BULLET: Jurnal Multidisiplin Ilmu
Volume 03, No. 05, Oktober-November, 2024
ISSN 2829-2049 (media online)
Hal 759-774

Information Assurance in the Era of Mobility: Challenges and Solutions

Mohammad Hasan Amin[1], Nahid Neoaz[2]

[1]Kettering University, Michigan

[2]Wilmington University, USA

[1]amin3672@kettering.edu, [2]nahidneoaz@yahoo.com,

Abstract

With more family and organizational members using mobile devices within homes and workplaces, mobile device security particularly in regard to information security is an important question. The information assurance principles, secure mobile technologies, trends, threats, policies and compliance in mobile systems are presented in this article. These basic features including cryptos, MFA, MDM, and SC are part of the mobile security technologies explained in the paper. It also looks into how these latest trends, for instance 5G networks, IoT, mobile payment and AI app impact and offer opportunities as well as risks. Therefore, the article discusses policy regimes and compliance and the emergence of threats such as mobile malware, phishing, and ransom ware. However, it also proscribes comprehension of future opportunities and further evolutions in the sphere of mobile information assurance including the creation of Artificial Intelligence, quantum-safe encryption, and the international cooperation in order to overcome the new threats on the horizon. The mobile systems adopted by different systems and software may prone to several hacking attacks, although, through proper policies’ integration and up-to-date technologies, mobile systems security is feasible than in the advancing technology world.

Keywords: m-IA, encryption, authentication, MDM, 5G, IoT, mobile malware, mobile payment, policy enforcement, emerging threats, AI and quantum encryption, mobile security in the future, BYOD, mobile threat vendors.

INTRODUCTION

Globally, within the last two decades, Mobile devices, wireless technology and the World Wide Web have affirmed the society’s mode of access, management & dissemination of information. Mobiles phones, tablets, laptops and the IoT devices have become basic necessity to people during work as well as in personal life. That of course has evolved as people depend more and more on mobility—raising the issue of how one might ensure that information is secure, accurate and well accessible—a discipline known as Information Assurance (IA). Information Assurance is a holistic approach to managing any risk that is in some way related to the use, processing, storage, and transmission of information [1]. It goes beyond traditional cybersecurity by focusing on the five core pillars: These are: confidentiality, integrity, availableness, identity/ authentication and finally non-repudiation. Confidentiality means that some data are out of reach of the outsiders and those not having the right to access the information. Information quality on the other hand must be protected to maintain three quality aspects; accuracy to keep data correct, and accessibility to ensure that information is available when needed. Certification makes sure the authenticity of users and their machines while validity eliminates chances of denying action or a transaction [2].

Information Assurance if done simultaneously with mobility has its own problems which clearly needs to be understood. Mobile contexts are highly dynamic, in the sense that the devices are often transferred from one network to another; from areas; from one domain to another. Such conditions retain susceptibilities which are not characteristic of standard non-moving networks. For instance handhelds prisons can be lost or stolen, used without permission and available to insecure WAPs [3]. Further, outsourcing cloud applications and storage brings risks associated with data privacy and security, compliance of third party are also other concerns. In addition to this, the fact that there is availability of several forms of the operating system for mobile devices means that several applications and pieces of hardware make the task even more complex. Mobile ecosystems are rather distributed and can consist of different levels of protection as well as different update rates compared to centralized systems. These are areas that are exploited by all manner of attackers with the goal of either gaining illicit access into a system or to install malicious code. For example, in the new era, the phishing in the mobile platform has become frequent which is including fake applications, links, and social engineering [4].

However, mobility offers opportunities by which information assurance can also be enhanced also. This has been boosted by security solution in mobility that includes mobile multifactor authentication, bio, and end-to-end encryption. For instance, current mobile devices give with portable contraption highlight safety measures like TPM or secure enclave, which makes guard keys and any other sensitive information [5]. Mobile device management

(MDM) enables an organization to set a level of security, to view activity that is performed by device, and to erase all data stored in the device in case of a loss, theft or any other unfavorable scenario. The advance of mobility in health, financial and government services triggers the requirement for Information Assurance in mobile situations. The uses of the mobile device include; in managing patient data, counseling and patient care monitoring. For this reason, the data should be protected to the highest level to prevent the breach of patients' trust and the law that governs it like HIPAA. Also in the financial market mobile banking applications cannot afford to relinquish the credibility, transactions and messaging interface to the fraudsters and identity thieves [6].

Increased reliance on mobility in the working environment renders it important that Information Assurance is coherent and comprehensive. It involves not only creating first and second-generation technical security solutions but also creating first and second generation of organizational security solutions for the users. Mobile devices the employee uses, for instance, in downloading apps or using public Wi-Fi, comes with risks; therefore, it has to be taught. The organizations require constant change of the security frameworks in relation to the appearance of threats and changes in the organizations' activities. And this leads us to the relation between Information Assurance and mobility which is now a crucial factor of the society [7]. Mobility when used together with the acknowledged advanced technologies targeted at improving organization performance is easier and efficient; however it is a risk worth managing to avoid nasty shocks and loss of trust. The strategy outlined in this paper is comprehensive and strategic, which enable organizations to capture possibilities of mobility optimally; this way, information assurance is not jeopardized.

MAIN CHALLENGES IN THE ACHIEVING OF GUARANTEED INFORMATION SECURITY IN MOBILE SYSTEMS

Taking in mind the increased deployment of mobile devices on the personal, organizational and industrial levels, handling IA in these areas is almost a herculean task. The dynamic, portable and networkable nature of mobile systems raises conceptually different kinds of issues and in context requires appropriate security precautions to protect the privacy, integrity and availability of the used information. This part describes some of the major challenges to the provision of information assurance in mobile environments [8].

Physical Security Risks: Mobile devices are transports, as has been described, and as such a good deal easier to lose, or have physically abstracted from, than are static computing systems. It is unfortunate that once a device is stolen, the attackers can have full access to the confidential information provided the device did not enforce adequate encryption or authentication. This threat is exacerbated by the fact that more and often use smart mobile devices for accessing the business networks the storing of information [9]. Furthermore lost containing asteroids or stolen devices make it easier for the attacker to emulate real users hence compromising secure web systems.

Unsecured Communication Channels: They are mobile and have wireless links such as wireless fidelity, mobile telephones or Bluetooth. Such channels are easily susceptible to interception, eavesdropping and man-in-the-middle attack this is often realized by users who connect to an open network. Therefore these threats can be utilized by the attackers to spy sensitive information such as login credentials, financial data and corporate communications –violations of confidentiality and integrity [10].

Fragmented Mobile Ecosystems: The first challenge of the mobile OSs is the great variability though there are different types of them, for instance Android, iOS, Windows, etc, and the heterogeneity of devices where these OSs are implemented relying on the aforementioned factors, Android faces higher risks due to the facts that it is an open source and there is no central ways of updating OSs among the manufacturing gadgets [11]. A disjointed OS security update regime implies that the average number of unpatched vulnerabilities on such devices is high and takes an ordinarily long time to leave the user vulnerable to known destructive activities.

Malicious Applications and Malware: The new social engineering trend that has manifested itself due to the mobile apps uses the risk created by new apps, phishing messages, downloading of new apps, apps that were not going through app stores vetting. Extremely numerous of these can surely snoop and steal personal information, track the activity of the user, or impose ransom ware on the devices. However, Google Play and Apple's App are relatively more secured and yet some of these malicious apps still make their way in. And one more problem is that people allow for many permissions in applications and do not understand that they allowed too many permissions [12].

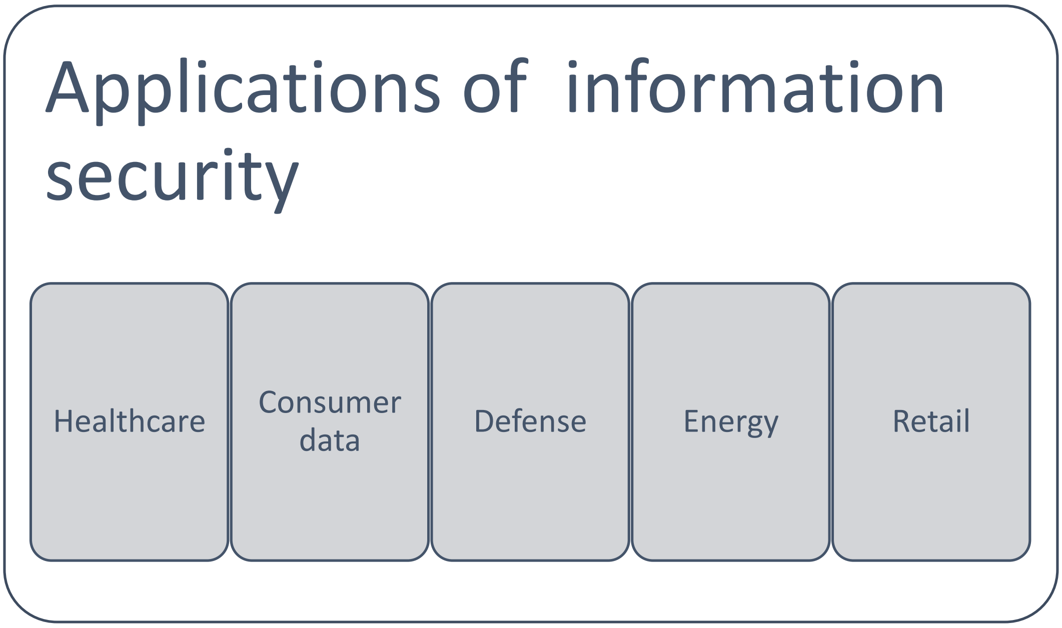

Figure: 1 showing applications of information security

Bring Your Own Device (BYOD) Policies: There is new trend where most firms have adopted the use own devices at workplace hence the ‘‘bring your own device ’’ policies implies the use of employees owned gadgets at workplace. Even as we see that BYOD has it positive side of the argument it has its disadvantages that we see are less expense and more flexibility, the major disadvantage being the vulnerability of organizational data since the organization has little control over the devices. Effectiveness of these measures can be observed in such negative aspects as users ignore the security rules set, use outdated applications, and knowingly download/reinstall unapproved applications that pose threats to the security of the company’s networks [13].

Data Synchronization and Cloud Dependencies: Mobile systems, for example, constantly synchronize the files in the Cloud storage services, to enable use on other platforms. However, this is not always convenient since it creates additional risks since we relay so much on cloud services. Data in transit or kept on the servers of other companies can be compromised, acquired by an illegitimate individual, or lost accidentally. The security of user data is a persistent challenge within the cloud settings because the data transits in various endpoints before reaching the intended point [14].

Evolving Threat Landscape: Exactly the same can be seen with the accelerated rate in the evolution of mobile technologies, with improved attack techniques as well. Mobile devices are on the firing line with regards to new emerging threats such as Advanced Persistent Threats (APTs), zero-day exploits among many others. New technologies like 5G, IoT and edge computing add to this list and we always need to learn how to protect ourselves anew. It is also important to note that the concept of information assurance in mobile systems is complex due to the dynamic and disperse as well as interrelated environment of the mobile systems [15]. These systems entail stringent security measures which consist of, encryption, update, fortified authentication and user consciousness. Organizations also need to enhance strategies including the Mobile Device Management (MDM) and Endpoint Detection and Response (EDR) solutions to deal with risks. If these challenges are well understood and effectively addressed, then it is possible to improve the security and reliability of mobile systems in an increasingly mobile oriented society [16].

TECHNOLOGIES SUPPORTING THE PROTECTION OF INFORMATION IN MOBILITY

Maintaining information assurance in the now mobile enterprise world involves the use of a range of technologies to protect data confidentiality, integrity and availability despite the threats. Mobile environments are different because devices connect and disconnect, often depending on a wireless connection; many programs rely on wireless connections; and more and more applications are appearing on mobile devices. This section basically discusses major technologies that support effective information assurance in mobility settings [17].

Encryption: Encryption is the key in mobile info-protection it ensures that the information is only available to the intended user. End-to-end encryption (E2EE) is employed in the messages' applications such as What Sapp and Signal that only the send and receive only can have access to the content of the communication. Likewise, device level encryption averts probable leakage of data stored in the client's mobile devices in cases of theft or missing. The current operating systems in smart devices like iPhone and Google Android factor in encryption mechanisms that afford data protection as the baseline option [18].

Authentication and Access Control: Mobile system security is very crucial and is mainly determined by a strong user identity authentication mechanism provided by advanced authentication technologies. MFA means adding multiple layers of protection on top of passwords including biometrics, tokens and otp, smf. Of the recognition technologies, biometrics has gone viral mainly due to the portability and accuracy that characterize mobile devices. Also, RBAC helps to protect data from different users mistakenly accessing data which is assigned to the other roles of the company [19].

Mobile Device Management (MDM): The Mobile Device Management solutions are crucial for the company that use mobile devices as corporate assets within their networks and the company, which implements BYOD policies. Become the main ways through which administrators can ensure that security policies are fulfilled, control device activities, and remotely as well as centrally manage software updates. The latter can also ensure protection of information with features such as, device encryption, application locking and remote data deletion. These capabilities make sure that mobile devices continue to be compliant to security standards of an organization [20].

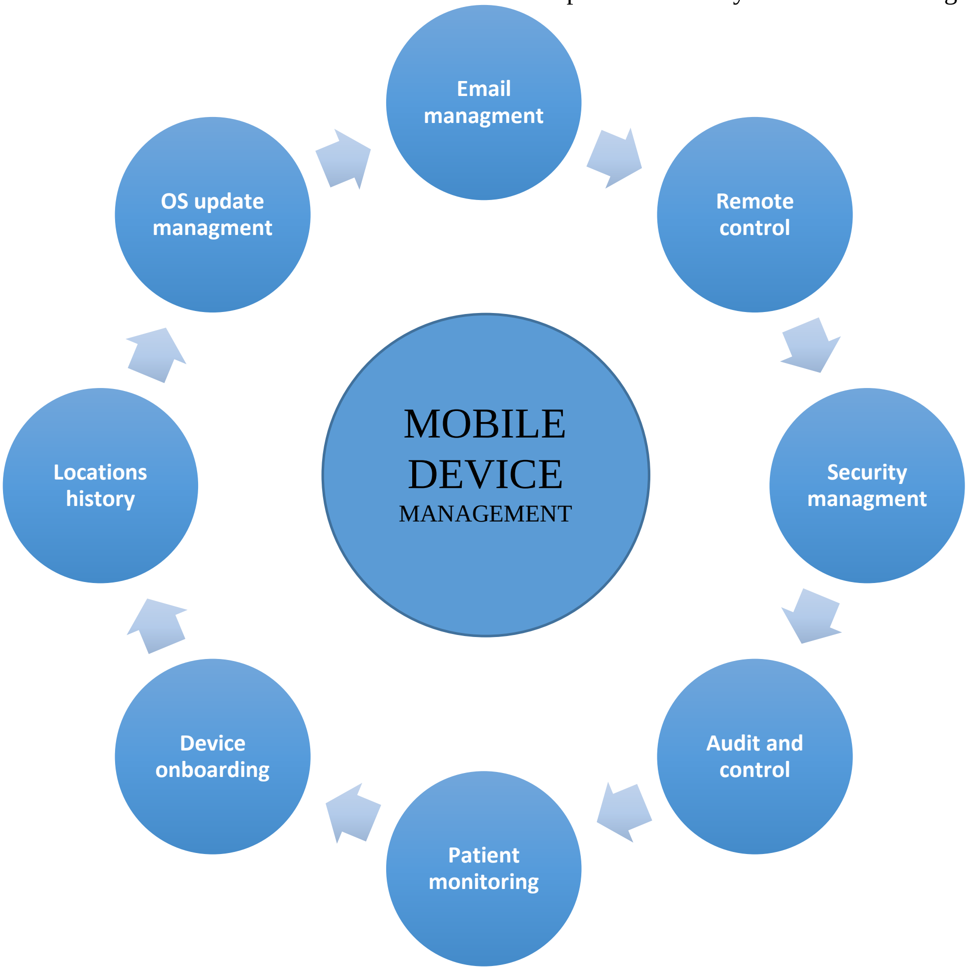

Figure: 2 showing mobile device management

Secure Communication Protocols: Mobile security flourishment requires the specification of technologies in an effort to safely transmit information in secure channels. Some basic examples of data protection in transit are HTTPS, Secure Sockets Layer (SSL), Transport Layer Security (TLS), etc, which help enciphers the transit of data and therefore keep the eavesdropping and man-in-the-middle attacks at bay. VPNs also build on security by encrypting all traffic between the mobile devices and corporate networks especially while using resources accessible through public Wi-Fi [21].

Threat Detection and Response Tools: Mobile threat detection and response technologies must be instituted in order to determine possible threats and control them in real time. Currently, focused security tools known as Mobile Threat Defense (MTD) apply machine learning and behavioral analysis to identify malware, phishing attempts and other network irregularities. Endpoint Detection and Response (EDR) systems further advance these features, maintaining an ongoing protective security vigil on mobile endpoints with programmed action against security breaches [22].

Application Security Frameworks: This article shows that the security of mobile applications is pivotal in providing Information assurance. Mobile application developers integrate platforms namely, Android's SafetyNet and Apple's App Transport Security (ATS) to enhance the creation of secure mobile applications. These frameworks assist to ensure that any coding activities undertaken are secure, and that reversing of code is restricted so as to ensure that data transfer between the app and the backend servers is as secure as possible [23].

Cloud Security Technologies: Whenever mobile systems depend on cloud services, cloud security technologies are truly required. Cloud IAM solutions, encryption solutions, and DLP implementations keep data, which is to be stored or processed in the cloud secure. Furthermore, the SASE which stands for Secure Access Service Edge combines cloud security as well as networking protection [24].

MOBILE DEVICES THAT ARE USING CLOUD BASED RESOURCES

The technologies that support information assurance in mobility include are various and are dynamic to meet the current risks and threats. With the help of encryption, authentication, secure communication protocols and the surrounding threat identification means, the protection of mobile conditions can be greatly improved at the organizational and individual levels. Therefore, the integration of these mobile systems will continue to be paramount in ensuring proper information assurance since it complicates the systems increase in interactions [25].

Information assurance in the context of a mobile driven environment goes beyond technological support and colors with well-set policies and compliance standards. Security practices regulate the authorized operation of mobile systems; compliance checks whether an organization complies with relevant rules and regulations [26]. Combined, such components form a basis for data protection as well as risk minimization in more mobile contexts, with a view to promoting ten dance or reliance.

Importance of Policies in Mobile Information Assurance: Mobile systems' policies are based on information assurance that follows a sequential way of providing secure operation. It spells out rules of conduct regarding the use of devices, handling of information, and conducts expected and approved of by all the relevant and interested parties for a specific organizational security framework. Lack of policies makes mobile systems open to attacks, unauthorized access and operational interferences on the data [27].

KEY AREAS ADDRESSED BY POLICIES INCLUDE:

Device Management: Policies identify how devices are configured, deployed and managed to have security measurements in place.

Access Control: Policies involve outlining user classification and their privileges, the ways by which user identity can be confirmed to allow an individual to access restricted data [28].

Acceptable Use: These policies define or describe the acceptable and improper use of mobile devices including limitations towards connection to insecure networks and/or downloading of unauthorized applications.

Bring Your Own Device (BYOD) Policies: The implementation of BYOD solutions has added a fresh set of problems to the field of mobile information assurance. Highly mobile employees may find a ban on Likkins' model inconvenient while accepting that restraining usage offers a sound security model for any enterprise Security monitoring is insisted on and made compulsory through mobile device management (MDM) Procedures for managing personal and corporate information (for instance, placing it in containers) Necessary measures for encryption on devices, password complexity and update frequency. How data on the corporate devices could be erased should the devices gets lost or if the employee leaves the organization sophisticated attack methods [29]. From advanced persistent threats (APTs) to zero-day vulnerabilities, mobile devices are constantly targeted by attackers seeking to exploit new weaknesses. Emerging technologies such as 5G, IoT, and edge computing further expand the attack surface, requiring ongoing adaptation to address new security challenges. The challenges of ensuring information assurance in mobile systems arise from the dynamic, fragmented, and interconnected nature of mobile ecosystems. These systems require robust security strategies that include encryption, regular updates, secure authentication mechanisms, and user awareness programs. Organizations must also adopt advanced tools such as Mobile Device Management (MDM) and Endpoint Detection and Response (EDR) solutions to mitigate risks. By understanding and addressing these challenges, it is possible to enhance the security and resilience of mobile systems in an increasingly mobile-driven world [30].

TECHNOLOGIES ENABLING INFORMATION ASSURANCE IN MOBILITY

Ensuring information assurance in the era of mobility relies on a suite of advanced technologies designed to protect the confidentiality, integrity, and availability of data, even in the face of dynamic and diverse threats. Mobile environments pose unique challenges due to the fluid nature of device connections, the reliance on wireless networks, and the proliferation of mobile applications. This section explores key technologies that enable robust information assurance in mobile systems [31].

Encryption: Encryption is the cornerstone of mobile information security, ensuring that sensitive data remains confidential and inaccessible to unauthorized parties. End-to-end encryption (E2EE) is widely used in messaging apps like What Sapp and Signal, ensuring that only the sender and recipient can access the content of communications. Similarly, device-level encryption protects data stored on mobile devices, safeguarding it from unauthorized access in cases of theft or loss. Modern operating systems, such as iOS and Android, incorporate built-in encryption mechanisms to protect user data by default [32].

Authentication and Access Control: Advanced authentication technologies play a critical role in verifying user identities and preventing unauthorized access to mobile systems. Multi-factor authentication (MFA) has become a standard security practice, combining passwords with additional factors such as biometrics (fingerprint, facial recognition), hardware tokens, or one-time passcodes (OTPs). Biometrics, in particular, have gained widespread adoption due to their convenience and reliability in mobile devices. Additionally, role-based access control (RBAC) ensures that users can only access resources and data relevant to their roles, minimizing the risk of data exposure [33].

Mobile Device Management (MDM): Mobile Device Management solutions are essential for organizations that deploy mobile devices within their networks or adopt Bring Your Own Device (BYOD) policies. MDM tools allow administrators to enforce security policies, monitor device usage, and manage software updates remotely. They can also secure sensitive data through features such as device encryption, application whitelisting, and remote data wiping. These capabilities ensure that mobile devices remain compliant with organizational security standards [34].

Secure Communication Protocols: Secure communication technologies are vital for protecting data transmitted over mobile networks. Protocols such as HTTPS, Secure Sockets Layer (SSL), and Transport Layer Security (TLS) encrypt data in transit, preventing eavesdropping and man-in-the-middle attacks. Virtual Private Networks (VPNs) further enhance security by encrypting all traffic between mobile devices and corporate networks, particularly when accessing resources over public Wi-Fi [35].

Threat Detection and Response Tools: Mobile threat detection and response technologies are essential for identifying and mitigating potential risks in real time. Mobile Threat Defense (MTD) solutions use machine learning and behavioral analysis to detect malware, phishing attempts, and network anomalies. Endpoint Detection and Response (EDR) systems extend these capabilities, providing continuous monitoring and automated responses to security incidents on mobile endpoints [36].

Application Security Frameworks: The security of mobile applications is critical for ensuring information assurance. Mobile app developers leverage frameworks like Android's SafetyNet and iOS's App Transport Security (ATS) to build secure applications. These frameworks help enforce secure coding practices, prevent reverse engineering, and ensure data is transmitted securely between the app and backend servers [37].

Cloud Security Technologies: With mobile systems heavily reliant on cloud services, cloud security technologies are indispensable. Identity and Access Management (IAM) solutions, cloud encryption, and data loss prevention (DLP) tools ensure that data stored and processed in the cloud remains secure. Moreover, Secure Access Service Edge (SASE) technologies integrate cloud and network security to protect mobile devices accessing cloud-based resources [38]. The technologies enabling information assurance in mobility are diverse and continuously evolving to address emerging threats and vulnerabilities. By integrating encryption, authentication, secure communication protocols, and advanced threat detection tools, organizations and individuals can significantly enhance the security of mobile environments. As mobile systems grow more complex and interconnected, the adoption of these technologies will remain a cornerstone of robust information assurance [39].

POLICY AND COMPLIANCE IN MOBILE INFORMATION ASSURANCE

In an increasingly mobile-driven world, maintaining robust information assurance requires not only technological solutions but also adherence to well-defined policies and compliance frameworks. Policies guide the secure use of mobile systems, while compliance ensures organizations meet regulatory requirements and industry standards. Together, these elements provide a foundation for safeguarding sensitive information, mitigating risks, and fostering trust in mobile environments [40].

Importance of Policies in Mobile Information Assurance: Policies serve as the cornerstone of information assurance in mobile systems. They establish guidelines for secure device usage, data management, and user behavior, ensuring that all stakeholders are aligned in protecting sensitive information. Without clear policies, mobile systems are more vulnerable to data breaches, unauthorized access, and operational disruptions [41].

Key areas addressed by policies include

Device Management: Policies specify how devices are provisioned, configured, and monitored to maintain security.

Access Control: Policies define user roles, permissions, and authentication methods to ensure that only authorized individual's access sensitive information.

Acceptable Use: These policies outline the appropriate use of mobile devices, such as restrictions on accessing unsecured networks or downloading unauthorized applications [42].

Bring Your Own Device (BYOD) Policies: The rise of Bring Your Own Device (BYOD) initiatives has introduced unique challenges in mobile information assurance. BYOD policies must strike a balance between employee convenience and organizational security. Effective BYOD policies typically include: Mandatory use of mobile device management (MDM) tools for security monitoring. Guidelines for separating personal and corporate data (e.g., through containerization). Requirements for device encryption, strong passwords, and regular updates. Procedures for remotely wiping corporate data in case of device loss or employee departure [43].

Regulatory Compliance in Mobile Information Assurance: Such entities will reasonably be subject to several regulatory conditions with regards to data protection and privacy. Adherence to these regulations is indispensable to avoid legal sanctions, loss of reputation of an organization and significant losses [44]. Key regulatory frameworks include:

General Data Protection Regulation (GDPR): Rules the data protection standards that govern the handling of citizens 'data by various organizations in the EU area. Mobile systems require adaption to achieve the features of GDPR; specifically, the data storage and transfer of data should be encrypted [45].

Health Insurance Portability and Accountability Act (HIPAA): Concerning the reuse or storage of the patient' information on a mobile device, HITECH mandates all healthcare organizations to protect such information [46].

Payment Card Industry Data Security Standard (PCI DSS): This one specifies a way of protecting the card payment data, which is important for the mobile payments.

Federal Information Security Management Act (FISMA): Applicable to US federal agencies and their contractors, this RFP demands extensive security precautions meant for mobile system interacting with governmental data [47].

CHALLENGES OF POLICY OF IMPLEMENTATION AND COMPLIANCE

Despite their importance, implementing policies and ensuring compliance in mobile environments present several challenges:

Device Diversity: This is because there are many types of mobile devices, operating systems, and settings, so enforcing compliance - especially within a large organization - is almost impossible [48].

User Behavior: At other times the employees may not even be aware of such policies and may therefore be found liable of violating the policies through Equalizing insecure networks or downloading unapproved programs.

Evolving Threat Landscape: There is invariably the need to upgrade regulations to fit new threats and vulnerability arising from facilities such as 5G and IoT [49].

Resource Constraints: That is because small and middle organizations often lack sufficient funds to adopt anti-harassment policies let alone enforce them.

Applicable Policies for Policy and Compliance: It has to conduct regular risk assessment with the intention of identifying threats to the mobile systems. Organize procedures for the mobile device security training of the employee for whom mobile safety and the conformity with the provided company rules on this issue will be explained. Write clear mechanisms for people not to adhere to the policy followed by the right action plan [50]. Use hard copies for monitoring the compliance level of the policies and for implementing the policies in to in real time. It is advised that the management engage legal and regulatory consultants to help with compliance to policies and ensuring compliance in mobile environments present several challenges:

Device Diversity: Due to the proliferation of multiple types of mobile devices, operating systems and their corresponding settings pegging down standard policies is cumbersome [51].

User Behavior: Some employees especially download application without the knowledge that it defies organizational policy services perhaps contracting with unsecured networks.

Evolving Threat Landscape: The polices need to evolve and effective measures have to be incorporate with new threats and vulnerabilities addressed by the new technologies as such as 5G and IoT devices [52].

RESOURCE CONSTRAINTS: SMALL AND MEDIUM-SIZED ORGANIZATIONS MAY NOT BE ABLE TO FULLY RESOURCE EFFECTIVE POLICIES AND PROCEDURES

Main Principles of Policy and Legal Compliance Mutually engage in the performance of risk assessment at least twice a year to ensure that risks in mobile systems are effectively detected. Communicate with employees on mobile devices and ways to use them securely, and other matters regarding the mobile policy. Describe the specific channels of an official for policy violations, or methods of correction. Implement the measures by using automated systems for real time compliance and policy enforcement [53]. Consults with legal and regulatory personnel to check on set industry standards emending policies and ensuring compliance in mobile environments present several challenges:

Device Diversity: This is because there is a variety of mobile devices, operating systems and configurations in use and thus it is hard to ensure uniformity is observed.

User Behavior: The employees are sometimes unaware of such policies and may end up violating them through to Equalizing insecure networks or downloading unapproved programs [54].

Evolving Threat Landscape: Regulations have to shift to address new risks and weakness created by new technologies like 5G and IoT.

Resource Constraints: Small and medium organizations may not have adequate resources to adopt and especially enforce anti-harassment policies [55].

Working Policies for Policy and Compliance Perform periodic risk analysis in order to determine threats pose to the mobile systems. Set up mobile security training for employees that will teach them about safer usage of mobile devices and consistency with the company’s rules on the subject. Set concrete procedures for non-compliance with policy, followed by the correct course of action. Employ automated solutions for tracking compliance levels and for applying policies directly in real–time [56]. It is advised that the management engage legal and regulatory consultants to help with compliance to policies and ensuring compliance in mobile environments present several challenges:

Device Diversity: The wide range of mobile devices, operating systems, and configurations makes it difficult to enforce uniform policies.

User Behavior: Employees may unknowingly violate policies, such as by using unsecured networks or downloading unauthorized applications.

Evolving Threat Landscape: Policies must adapt to new threats and vulnerabilities introduced by emerging technologies, such as 5G and IoT devices [57].

Resource Constraints: Small and medium-sized organizations may lack the resources to implement and enforce comprehensive policies.

Best Practices for Policy and Compliance

To address these challenges, organizations can adopt the following best practices:

- Conduct regular risk assessments to identify vulnerabilities in mobile systems.
- Provide ongoing training to employees on secure mobile practices and policy adherence.
- Establish clear accountability for policy violations, along with remediation procedures.
- Use automated tools to monitor compliance and enforce policies in real time.
- Collaborate with legal and regulatory experts to ensure alignment with industry standards.

This implies that in a mobile environment policy and compliance mean the same thing as information assurance. Some of these risks include; Misuse of company information, unauthorized access to information, viruses and loss of information, privacy violation, and noncompliance with legal requirement. Therefore, through the policies regarding usage of mobile systems in the organization, a proper implementation of BYOD, and rules and regulations, and such risks can be mitigated through, secure utilization of the systems. In the future, therefore, control over policy administration, and compliance checking will continue to be crucial to maintaining information integrity while encouraging trust in the mobile business operations [58]. Mobile technology change has been on a very fast pace, and it has touched almost all aspects of life, communication and work and information. Though, as these gadgets affect people's personal and workplace experience, they also become the prime targets for hackers and other criminals. Therefore, converging technologies such as 5G mobile communication technology, IoT gadgets, and cellular mobile payment also open up deeper opportunities but aggregate many felicitous challenges that must be solved to foster information security. This section views the likely future outlook of mobile information assurance along with analyzes the risks that are associated with security threats [59].

TRENDS OF MOBILE TECHNOLOGY

Adoption of 5G Networks: The everyday technological developments have highly favored the 5G networks pushing the speed, reliability and connections of mobile devices forward. While this improves user experience and facilitates issues such as data streaming and edge computing, it expands the exposure zone. The high bandwidth and low latency provide the attacker with efficiency in attack and big scale network can be invaded in real time basis [60].

Proliferation of IoT Devices: The IoT setting is becoming more saturated with tens of millions soon billions of connected things from personal wearables, smart home devices to industrial IoT. Such devices are incorporated in ordinary portable systems, employing the same networks, and information interchange. However, the most important residences of IoT devices are ailailable from Ill-equipped security notations where most of them are relatively simple, therefore presenting reasonable targets for unauthorized entry into more elaborate networks [61].

Mobile Payment Systems: One of the most employed innovation in everyday life is the application of mobile payments like Apple Pay and Google Pay and other touchless payments. Despite the fact that these technologies are helpful, these make hackers obtain monetary data or exploit payment procedures. This remains so to ensure users remain assured on the systems they use to make these mobile payments [62].

Rise of AI and Machine Learning in Mobile Systems: The mobile systems are now adopting AI in all its forms which include ML in functions like voice recognition, application customization and analysis. However, in the wrong hands, they can be leveraged by the attacker to generate more complex form of malware or even more sophisticated phishing attacks [63].

NEW ASPECTS RELATING TO PROTECTION OF MOBILE INFORMATION

Advanced Mobile Malware: Mobile malware is still rampant and is even at present creating its variants that are hard to identify by more traditional means. For instance, there are the malware type which do not require interaction at all such as the Pegasus spyware. These threats interfere with student information and individual privacy, the utility of the gadget in use [64].

Phishing and Smashing Attacks: Smishing that is the use of text messages and prospering that is the use of emails are more person and difficult to differentiate. Social engineering is the act of playing on the psychological vulnerabilities of users within an organization or key systems, this is usually done in an effort to extract a specific type of data or install a given program. Apparently, with handy apps like instant messaging apps, the possibilities of such an attack have also shifted to other platforms [65].

Threats to IoT-Integrated Mobile Ecosystems: The connectivity of IoT devices jointly with the mobile systems raises other risks. For example, if an attacker gets an opportunity to penetrate the security loopholes of an IoT system then it becomes easy for the attacker to exploit it to gain access to other valuable mobile data's or even corporate organizations. Another threat that is firmly connected with the IoT devices is a Distributed Denial-of-Service (DDoS) attack [66].

Exploitation of 5G and Edge Computing: On the same current note, 5G and edge computing are advantage for mobile by increasing its effectiveness; but they are threats. Edge computing is dispersed, and, as a result, there are several entry points as data processing takes place close to the consumer. In this case, breach in the edge devices may be used by the attackers to contaminate data while in the network for storage in central servers [67].

Mobile Ransom ware: Mobile ransom wares are being launched through political links. These attacks alter the password or even lock its user's data and demand a ransom to unblock the device or data. Now people use the mobile system for business and other related activities, and the outcome of ransom ware is beyond imagination [68].

Implications for Information Assurance: The specified trends and threats mean the need for proper proactive activities for enhancing mobile information assurance. Organizations and individuals must adopt advanced security measures, such as:

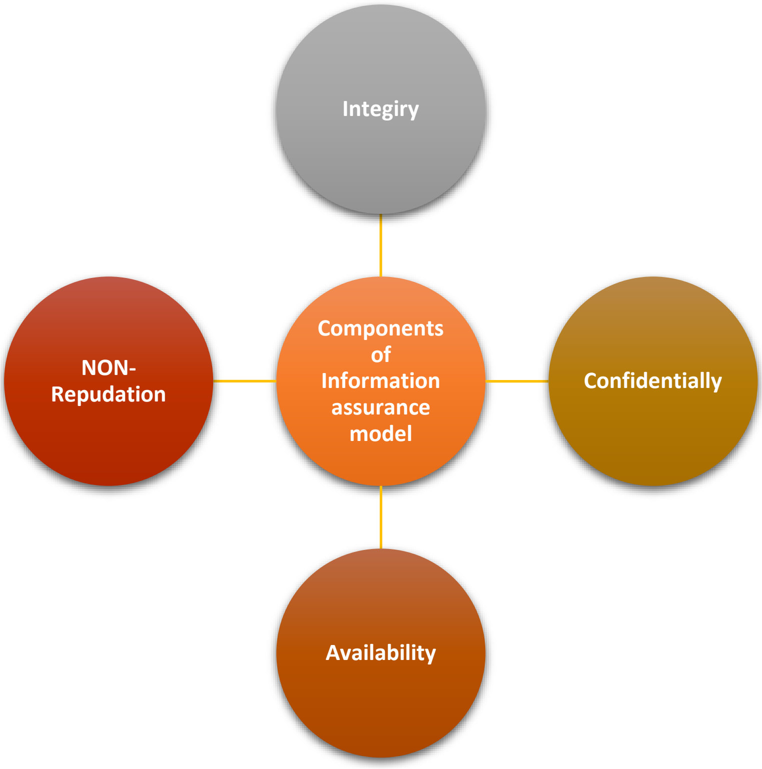

Figure: 3 showing components of information assurance model

AI & Machine learning provided live threat identification and countermeasures matrices. Less vulnerability of IoT devices, more frequent updates, adherence to high standard of authentication. Stoppages of encryption of mobile transaction and communication. Remind the users of the presence of phishing, smishing, and social engineered incidents and informatively update them often [69]. To implement best practices of SASE for right network and cloud environment. Mobile information assurance is the ensuring that information that is resident in, or transmitted to/from, one or more systems is secure within the mobile environment that is synonymous with the technological advancement and the threats. Even as such promising values as 5G, IoT, and AI existed in the present, they generated more threats that should be solved regularly from time to time. Through learning these trends, it is possible for all the parties particularly the organizations and the users avoid several risks in order to enjoy the secure use of mobile systems as the world on advances [70].

Anticipated Development Trends in Mobile Information Protection

Due to the mobile technology and the evolving threat situations, mobile information assurance is more of an evolving and growing area of practice. Mobile systems hence offer an interesting and challenging area since the part played by these devices in people’s daily and working lives increases, the need for the right security solutions from the actual application of new technologies together with effective policies and partnerships also increases. The present section is therefore concerned with establishing any broad future trends and programmers likely to characterize the form of mobile information assurance in the following years [71].

Integration of Artificial Intelligence (AI) and Machine Learning (ML): After gaining this knowledge we realized that both AI and ML have the capability to revolutionize mobile security greatly. These technologies can enable one to do threat prediction in that one is able to feed data sets into it to look for signs of threat. For example, Mobile Threat Defense (MTD) solutions, built on the AI technology, are able to discover the phishing threats, malware and zero days risks in the process of their occurrence [72]. Mobile systems can also get protect in the future by new self-learning solutions to protect against new kinds of threats, which is increasing the security and reliability of the mobile devices. But as the attackers also employ AI for manufacturing elaborate threats, the question of nice usage of the AI and back will become reflections.

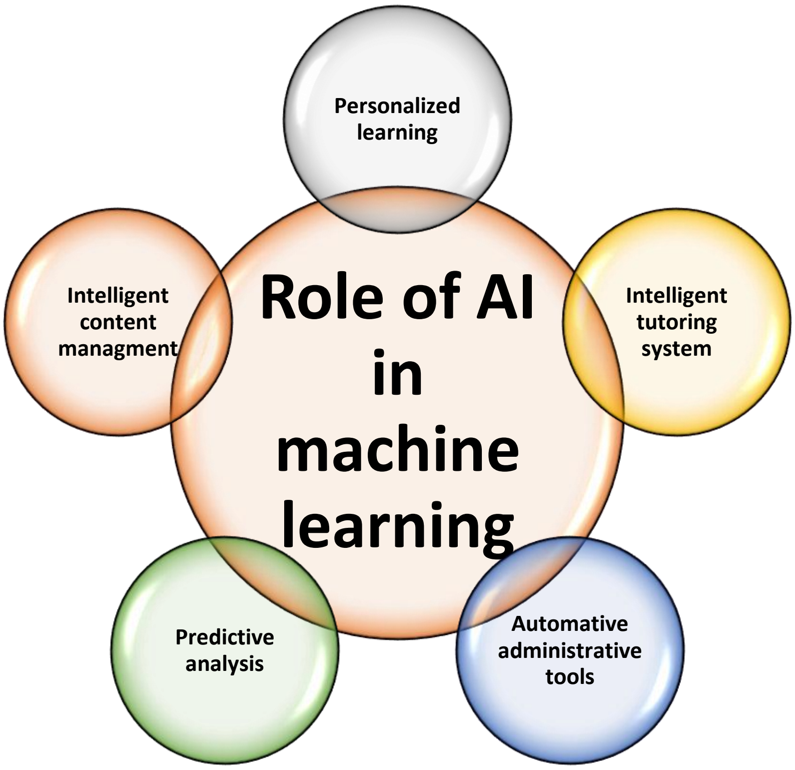
Personalized learning
Intelligent content managment
Role of AI in machine learning
Intelligent tutoring system
Predictive analysis
Automative administrative tools

Figure: 4 showing role of AI in machine learning

Advancements in Biometric Security: Recognition techniques such as face recognition, fingerprint scan, voice recognition are now considered to improve even further in the future. Nonetheless, the prospective future biometric technologies consist of more biometrics modes besides when two or several biometric factors are involved. Similarly, continuative authentication that is accountable for identification during the period of utilization will be used more frequently. Such developments will remove the usage of the passwords, which are still a vulnerability in mobile security till date [73].

Quantum-Resistant Encryption: Quantum computers are expected to appear in the future while standard encryption is at risk to be attacked by the quantum computers. Hence, the task is involved in development and deployment of the quantum-resistant encryption algorithms for the Mobile data security. We need to embrace these more elaborate cryptographic methods in order to disallow similar attacks from occurring in the future, both for organizations and the manufacturers of mobile devices [74].

Enhanced Security for IoT and 5G Ecosystems: The new and broader relationship between IoT devices and the already existing 5G networks also point at the need for the safety of such connected spaces. The following work will be devoted to the expansion and improvement of the security and the anti-tampering of IoT devices as well as their downstream firmware, as well as to search for efficient ways to protect edge computing [75].

Global Collaboration and Standardization: When mobile transnational systems are being created, protection of these systems is likely to require international assistance. They will have to develop continued standardized plans, directions, and definitions for the framework of reference architectures that can regulate security measures' organizational patterns transcending organizational boundaries. Of course, the transnational oriented problems would indeed involve semi self-initiatives through partnership formation, public-public, public-private, as well as bilateral/bilateral and multilateral arrangements [76]. Otherwise, new roles, perspectives, and clusters – this time, permitting collaboration – will define the orientation in the future of mobile information assurance, new stances, approaches, ideas, and technologies. Balanced with newer construct like AI, conclusive encryption, and enhanced facial recognition, mobile systems can jointly grow regulation, commitment, and international collaboration effectively to keep secure and genuine to the regularly emerging threats adequately.

CONCLUSION

It has improved the fluency of communication, the ability to work away from home and the interaction with the world becoming smooth, with the negative effect of creating several types of security problems. Thus, effective information assistance in the mobile environment can only be reached when using the several facet of approach that is the better technologies, good policies and some aggressive to the threats. This paper aims to make readers understand the fundamentals of information assurance in mobility and the technologies available to ensure secure systems for such information and for providing the conflicting operations. The components are Encryption, Authentication, Communications, and Authentic Mobile Threat Detection Systems which forms the structure of the Mobile Security. The enablers or the form of security could be mobile Policies and Compliance Frameworks. Services based on newer technologies like 5G, IoT and AI based services are the opportunities that lay hidden in threats since there are newer threats and there are always new ways to exploit a vulnerability.

Further work shall focus on aligning the mobile ecosystem, to further innovations such as quantum-resistant encryption, efficient biometric identification, and AI threat identification. They also call for governments, organizations, and leaders of the industries to synchronize efforts in formulating standard needs and tendencies across the globe besides addressing inter-continental difficulties. An effort to acquire information assurance in mobile environment is still ongoing; hence it requires active, creativity and collaboration.

REFERENCES

1. Treiblmaier H, Rejeb A and Strebinger A 2020 Blockchain as a Driver for Smart City Development: Application Fields and a Comprehensive Research Agenda Smart Cities 3 853– 72
2. Elagin V, Spirkina A, Buinevich M and Vladyko A 2020 Technological Aspects of Blockchain Application for Vehicle-to-Network Information 11 465
3. Jabbar R, Kharbeche M, Al-Khalifa K, Krichen M and Barkaoui K 2020 Blockchain for the Internet of Vehicles: A Decentralized IoT Solution for Vehicles Communication Using Ethereum Sensors 20 3928
4. Rotuna C, Gheorghita A, Zamfiroiu A and Smada D-M 2019 Smart City Ecosystem Using Blockchain Technology IE 23 41–50
5. Gösele M and Sandner P 2019 Analysis of blockchain technology in the mobility sector Forsch Ingenieurwes 83 809–16
6. Wong P F, Chia F C, Kiu M S and Lou E C W 2020 The potential of integrating blockchain technology into smart sustainable city development IOP Conf. Ser.: Earth Environ. Sci. 463 012020
7. Tarulescu S, Tarulescu R, Soica A and Leahu C I 2017 Smart Transportation CO 2 Emission Reduction Strategies IOP Conf. Ser.: Mater. Sci. Eng. 252 012051

8. Zhang X, Xu Q, Lu J and Xu J 2021 Conceptual characteristics and analysis of typical application scenarios of energy blockchain J. Phys.: Conf. Ser. 1738 012113
9. Creutzig F 2021 from smart city to digital urban commons: Institutional considerations for governing shared mobility data Environ. Res.: Infrastruct. Sustain. 1 025004
10. Finger, M., Bert, N. & Kupfer, D. (2015) 3 rd European Intermodal Transport Regulation Summary "Mobility-as-a-Service: from the Helsinki experiment to a European model?" Technical report, European Transport Regulation Observer No 2015/01. Finnish Transport Agency (2015). MaaS Services and Business Opportunities. http://www2.liikennevirasto.fi/julkaisut/pdf8/lts_2015-56_maas_services_web.pdf
11. Gerpott, T. J. and Thomas, S. (2014). Empirical research on mobile Internet usage: A meta-analysis of the literature. Telecommunications Policy, 38, pp 291-310. Heikkilä, S. (2014). "Mobility as a Service-A Proposal for Action for the Public Administration, Case Helsinki." https://aaltodoc.aalto.fi/bitstream/handle/123456789/13133/master_Heikkil%C3%A4_Sonja_2014.pdf?sequence=1
12. Herring, H., and Sorrell, S. (eds) (2008). Energy Efficiency and Sustainable Consumption. The Rebound Effect. Palgrave Macmillan, Basingstoke. Hoadley, S. (ed) (2017) Mobility as a Service: Implications for Urban and Regional Transport. Discussion paper.
13. POLIS, Brussels, Belgium. Jittrapirom, P., Caiati, V., Feneri, A.-M., Ebrahimigharehbaghi, S., Alonso-González, M., J. & Narayan, J. (2017). Mobility as a Service: a Critical Review of Definitions, Assessments of Schemes, and Key Challenges. Urban Planning, 2, 13-25.
14. Lee, D. (2016) Is Uber getting too vital to fail? http://www.bbc.com/news/technology-38252405 accessed 28th August 2017.
15. Yang, Y., & Ma, M. (2015). Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds. IEEE Transactions on Information Forensics and Security, 11(4), 746–759.
16. Yang, Y., Liu, X., & Deng, R. H. (2018). Lightweight break-glass access control system for healthcare Internet-of-Things. IEEE Transactions on Industrial Informatics, 14(8), 3610.
17. Yang, K., Jia, X., & Ren, K. (2014). Secure and verifiable policy update outsourcing for big data access control in the cloud. IEEE Transactions on Parallel and Distributed Systems, 26(12), 3461–3470.
18. Ying, Z., Li, H., Ma, J., Zhang, J., & Cui, J. (2016). Adaptively secure ciphertext-policy attribute-based encryption with dynamic policy updating. Science China Information Sciences, 59(4), 042701.
19. Li, H., Liu, D., Alharbi, K., Zhang, S., & Lin, X. (2015). Enabling fine-grained access control with efficient attribute revocation and policy updating in smart grid. TIIS, 9(4), 1404–1423.
20. Martins, A., and Eloff, J. (2001). Information Security Culture. Retrieved December 12, 2012, from http://etd.rau.ac.za/theses/available/etd-04292004-10222/restricted/SEC2002FinalVersion.pdf - 12thDecember,2012
21. Mayring, P. (2000). Qualitative Content Analysis. Forum: Qualitative Social Research, 1(2). Retrieved June 17, 2013, from http://217.160.35.246/fqs-texte/2-00/2-00mayring-e.pdf.
22. McDonough, C. (2003). Identifying the Risk Involved In Allowing Wireless Portable Devices Into Your Company. InfoSec Reading Room. SANS Institute McDowell, M. (2008). Business Mobility: A Changing Ecosystem. Information Knowledge Systems Management, 7, 25–37.
23. McIntosh, J.C., & Baron, J.P. (2005). Mobile Commerce's Impact on Today's Workforce. International Journal of Mobile Communications, 3 (2), 99–113.
24. Michael, H. (2012). Android malware perspective: only 0.5% comes from the Play Store. Retrieved February 15, 2013, from http://www.phonearena.com/news/Android-malware-perspectiveonly-0.5-comes-from-the-Play-Store_id36696
25. Moody, D., & Walsh, P. (1999). Measuring the Value of Information: An Asset Valuation Approach. University of Melbourne, Department of Information Systems, Melbourne Musaji, Y. (2006). A Holistic Definition of IT Security—Part 2. Infromation Controls Journal (ISACA)
26. Olzak, T. (2006). Strengthen Security with an Effective Security Awareness Program. Retrieved December 17, 2012, from http://adventuresinsecurity.com/Papers/Build_a_Security_Awarsseness_Program.pdf
27. Patton, M.Q. (2002). Qualitative Research and Evaluation Methods.Thousand Oaks, CA: Sage.
28. Post, G. V., & Kagan, A. (2007). Evaluating Information Security Tradeoffs: Restricting Access Can Interfere With User Tasks. Computers and Security, 26 (3), 229 - 237.

29. PricewaterhouseCoopers (2012). Changing the Game: Key Findings from the Global State of Information Security Survey 2013. Retrieved February 21, 2013, from http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013- giss-report.pdf
30. Pinto, F., Afghah, F., Radhakrishnan, R., Edmonson, W.: Software Defined Radio implementation of DS-CDMA in inter-satellite communications for small satellites. In: 2015 IEEE WiSEE, pp. 1–6 (Dec 2015)
31. Velasco, C., Tipantuña, C.: Meteorological picture reception system using software defined radio (SDR). In: 2017 IEEE Second Ecuador Technical ChaptersMeeting (ETCM), pp. 1–6 (Oct 2017)
32. Pei, Y., Chen, H., Pei, B.: Implementation of GPS Software Receiver Based on GNU Radio. In: Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC). pp. 1–3 (July 2018)
33. Janicik, J., Wolff, J., Friedman, A.: Cybersecurity in Modern Spacecraft Operations. In: Proceedings of the 28th Annual AIAA/USU Conference on Small Satellites,. No. SSC14-P4-5 in Poster Session (2014).
34. Dillon, H.: Receiving weather satellite images with Softrock. http://www.alternet.us.com/?p=1398 . Accessed 30 Jan 2019
35. Baguley, R.: Full Earth Disc Images from GOES-17 Harvested By SDR (2019). https://hackaday.com/2019/05/03/full-earth-discimages-from-goes-17-harvested-by-sdr/ . Accessed 14 Jun 2019
36. Maloney, D.: Eavesdropping On Cosmonauts with An SDR (Mar 2019). https://hackaday.com/2019/03/28/eavesdroppingon-cosmonauts-with-an-sdr/#more-350387. Accessed 14 Apr 2019
37. Rtl-sdr.com: RTL-SDR Tutorial: decoding Inmarsat STD-C EGC Messages (Aug 2015). https://www.rtl-sdr.com/rtl-sdr-tutorialdecoding-inmarsat-std-c-egc-messages/.
38. Accessed 15 May 2019 69. Chweh, C.: Autonomy in space. IEEE Intell. Syst. Their Appl. 13(5), 78–80 (1998)
39. Webster, G., Brown, D., Cantillo, L.: Nasa mars rover can choose laser targets on its own. https://mars.nasa.gov/news/nasa-marsrover-can-choose-laser-targets-on-its-own/. Accessed 08 May 2019
40. Obata, T., Nakasuka, S., Aoyanagi, Y., Matsumoto, T., Shirasaka, S.: On-Orbit Demonstrations of Robust Autonomous Operations on CubeSat. In: 32nd Annual AIAA/USU Conference on Small Satellites. No. SSC18-WKX-02 in A Look Back: Lessons Learned (2018)
41. Kennedy, A.K., Cahoy, K.L.: Initial Results from ACCESS: An Autonomous CubeSat Constellation Scheduling System for Earth Observation. In: 31st Annual AIAA/USU Conference on Small Satellites. No. SSC18-X-03 in Ground Systems (2017
42. Ogilvie, A., Allport, J., Hannah, M., Lymer, J.: Autonomous Satellite Servicing Using the Orbital Express Demonstration Manipulator System. In: 9th International Symposium on Artificial Intelligence, Robotics and Automation in Space (01 2008)
43. NASA: Cubesat Proximity Operations Demonstration (Mar 2016). https://www.nasa.gov/sites/default/files/atoms/files/cpod_fact_sheet-7march2016.pdf. Accessed 29 May 2019
44. SpaceX: Starlink mission overview (May 2019). https://www. spacex.com/sites/spacex/files/starlink_press_kit.pdf. Accessed 08 Feb 2019
45. Tepe, A., Yilmaz, G.: A survey on cloud computing technology and its application to satellite ground systems. In: 2013 6th International Conference on Recent Advances in Space Technologies (RAST), pp. 477–481 (June 2013)
46. Kongsberg: KSAT. https://www.kongsberg.com/ksat/. Accessed 01 April 2019
47. Earth-i: Earth-i to use KSAT's Ground Stations to Receive First Commercial Full-Colour Video from Space (Dec 2017). https://earthi.space/press/earth-i-use-ksats-ground-stations-receivefirst-commercial-full-colour-video-space/ . Accessed 01 April 2019
48. HawkEye 360: HawkEye 360 Selects Norway's Kongsberg Satellite Service (KSAT) to Provide Ground Station Services for Pathfinder Mission (Apr 2018). https://www.he360.com/hawkeye-360-selects-norways-kongsberg-satelliteservice-ksat-to-provide-ground-station-services-for-pathfindermission/
49. Li, Y. (date2017) Future Roles of Public Authorities in Mobility as a Service (MaaS), Workshop Report. Smart Procurement for Better Transport H2020 Project.
50. Kamargianni, M., Li, W., Matyas, M., House, C., Count, W. (2016). A Comprehensive Review of "Mobility as a Service" Systems. In: 95th Annual Meeting of the Transportation Research Board.

51. Washington DC. MaaS International (2017). Finnish company MaaS Global completes funding round, raising €14.2 million. Press Release 02.08.2017, http://maas.global/press/. Last accessed 30th August 2017.
52. Morton, C., Budd, T. M., Harrison, G. and Mattioli, G. (2017). Exploring the expectations of transport professionals concerning the future automobility system: visions, challenges, and transitions. International Journal of Sustainable Transportation, 11, 493-506.
53. Abiodun, M. K., Awotunde, J. B., Ogundokun, R. O., Misra, S., Adeniyi, E. A., Arowolo, M. O., & Jaglan, V. (2021). Cloud and big data: A mutual benefit for organization development. Journal of Physics: Conference Series, 1767(1), 012020. 47.
54. Wu, F., Xu, L., Kumari, S., Li, X., Shen, J., Choo, K. K. R., & Das, A. K. (2017). An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment. Journal of Network and Computer Applications, 89, 72–85. 48.
55. Liu, C., Chen, J., Yang, L. T., Zhang, X., Yang, C., Ranjan, R., & Kotagiri, R. (2013). Authorized public auditing of dynamic big data storage on a cloud with efficient verifiable fine-grained updates. IEEE Transactions on Parallel and Distributed Systems, 25(9), 2234–2244. 49.
56. Baek, J., Vu, Q. H., Liu, J. K., Huang, X., & Xiang, Y. (2014). A secure cloud computing based framework for big data information management of the smart grid. IEEE Transactions on Cloud Computing, 3(2), 233–244. 50.
57. Dhawale, C. A., Misra, S., Jambhekar, N. D., & Thakur, S. U. (2016). Mobile computing security threats and solution. Int. J. Pharm. Technol, 8, 23075–23086.
58. Jambhekar, N. D., Misra, S., & Dhawale, C. A. (2016). Cloud computing security with collaborating encryption. Indian Journal of Science and Technology, 9(21), 1–7.
59. Awotunde, J. B., Ayo, F. E., Ogundokun, R. O., Matiluko, O. E., & Adeniyi, E. A. (2020, July). Investigating the roles of effective communication among stakeholders in collaborative software development projects. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), LNCS (Vol. 12254, pp. 311–319).
60. Yang, Y., Zheng, X., Chang, V., & Tang, C. (2017). Semantic keyword searchable proxy reencryption for postquantum secure cloud storage. Concurrency and Computation: Practice and Experience, 29(19), e4211
61. Azeez, N. A., Salaudeen, B. B., Misra, S., Damaševiˇcius, R., & Maskeli¯unas, R. (2020). Identifying phishing attacks in communication networks using URL consistency features. International Journal of Electronic Security and Digital Forensics, 12(2), 200–213.
62. Yang, Y., Liu, X., Deng, R. H., & Weng, J. (2017). Flexible wildcard searchable encryption system. IEEE Transactions on Services Computing, 13(3), 464–477
63. Osho, O., Musa, F. A., Misra, S., Uduimoh, A. A., Adewunmi, A., & Ahuja, R. (2019, October). AbsoluteSecure: A tri-layered data security system.In International Conference on Information and Software Technologies (pp. 243–255). Springer, Cham.
64. Bethencourt, J., Sahai, A., & Waters, B. (2007, May). Ciphertext-policy attribute-based encryption. In 2007 IEEE Symposium on Security and Privacy (SP'07) (pp. 321–334). IEEE
65. Waters, B. (2011, March). Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In International Workshop on Public Key Cryptography (pp. 53–70). Springer, Berlin, Heidelberg
66. Ayo, F. E., Folorunso, S. O., Abayomi-Alli, A. A., Adekunle, A. O., & Awotunde, J. B. (2020). Network intrusion detection based on deep learning model optimized with rule-based hybrid feature selection. Information Security Journal: A Global Perspective, 29(6), 267–283.
67. Yang, Y., Liu, X., Deng, R. H., & Li, Y. (2017). Lightweight sharable and traceable secure mobile health system.IEEE Transactions on Dependable and Secure Computing, 17(1), 78–91.
68. Thrana, S.A.: Innovative NewSpace Ground Segment—Global Coverage Available through the Cloud. In: 30th Annual AIAA/USU Conference on Small Satellites. No. SSC16–VII–07 (2016)
69. Signals, R.: RBC Signals Announces New Integration Agreement with Kubos. http://rbcsignals.com/rbc-signals-announcesnew-integration-agreement-with-kubos/. Accessed 29 May 2019
70. Shah, S.: AWS Ground Station first customers include DigitalGlobe, BlackSky and Spire (Nov 2018). https://www.computing.co.uk/ctg/news/3067137/aws-ground-station-first-customersinclude-digitalglobe-blacksky-and-spire . Accessed 01 April 2019
71. Witjes, N., Olbrich, and P.: A fragile transparency: satellite imagery analysis, non-state actors, and visual representations of security. Sci. Pub. Policy 44(4), 524–534 (2017). https://doi.org/10.1093/scipol/scw079

72. Council, C.S.C.: Cloud security standards: what to expect and what to negotiate version 2.0. https://www.omg.org/cloud/deliverables/CSCC-Cloud-Security-Standards-What-toExpect-andWhat-to-Negotiate.pdf . Accessed 26 Feb 2020
73. Wikipedia.com: Edge computing. https://en.wikipedia.org/wiki/ Edge_computing. Accessed 25 Jun 2019
74. Musa, S.: Smart City Roadmap. https://www.academia.edu/21181336/ Smart_City_Roadmap. Accessed 25 May 2019
75. Fleet Space Technologies: Fleet Portal. https://www.fleet.space/portal . Accessed 15 May 2019
76. The Consultative Committee for Space Data Systems: Overview of Space Communications Protocols. techreport 130.0-G-3, The Consultative Committee for Space Data Systems (Jul 2014). https://public.ccsds.org/Pubs/130x0g3.pdf 01 April 2019