-modal (shared) mobility: review of a supply–demand value proposition canvas. Transp. Rev. 40(5):670–84
38. Kapuku C, Kho SY, Kim DK, Cho SH. 2021. Assessing and predicting mobility improvement of integrating bike-sharing into multimodal public transport systems. Transp. Res. Rec. 2675(11):204–13
39. Fitch D, Mohiuddin H, Handy S. 2020. Investigating the influence of dockless electric bike-share on travel behavior, attitudes, health, and equity. Rep. UC-ITS-2019-03, Univ. Calif. Inst. Transp. Stud., Davis, CA 39. Qiu LY, He LY. 2018. Bike sharing and the economy, the environment, and health-related externalities. Sustainability 10(4):1145
40. Clockston RLM, Rojas-Rueda D. 2021. Health impacts of bike-sharing systems in the U.S. Environ. Res. 202:111709
41. Nijland H, van Meerkerk J. 2017. Mobility and environmental impacts of car sharing in the Netherlands. Environ. Innov. Soc. Transit. 23:84–91
42. Noland RB, Smart MJ, Guo Z. 2016. Bikeshare trip generation in New York City. Transp. Res. A 94:164– 81
43. Gehrke SR, Sadeghinasr B, Wang Q, Reardon TG. 2021. Patterns and predictors of dockless bikeshare trip generation and duration in Boston's suburbs. Case Stud. Transp. Policy 9(1):756–66
44. Martinez LM, Viegas JM. 2017. Assessing the impacts of deploying a shared self-driving urban mobility system: an agent-based model applied to the city of Lisbon, Portugal.Int. J. Transp. Sci. Technol. 6(1):13–27
45. Bekka A, Louvet N, Adoue F. 2020. Impact of a ridesourcing service on car ownership and resulting effects on vehicle kilometers travelled in the Paris Region. Case Stud. Transp. Policy 8(3):1010–18
46. Tirachini A, Chaniotakis E, Abouelela M, Antoniou C. 2020. The sustainability of shared mobility: can a platform for shared rides reduce motorized traffic in cities? Transp. Res. C 117:102707
47. Yu B, Ma Y, Xue M, Tang B, Wang B, et al. 2017. Environmental benefits from ridesharing: a case of Beijing. Appl. Energy 191:141–52
48. Tirachini A, Gomez-Lobo A. 2019. Does ride-hailing increase or decrease vehicle kilometers traveled (VKT)? A simulation approach for Santiago de Chile. Int. J. Sustain. Transp. 14(3):187–204
49. Di X, Ban XJ. 2019. A unified equilibrium framework of new shared mobility systems. Transp. Res. B 129:50–78
50. Lee JB, Byun W, Lee SH, Do M. 2014. Correlation between optimal carsharing locations and carbon dioxide emissions in urban areas. Int. J. Environ. Sci. Technol. 11(8):2319–28
51. Cannoy, S. D., & Salam, A. F. (2010). A framework for health care information assurance policy and compliance. Communications of the ACM, 53(3), 126-131.
52. Chakraborty, R., Ramireddy, S., Raghu, T. S., & Rao, H. R. (2010). The information assurance practices of cloud computing vendors. IT professional, 12(4), 29-37.
53. Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach? Journal of Management Information Systems, 29(3), 157-188
54. Cooper, S., Nickell, C., Piotrowski, V., Oldfield, B., Abdallah, A., Bishop, M., & Pérez, L. C. (2010). An exploration of the current state of information assurance education. ACM SIGCSE Bulletin, 41(4), 109- 125.
55. Ezingeard, J. N., McFadzean, E., & Birchall, D. (2005). A model of information assurance benefits. Information Systems Management, 22(2), 20-29.
56. Hamill, J. T., Deckro, R. F., & Kloeber Jr, J. M. (2005). Evaluating information assurance strategies. Decision Support Systems, 39(3), 463- 484.
57. Höne, K., & Eloff, J. H. P. (2002). Information security policy—what do international information security standards say?. Computers & security, 21(5), 402-409.
58. Knapp, K. J., Marshall, T. E., Kelly Rainer, R., & Nelson Ford, F. (2006). Information security: management's effect on culture and policy. Information Management & Computer Security, 14(1), 24-36.
59. Paul, P.K., Chatterjee, D., Bhuimali,A., Atarthy, A. (2016). Cyber Crime: An Important facet for promoting Digital Humanities—A Short Review in Saudi Journal of Humanities and Social Science, 1 (1), 13-16
60. Proia, A., Simshaw, D., & Hauser, K. (2015). Consumer cloud robotics and the fair information practice principles: Recognizing the challenges and opportunities ahead. Minn. JL Sci. & Tech., 16, 145.
61. Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). A policy framework for information security. Communications of the ACM, 46(7), 101-106. 18. Reidenberg, J. R. (1994). Setting standards for fair information practice in the US private sector. Iowa L. Rev., 80, 497.
62. Schou, C. D., & Trimmer, K. J. (2004). Information assurance and security. Journal of Organizational and End User Computing, 16(3), 123-145.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

E-ISSN : 2962-1658
Volume 3, Number 4 , October, 2024
https://doi.org/10.47709/ijmdsa.vxix.xxxx

63. Abate, K. H., Abebe, Z., Abil, O. Z., Afshin, A., Ahmed, M. B., Alahdab, F., et al. (2018). Global, regional, and national incidence, prevalence, and years lived with disability for 354 diseases and injuries for 195 countries and territories, 1990–2017: a systematic analysis for the Global Burden of Disease Study 2017. Lancet 392, 1789–1858. doi:10.1016/S0140-6736(18) 32279-7
64. Anglada-Martinez, H., Riu-Viladoms, G., Martin-Conde, M., Rovira-Illamola, M., Sotoca-Momblona, J. M., and Codina-Jane, C. (2015). Does mHealth increase adherence to medication? Results of a systematic review. Int. J. Clin. Pract. 69, 9–32. doi:10.1111/ijcp.12582
65. Bidmon, S., and Terlutter, R. (2015). Gender differences in searching for health information on the internet and the virtual patient-physician relationship in Germany: exploratory results on how men and women differ and why. J. Med. Internet Res. 17, e156. doi:10.2196/jmir.4127
66. Cheen, M. H. H., Tan, Y. Z., Oh, L. F., Wee, H. L., and Thumboo, J. (2019). Prevalence of and factors associated with primary medication non-adherence in chronic disease: a systematic review and meta-analysis. Int. J. Clin. Pract. (Esher) 73, e13350. doi:10.1111/ ijcp.13350
67. De Geest, S., Zullig, L. L., Dunbar-Jacob, J., Helmy, R., Hughes, D. A., Wilson, I. B., et al. (2018). ESPACOMP medication adherence reporting guideline (EMERGE). Ann. Intern Med. 169, 30–35. doi:10.7326/M18-0543
68. Eis, S., Solà-Morales, O., Duarte-Díaz, A., Vidal-Alaball, J., Perestelo-Pérez, L., Robles, N., et al. (2022). Mobile applications in mood disorders and mental health: systematic search in apple app store and google play store and review of the literature. Int. J. Environ. Res. Public Health 19, 2186. doi:10.3390/ijerph19042186
69. Foley, L., Larkin, J., Lombard-Vance, R., Murphy, A. W., Hynes, L., Galvin, E., et al. (2021). Prevalence and predictors of medication non-adherence among people living with multimorbidity: a systematic review and meta-analysis. BMJ open 11, e044987. doi:10.1136/bmjopen-2020-044987
70. Gast, A., and Mathes, T. (2019). Medication adherence influencing factors - an (updated) overview of systematic reviews. Syst. Rev. 8, 112. doi:10.1186/s13643-019- 1014-8 Glide (2023).
71. Glide. Available at: https://www.glideapps.com/(Accessed January 26, 2024). Hamine, S., Gerth-Guyette, E., Faulx, D., Green, B. B., and Ginsburg, A. S. (2015). Impact of mHealth chronic disease management on treatment adherence and patient outcomes: a systematic review. J. Med. Internet Res. 17, e52. doi:10.2196/jmir.3951
72. Horne, R., Cooper, V., Wileman, V., and Chan, A. (2019). Supporting adherence to medicines for long-term conditions: a perceptions and practicalities approach based on an extended common-sense model. Eur. Psychol. 24, 82–96. doi:10.1027/1016-9040/a000353

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.