Review Article

Perspectives of Managing Mobile Service Security Risks

Mohammed Ahmed Truki AlSudiary

MIS Department, College of Business Administration, King Saud University, Riyadh, Saudi Arabia

Correspondence should be addressed to Mohammed Ahmed Truki AlSudiary; mas@ksu.edu.sa

Received 12 June 2014; Accepted 5 October 2014

Academic Editor: Muhammad Khurram Khan

Copyright © 2015 Mohammed Ahmed Truki AlSudiary. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The rapid growth of mobile telecommunications industry has been influencing the tremendous technological diffusion offering lower access cost, mobility, and convenience based communication as compared to wired telecom. The global rise of mobile competition helped service providers to offer much improved services both in terms of capabilities, information processing, retrieval, and communication over typical problems of inefficiencies generated by monopolies in wired networks. While there are significant opportunities to leverage the growth of mobile devices to increase the effectiveness of mobile users, also there are significant concerns about security and privacy of sensitive data that must be handled in these devices. Correspondingly, cyber security is becoming one of the top priorities for any nation. This paper reviews and presents some of the literature exercises in this regard. Objectives of this paper are: (i) to bring into light the explicit and implicit assumptions on the nature of technological change and how they could raise security issues, (ii) to discuss the technology and management perspectives on the security issues, and (iii) to present them through a methodology oriented taxonomy. It is believed that the adoption of methodology driven by sense-and-respond model would serve as an effective means to achieve these objectives.

1. Introduction

Information and communication technology (ICT) has an increasing importance and development in business life. Importance of ICT has been arising because of the state-of-the-art developments taking place in wireless communication technology as well as the businesses that have tendencies to reach their customers through mobile services [1]. Mobile communication networks are made possible by the convergence of several different technologies specifically computer networking protocols, wireless/mobile communication systems, distributed computing, and the Internet [2]. As smart mobile phone services use this converging technology, risks of attacking the security and privacy of mobile subscribers from using third party downloading “apps” could become a means and are growing [3].

These wireless technologies along with further development of state-of-the-art mobile technologies and the associated web services have led to the evolution of what is called the ubiquitous and pervasive computing phenomenon on the Internet (You et al., 2013) [4]. Ubiquitous networking and mobile computing can offer sensing and monitoring capabilities to smart homes equipped with security, identification, personalization systems, intelligent assembly systems, and so forth. It allows operating on e-mail, voice-mail, fax based applications, and audio and video applications along the sidewalks, in the car, and in airplanes too (see Figure 1) [2].

Ubiquitous services offer access, search, and service consumptions from an array of services and content providers anytime, anywhere while they are on move seamlessly. Mobile ubiquitous environment, while offering such useful functional capabilities and advantages, is bringing along new and unique security challenges or risks with it unfortunately [5]. In fact, during 2013 State of Union Address, President Barrack Obama cited cyber security as one of the top priorities for the United States [6].

A risk is the probability of causing a problem when a threat is triggered by vulnerabilities. Threats are much related to the characteristics of the assets and vulnerabilities are relevant to the security controls [7]. Varying definitions of vulnerability define risk as related to demographic characteristics, interpersonal relationships, access to resources, individual capacity, and the availability of support, with the
consideration of race and poverty as central factors. Information security assets are information technology resources associated with business assets. An asset is defined as any element of information that possesses a value. It includes tangible and intangible assets. The loss (or damage) of assets in an organization due to the cyber security incidents is measured by considering assets, threats, and vulnerabilities and so, the risk of information system’s asset could be determined by the following formula: \( \text{risk} = \text{threat} \times \text{vulnerability} \times \text{impact} \) [7].

In view of managing mobile security challenges and/or risks, several perspectives can be brought into the picture. Subsequent sections deal with these perspectives.

### 2. Methodology

To assess the security awareness in a mobile communication environment, a literature survey has been conducted to describe the security perspectives. Security and privacy management systems raise challenges to the domain of risk management of mobile security in view of demanding an integrated and holistic solution framework. So, firstly it is believed that the security taxonomy with the supply chain management paradigm would provide a comprehensive knowledge map of relevant artifacts and issues. Secondly risk management in mobile security aspect seeks practical analysis capabilities. In order to effectively describe and present such artifacts and issues, selection of a suitable management methodology becomes crucial as a driver and to conduct the risk assessment based performance management [8].

End-to-end systems in the pervasive computing environment are the fundamental requirements from the service provider (as well as device manufacturers) to sense and respond to the customer’s rapidly changing demands, and respond by launching new services. Service providers and device manufacturers are influencing each other in terms of obtaining extended service capabilities by relating service platform to device environment seamlessly [9]. Firmly embedding the cloud in the end-to-end processes is important because cloud has a potential to minimize the conflict that arises during legislation and internal policies while intending to offer a coherent system of governance, risk management, and compliance [10]. Cloud computing inherently combines three service paradigms such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). However, business process management as a service layer of the cloud computing layers can also be suggested [11]. It creates a one-stop transparent environment to providers so as to provide detailed information to their customers transparently who are involved in service delivery in order to satisfy the governance policy and also to better understand the service frauds (if occurred).

CRASP management methodology is developed and proposed (earlier by [12]) based on the basic premise of strategic sense-and-respond paradigm. The same sense-and-respond paradigm can also be made applicable to real-world
security in the form of CRASP methodology with a modified view by including both customer perspective and provider perspective to the generic business model suggested by [13]. So the objective of adopting CRASP management methodology is to offer the satisfying features such as security, usability, flexibility (adaptability), and cost efficiency [14]. Underlying the trend toward this sense-and-respond technology is the ideality of giving IT systems a deeper understanding of the semantics [15] of what can be observed as shown in figure (see Figure 2).

CRASP management methodology offers a way to drive innovation and business growth by leveraging the emerging technology for sustainable mobile business growth. Today’s mobile device cannot be viewed as simple phones anymore. It has evolved as a digital representation of self in the digital world by moving through the journey of stages such as acting as a communication platform, as an application platform, and sense-and-respond platform (using built-in GPS, digital camera, and environment sending as well as responding by sending text, audio, and video messages for authenticating self). With digital information management capabilities that a mobile is offering, it has changed the way business gets done [16].

3. Perspectives of Managing Mobile Service Security Risks

The adoption of mobile services is driven by an increasing need for mobility, but also by technical opportunities to streamline business processes and enhance interactivity. Security of wireless information is an important issue in mobile business. Providing an integrated perspective can potentially present the performance and security issues [17]. Usually the mobile business services sector can be driven by both demand and supply side factors. But the following classification of agile based perspectives is brought into the picture by following the CRASP methodology [12] and also by considering cloud computing model paradigm for an effective and efficient way of conducting mobile business service provisioning. Thus, the current model prefers to act as a hybrid model of demand and supply based as well as CRASP methodology based. Since the cloud provider acts as an agent for both cloud consumer and cloud owner, adopting this paradigm allows cost saving for both consumers (in terms of service cost) and provider (in terms of service efforts by not managing lower-level infrastructure components) in a manner that guarantees the security of the consumer's data and applications. Security is not a simple concept and cannot be easily measured. The three main security objectives that are required to be preserved in this regard are confidentiality (privacy), integrity, and availability (accessibility and usability) [18]. Hence, it is considered as the security issue structure under CRASP methodology taxonomy. Thus, business concerns, privacy protection, security, and risk free environment are breakpoints for making mobile commerce and mobile business popular (Wu and Wang, 2005) [19]. When it comes to dealing with the holistic or integrated mobile service view, it is believed that service encounter approach [20, 21] has a potential to suitably represent and adopt.

3.1. Sensor Perspective. Through the use of sensors, actuators, and context awareness, the virtual world is highly intermingled with the physical world creating opportunities through seamless interactions with everywhere anytime services availability. Providing information security and privacy in such environment is becoming a challenge. The main components of system architecture include policy service, context service, and event service (see Figure 2). The policy service manages security policies and encryption keys. The context service processes sensor data to derive high level context. The event service provides secure communication among components within the system [22].

3.1.1. Multimedia Based Sensing: Sensors and Types of Sensors. Devices, which perform an “input” function, are commonly called sensors because they sense a physical change in some characteristic that changes in response to some excitation. Devices that perform an output function are generally called actuators and are used to control some external device [23]. Sensors are an important part to any measurement and automation application. The sensor is responsible for converting some types of physical phenomenon into quantity measurable by a data acquisition system. Sensors are particularly useful for making in situ measurements such as in industrial process control. Some of the evaluating factors for selecting a sensor include accuracy, calibration, cost, environment, range, repeatability, and resolution [24]. Broadly, sensors can be categorized as vision based sensors, sound based sensors, touch based sensors, smell based sensors, and taste based sensors. These are natural sensors that are applicable to human

![Figure 2: Generic business model with sense-adapt-respond model](image-url)
beings. Industrial automation based sensors use artificial sensors (made by humans and machines). These artificial sensors when made as electronic devices can be classified into analog sensors and digital sensors and passive sensors and active sensors [23]. Similar to the role of natural sensors that help in better human decision making, there is a need to use the artificial sensors for better decision making capabilities in governance and business through process automation controls. In many scenarios, the basis for automation is context information that can be acquired unobtrusively by means of sensors. Consequently, it is vital to ensure the validity of the context information, especially in cases where automatic decisions can have severe security implications. In smart environments, the validity of context information can be ensured simply using a centralized context storage that is securely connected to all trusted sensors [25].

3.1.2. Enabling Security to Different Types of Sensors

(i) Accessibility Risks. Context-aware access control merges data from multiple context sensors and uses this data to determine whether users should be given access to context restricted resources. Encryption is used to restrict access to data resources [22]. The idea of encrypting sensitive data is done based on the confidential or secret levels such as SECRET and TOP SECRET. Each type of secret requires encoding with different key length. So handling the accessibility in the form of enabling cryptographic interoperability becomes a challenge in passing [26]. 4G packet-based routing of the sensor network is connectionless and thus inherently unreliable. Unreliable wireless communication channel might damage these packets. If protocol lacks the appropriate error handling, critical portions of data such as cryptographic key could get spoiled. Accessing such networks might result in unreliable communication. Synchronization issues can be critical to sensor security. Anything that has leaks with respect to sensors and sensor data would lead to subsequent wrong interpretations. Wrong usage and interpretations mean a kind of risk [27].

(ii) Usability Risks. The issue of digital or analog data conversion when using the sensors because different network providers might use different data transfer mechanisms (circuit-switching based or packet-data based data transfers) might arise [28]. It is because different network carriers provide access to different kinds of mobile systems. For example, in the US, Sprint, Verizon, and US Cellular use CDMA. AT&T and T-Mobile use GSM. The issue of improper matching of frequency band issue could arise when trying to use a CDMA based mobile among different network carriers.

(iii) Privacy Risks. Risk of sensitive data leakage (inadvertent or side channel). Call usage patterns could also indicate the identity and hence might lead to privacy risk. Smart phones store data in a unique way. Finding patterns from such smart phone could act as a finger print from the privacy perspective. Surveillance attacks could affect privacy. If proper attention on user policies and end user licensing agreements is not paid, it could lead to suboptimal privacy protection.

(iv) Integrated Security Risks. Managing the cryptographic interoperability becomes a challenging issue (see Figure 3).

3.2. Adoption Perspectives

(a) Context Perspective. Context-aware systems are able to adapt their operations to the current context without explicit user intervention and thus aim at increasing usability and effectiveness by taking environmental context into account [29]. The context service captures and processes contextual information from various sensors. Various contextual information is captured using various sensors, like temperature, lighting levels, sound levels, time and date, and schedule. High-level activities can be implied by fusing sensors or gathering raw data from various sensors and deriving higher-level contextual information. The context managers use first order logic to reason about contextual situation and derive higher-level or abstract contexts from sensor data. Sensor brokers mediate access to data produced by sensors and provide primitives for enabling communication with other components and service a smart space infrastructure [22].

(b) Network Perspective: Wireless Network Security Issues. Wide area wireless networks can be an enormous benefit to corporation because of their potential to reach very large extents of an enterprise application. The more the range of coverage by network, the more the potential of increasing the vulnerability of the devices, application, and data that can be expected. Today’s legacy and emerging wireless wide-area networks or 3G mobile networks, such as GSM (global system for mobile communication), UMTS (universal mobile telecommunication system), GPRS (general packet radio service), EDGE (enhanced data for global evolution), and CDMA2000 (code division multiple access 2000), already include security provisions in passing [30–32]. However, globally, there are more than 478 commercial networks with 4G based HSPA (high speed packet access) in more than 181 countries as of October 2012. Propelling the strong growth of selection of devices is due to the supporting HSPA. As
of October 2012, there were more than 3847 commercial HSPA devices worldwide from more than 285 suppliers [33]. Correspondingly, 4G mobile security has gained importance. 3G network infrastructure is usually wholly owned by the network operators and access is denied to other network entities. Since 4G is an open, heterogeneous, and IP-based environment, it will suffer from new security threats as well as inherent ones; therefore, the security must be addressed at the security architecture level [34]. The study of security issues in 4G networks has revealed that both WiMAX (Worldwide Interoperability for Microwave Access) and LTE (Long Term Evolution) security architectures are at advanced stage of specification. At MAC (Media Access Control) layer level, WiMAX is susceptible to DoS (Denial of Service) attacks, eavesdropping, replay attack, service degradation, and vulnerabilities due to faulty key management. Specific vulnerabilities include illegal use of user’s mobile equipment, location tracking, DoS attacks, and data integrity attacks. The robustness and effectiveness of end-to-end security approaches in WiMAX and LTE will become clear only after deployment [35]. As every network provider has his own security requirements, it is impossible to make a 100% secure system associated with 4G based heterogeneous network [36].

Fundamentally, mobile networks offer circuit-switch based data transfer mechanism and packet-data network mechanism [30]. Most of the fourth generation networks adopt packet-data transfer mechanism. Communication over the air interface between the mobile device and the network introduces additional security threats [37]. Moreover, it is required to address the security issues with an end-to-end approach. So with the large adoption of mobile communication, security in the wireless access network gained increasing interest over the last years and especially with 4G networks recently. When security is being provided, it impacts the network performance (e.g., end-to-end delay and throughput). Wireless networks could be wireless wide area networks (WWANs) or wireless local area networks (WLANs). WWAN family includes LTE (Long Term Evolution) or EPS (Evolved Packet System) and WLAN includes Wifi (802.11) technology. Broadcast nature of wireless network exposes subscribers to a greater risk from intruders who may eavesdrop and potentially alter transmitted messages, impersonate a legitimate subscriber, and therefore gain unauthorized access to network equipments. The wireless access network faces dual challenge of mobile management and security provisioning. In view of security concern, an impact of the authentication delay of approximately 64% of the total handoff latency is shown. Hence, it is required to have the security fast reestablishment during the handoff process [38].

(i) Accessibility Risks. Wireless network accessibility related security threats can be passive or active attacks. A passive intruder seeks to learn information from the communication. Though passive intruders do not get motivated to affect the original communication, the information gathered could be misused. On the other hand, an active intruder attempts to alter the exchanged messages, abuse the network resources, or affect the functioning of communicating entities [38].

(ii) Usability Risks. These are risks that could be faced by both providers and subscribers related to unauthorized consumption and use of network resources in an inappropriate way [38]. For example, mobiles that have Wi-Fi option can be switched on by subscribers in an open accessible internet environment without getting paid for its use by prepaid subscribers. On the other hand, subscribers might automatically get charged for making these Wi-Fi options “ON” irrespective of verifying the fact that these networks are effectively being used with those features (Wi-Fi and/or Bluetooth) by the subscriber or not.

So, the implication here is that some of the subscribers might get dissatisfied for these automatic deductions of charges carried by the network provider. Such policies need to be revisited to see if those options are just enabled by mistake and are not being used (by closely observing if the data transfer/actual downloads took place). Otherwise, it affects the purchase and use of smart mobiles. It is the usual tendency of any smart phone customer to see if these features are effectively working initially for the first attempt. They may not have the real intention to effectively use it at the time of purchase as well as in view of verifying the features. So, what is important here is the verification of whether such features are being effectively used in terms of data transfer or not. It can be done by interacting with the user to verify if the user is really interested in enabling those features for regular use. This is what can be understood as the situation of business exploitation for earning huge profits as mentioned in Section 3.2(iii) in this paper. It is because most of the business service providers are well aware of CRM (customer relationship management) concepts that are effectively being implemented and the business services when purchased are inherently charged for these CRM services too.

Other implications are the exploitation and misuse of the features by the intruders when acquiring the unauthorized access to such open networks. There is a potential that these intruders might prevent signaling from being transmitted inducing protocol failure (e.g., the suspected feature of the case of the 2014 event of Malaysian Airlines crash into the Hindu Ocean).

(iii) Privacy Risks. These are the risks that affect the subscriber privacy through identity theft and subscriber tracking. Observing pattern of the messages, location determination, and identifying the communicating hosts are the normal activities that are performed by the intruders. The nature of the communication is guessed based on observing the frequency and length of the exchanged messages [38]. Proper use of functions by software developers during software coding also affects data privacy. One example is the case of improper use of functions during sending login and password information by developers. While the use of POST functions protects the login and password information without displaying at the URL bar, the use of GET function actually reveals it [39].

(iv) Integrated Security Risks. These are the risks generated out of providing continuous access to subscribers while they are moving from one network provider to another network provider seamlessly. The potential risks could be raised from
signaling traffic and user traffic. Such seamless access might lead to unauthorized access to network services, denial of service, or even redirection of other users and control traffic in view of affecting source national security or the destination national security or the targeted national security in which the intruder is currently using the network.

3.3. Response Perspective. Various authentication mechanisms have been created and updated over the years in response to information security solutions in view of encountering the challenges and risks related to attacks and vulnerabilities. The concept of public key infrastructure (PKI) can provide technically sound and legally acceptable means to implement and satisfy the requirements of public key cryptography (PKC) [14]. PKI implementation features include strong authentication, authorization, data confidentiality, data integrity, and non-repudiation. It adopts lightweight directory access protocol (LDAP) as a predominant protocol in support of PKIs accessing directory services for distributing and managing digital certificates that often are used by web services for authentication. LDAP conforms to the X.500 data model [46]. However, a PKI can be depicted as a wireless PKI model aimed at securing M-commerce based on mobile phone through wireless communication having the adopted features such as optimization of a certificate validation with server-based certificate validation protocol (SCVP), reduced computation complexity of public key algorithm with ECDSA, and the adoption of 163-bit ECC/1024-bit RSA security mechanism (as against RSA private key mechanism of implementing algorithms) and will become more helpful in view of managing the cost [47]. Specific to the context of mobile environment, the PKI can be termed as MobilePKI. In order to solve mobile security problems, MobilePKI refers to

(c) Data in Transit Perspective: WAP Based Security Issues. Wireless application protocol (WAP) is an open protocol for the transmission of web like content to mobile phones and other wireless devices [40] and has become a motivating factor for developers, manufacturers, and content providers to adopt to also benefit from the economies of scale [41]. It can be used to access e-mail but the experiences in China showed that access to general e-mail was disappointing due to the restriction associated with the device. SMS based messaging is mostly adopted with a handset rather than e-mail [42]. 4G system based WAPS use X.805 protocol. X805 categorizes security threats of 4G as information or other resources destruction, changing or corrupting information, loss of information, leakage of information, or service interruption. However, 4G introduced security gateway facilitates security between domains that range from regional network to national mobile subscriber identity (national mobile subscriber identity) in clear text over air interface causing user to suffer from illegal tracing risk [44]. Careful design and selection of authentication protocol can serve as security mechanism in 4G network scenarios. EAP-SIM is a protocol for authentication and session key distribution using Global System for Mobile Communication (GSM) Subscriber Identity Module (SIM). The protocol offers mutual authentication through a challenge-response algorithm that occurs between the SIM card and the authentication service [44]. SPAKA scheme is one of the proposed schemes and is a self-certified public-key based AKA to offer fast access, flexibility, scalability, and nonrepudiation proof for 4G systems by categorizing authentication scenarios into registration authentication (first time registration) and call authentication (handoff process) [44]. Many 4G services are delayed sensitive. Guaranteeing short delays in networks with different access architecture and coverage becomes an issue. 4G forces the architects to make special architecture designs in terms of concealing the complexity to the user. It demands to have prior channel information in case of spectrum issues. It demands complex resource allocation management. It demands higher power consumption [43]. Quality of service of network nodes towards performance efficiency is also important in this regard [5].

(ii) Usability Risks. One usable risk associated with WAP is the consumption of more time to read with care. In smart mobile phone browsing scenario, there is a higher probability that the site does not know what the user wishes to access; it would present a generic or the irrelevant. Browsing, reading, and scrolling times become crucial challenges while using WAP based mobile phones [40]. Subscribers are required to be aware of different governance regulations when moving across different nations. But cost of smart mobile phones is usually more than that of other types of mobiles.

(iii) Privacy Risks. There is a risk of easily getting traced which is associated with seamless connectivity. Frequent downloads of getApp kind of applications can introduce new holes leading to more attacks at the application level that could affect privacy. GPS based spoofing could put others at risk. Data transmitted over Wi-Fi, Hotspots, and WLANs can often be intercepted quite easily resulting in real security risk [43].

(iv) Integrated Security Risks. Some of the integrated security risks related to adaptiveness are standardization issues, inconsistent policy based management issues [43], deciding the key length during the encryption related issues, and privacy and intellectual property issues [45].
Passport Certificate Server, which is a light weight PKI server [48].

(i) Accessibility Risks. One of the accessibility risks is to make sure that the user accessing the services is the same that authenticates with the mobile phone. Attending to such risk requires the need to attend only after solving the strong authentication method that guarantees that the identification methods used really provide strong authentication [14].

(ii) Usability Risks. Multiple password authentications are one more challenge. It raises the issue of forcing the user to repeat and write down (or memorize) multiple passwords to each different but relevant contexts. Authenticating with multiple passwords makes the user less usable. So single-sign-on (SSO) systems were developed to solve those issues. In SSO systems, two types of SSO are used: (i) pseudo SSO and (ii) true SSO. Pseudo-SSO limits itself to provide the identity information that corresponds to a specific service provider only. So in case of multiprovider environments (as a result of providing multimobile networking accessibility through collaboration strategy) managing such identity becomes an issue. Hence, there is a need to have true-SSO that relies on managing the identities of the user to provide authentication based on normalization of (multiple) service providers to confirm the specifications of the authentication mechanisms that the identity provider implements [14].

(iii) Privacy Risks. In many situations security and privacy always conflict. On one hand, security perspective demands for getting answers for their too many personal questions, on the other hand customers might feel that they are losing their privacy. Cross verification is a technique that is normally being used by many financial and credit bureaus as a part of dynamic knowledge-based authentication [49]. During this process, they pose many personal questions in view of making sure that the persons saying “who they are” are the persons that “actually they are”. If firms do not focus on maintaining the right balance act of asking contextually appropriate questions, customers might get upset with those questions that are like digging for personal details and might lose the opportunity of attracting and retaining business customers as the customers may feel that they are losing their privacy. Similarly many firms such as Twitter, Facebook, and LinkedIn work with third-party analytics vendors, such as Omniture (now part of Adobe Systems), DoubleClick, and Google Analytics firms that use browser cookies and dynamic knowledge based authentication to build a unique profile of a person. Most of the people do not even know the extent to which their Internet activity is being tracked and such tracking help building unique personal profiles. So the potential risk of privacy is the leakage of the identities based on these unique personal profiles built.

This discussion raises an implication of demand to design a wise public policy related to security and policy focusing at the meta-level concerns of web activities (e.g., predicting the motives, intentions, and concerns), which must be able to make sure that common citizens of a nation are protected against exploitations that might take place with private business parties whose motive is to cheat the customer for gaining large profits or with some public parties such as law enforcement and law agencies (e.g., police and justice departments) where some of their motives could be to benefit from exploiting the general public through blackmailing for earning extra money (bribing) and so forth. So focusing on this aspect will help national level intelligence agencies such as the Federal Bureau of Investigation and State level Intelligence Agencies and/or vigilance agencies in consolidating and reconfirming the final interpretations towards better judgments.

(iv) Integrated Security Risks. Traditional security operations and technology are focusing on designing only those security solutions that are limited to rely on events, log files, and alerts. However, analyzing a variety of nontraditional and unstructured datasets and forensic and historic analysis, visualizing and querying data in new ways, and integrating it with external intelligence to develop a complete threat profile are important. When big data analytics are added to security intelligence, the benefits are straight forward yet significant. It provides both detective and preventive intelligence support in order to properly provide enterprise response in terms of enhancing security decision making [6].

3.4. Cloud Perspective. A federated cloud offers a structure and a legal framework that enables authentication and authorization across different organisations and acts like trusted third party [46]. Security concerns raised by cloud computing are generally provider-related vulnerabilities, additional security concerns, availability, and third party data control [7].

PKI deployed in concert with single-sign-on (SSO) mechanisms are ideal for distributed environments, such as federated cloud environments, where users navigate between an abundance of cross-organisation boundaries [46]. Cyber security metrics characterizes as the extensions of system’s security controls in compliance with relevant procedures, processes or policies. When treating the domain of mobile security management from risk management perspective, a set of MTTF-like metrics can also be proposed to capture the concept of cyber security in passing [7].

(i) Accessibility Risks. Mobile services to users are available when they become subscribers. When subscribers sign up for service from a service provider on a contractual basis, the service provider then delivers services of data processing, data access, and data storage to subscribers. In the emergent cloud computing scenario, it poses a significant regulatory challenge on the application of data protection rules particularly on the regime regulating cross-border data flow. For example, with respect to the EU based protecting directives context as the rights and responsibilities in specific are not available in clear and transparent in finding information with regard to the existence of cloud that spans across multiple data centres, comprehensive reconciliation of data could pose a compliance issue against Article 25 prohibition on the extra-EU transfer of personal data with respect to virtualization and ad hoc data access and storage as mentioned in passing [50].
Protecting a user's account from theft is an instance of a larger problem of controlling access to objects including memory devices and software [46].

(ii) Usability Risks. If any risks are affecting confidentiality, authentication, and data usage of a mobile user, then they are called usability risks. On one hand, cloud could pose third party security risk problems [51]; on the other hand, it could also be argued that cloud may actually enhance privacy and security for sensitive data [52]. In case of the data stored in multiple locations (in multiple servers), the user might get the reduced risk of legality or the increased the risk of failure of protection in terms of not claiming a specific jurisdiction. If cloud provider is an agent of competitor, there is possibility that all the important private information could pass easily through corrupted prosecutors and intelligence agencies without further notice or processes [51]. On the other hand, it can also be argued that as service providers will have higher potential to employ specialized and dedicated staff to address the security and privacy issues, clouds will have higher potential to better manage security activities in terms of security configuration control, vulnerability testing, and security audits and security patching [52].

(iii) Privacy Risks. Personal sensitive and private data leakage that could affect the social and economic status of an individual in the society could be termed as privacy risk. Unintentional reminisce could leak privacy data during data management in association with disk and storage segmentation with the data centre staff across data centres in view of conducting nodal level performance and optimization management of user data [46]. Adopting numeric coding techniques and its use (instead of using long textual description of volume labels) during meetings and in routine maintenance management will help to protect privacy data loss risks.

(iv) Integrated Security Risks. Integrated security issues include standardization issues, pricing and billing issues, inconsistent policy based management issues [43], increased mobile service provider competition, increased content management from push based to pull based strategies being followed [53], increased process of authorization and control mechanism, more opportunity to strange and anonymous intruders to affect both the service provider’s and the subscriber’s tangible and intangible assets, the problem of claiming the service ownership, jurisdiction conflict problem in filing and prosecution issues for enforcing law on intruders (subjected to Interpol limitations), and potentially more prone to get child sexual abuse images, online frauds, deployment of viruses, botnets, and e-mail scams. More demands to have innovative forensic laboratory to support digital crime investigations and more focus on internet security governance, inadequate legislation, and lack of resource as major impediments to fight against cybercrime are an issue [54].

4. Implications

Policy makers and regulators need to analyze the nature of security weaknesses that relate to storing sensitive data in the cloud. In the first place, they should be in a position to segment what is government sensitive data with respect to confidentiality, privacy, and secrecy; otherwise, when mobile users try to use their smart phones and Google apps kind of applications to access such crucial and sensitive information, there is a risk of government data ending up on computer servers in other countries and/or involving parties that are outside the legal jurisdiction of national/regional courts [52]. WPA-2 is a security for wireless networks based on IEEE802.11i standard; WPA-2 provides government grade security by implementing the NIST (USA) FIPS 140-2 compliant AES encryption algorithm and 802.1x based authentication [45]. However, fundamentally in general it has to be understood that policies and law can help protecting risks (from governance perspective) to the most extent in terms of having strong principles, definitions and it application scope. They are expected to provide a means to serve as process level management encapsulations (unbound). Any detailed inferences on these risks would demand to look at the specific case data and its detailed analysis (bound), without which it is difficult to judge and provide a decision. It is important to make a verification on whether binding level inferences are true are fallacious. So, one metarule that helps to verify the conduct is the alignment of bounded rationality based analysis and its findings against the underlying abstract core principles specified in the policy and law. If the verification can be made through the identification of the presence of such principles, definitions, and so forth, either in direct manner or indirect (inferred) manner, then it can be inferred that there is compliance, otherwise not. Any comprehensive and holistic system must be in a position to code these meta-level rules effectively. In particular, the vigilance department must be in a position to help the good governance in coding such metarules in view of aligning them to the existing constitution, relevant policy, and laws. People on earth do essentially live with bounded rationality whereas ethics are available in the form of scriptures lying at unbounded level (e.g., policy, principles, and definitions).

The point of the highest level of maintaining regulations could become the source of potential for the leak of such sensitive information at the highest levels that could generate risk. So, the conduct that affects higher levels (which constitute the taxonomy of further lower level structures, processes, and controls) in terms of their bounded rationality based compliances to unbounded level process management level compliances become crucial to effective good governance.

So, the explanation that was given on metarule verification implies that people can be considered ethical only when they are aligning to scripture based living or at least show their tendencies towards it transparently; otherwise, people themselves become potential source of generating risk to the society. The reported findings and interpretations on security domain in general [55] say that the source for 80 percent of the malicious activity could be generating from internal people or internally designed processes. However, it cannot be denied that the fact of just considering the frequency is not enough and considering it alone is not important but also the intensity of impact does matter significantly (refer to mathematical equation given for risk assessment in the
introduction section). This is the reason why self-regulation theory and gate-keeping theory have gained importance in security management domain especially to deal with it and in achieving internal peace, security, and stability irrespective of whether the domain is belonging to tangible matter (people oriented) or intangible matter (process oriented). The role of technology here is treated as just an instrument or a means to conduct the process effectively and efficiently. These theories act as fundamental and meta-level theories of conduct to control and assess the potential strategic realizations and manifestations of performance management.

When virtualization (e.g., cloud computing environment) is adopted, use of simulation technique could serve as a testing environment. It means that the whole activities conducting on internet media could be treated as a set of simulation activities. Then the frequency of performance of such intangible malicious activities could mean testing on self-robustness in view of practicing and achieving control on self-regulation process based on self-regulation theory and gate keeping theory (as long as it is not affecting the third party privacy and security especially in a tangible manner).

Shibboleth system has a higher potential to cloud computing environment based security and privacy management. It adds value in terms of offering business process improvement via user attributes, extensive policy controls, and large-scale federation support via metadata [46]. In order to effectively deal with metarules for collaborative decision making, metadata is required to be accessed at the database schema level. But there is a possibility of compromising the privacy of users’ data items stored using a cloud provider’s simple storage device. Hence, database schema redesign and dynamic reconstruction of metadata for the preservation of cloud users’ data privacy become crucial. Such redesign could refer to the use of cryptographic techniques in sensitivity parameterization parent class membership of cloud data attributes and its application to relational privacy preservation operations especially to better manage the private clouds [56].

5. Conclusion

Synthetic indicators give quite faithful and uniform picture on national relative positions in innovative activities. The most relevant divergences can be attributed to different interpretations of technological change or research and management methodologies. In spite of having few significant descriptive outliers in the body of the text, the proposed convergent methodology and the initial version of this draft is believed to help in identifying and building an integrated theoretical framework of security risk factors through abstraction leading to measuring security risk performance management. It is required to highlight that the use of this methodology is to emphasize and focus on the presence of the inherent link between the macrolevel abstraction and the microlevel abstraction. While mobile services represent macrolevel abstractions, security risks with the corresponding state-of-the-art technology adoption describe the microlevel abstraction representation. It is believed that the effectiveness of security risk management lies in designing and visually manifesting this inherent link. It is a visual field that sets up the correlation between the actuators and sensors using some kind of sensoritic map of the sensoric input created from random senses initially but the goal is to establish or incorporate the innate knowledge of modality for faster validations and to support the corresponding responses in future [57] towards avoiding the potential risk of evil attacks and threats right at the gatekeeping mechanism level itself.

Thus, integrated data security gatekeeper is an important component to manage security and all critical exchanged information are going through the gatekeeper. Communication control in the gatekeeper is the key to manage interaction between applications and secure communication control. It enables both integrity and confidentiality (control of information flow) guarantees to be enforced by the system. Therefore, the gatekeeper must be tamper-proof and must take care of storing all the cryptographic material and performing cryptographic operations, especially signing and verifying safety messages [58].

Conflict of Interests

The author declares that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

The author extends over his appreciation to the Deanship of Scientific Research at King Saud University, Riyadh, for funding this work through the research group Project no. RGP-208.

References

[1] A. Ozer, M. T. Argan, and M. Argan, “The effect of mobile service quality dimensions on customer satisfaction,” Procedia—Social and Behavioural Science, vol. 99, pp. 428–438, 2013, Proceedings of the 9th International Strategic Management Conference.
[2] S. Pierre, “Mobile computing and ubiquitous networking: concepts, technologies and challenges,” Telematics and Informatics, vol. 18, no. 2-3, pp. 109–131, 2001.
[3] A. Mylonas, A. Kastania, and D. Gritzalis, “Delegate the smartphone user? Security awareness in smartphone platforms,” Computers & Security, vol. 34, pp. 47–66, 2013.
[4] I. You, M. R. Ogiela, Y.-S. Chen, and Q. Huang, “Mobile and internet services in ubiquitous and pervasive computing environments,” Information Sciences, vol. 230, pp. 1–2, 2013.
[5] A. Leung, Y. Sheng, and H. Cruickshank, “The security challenges for mobile ubiquitous services,” Information Security Technical Report, vol. 12, no. 3, pp. 162–171, 2007.
[6] IBM-SeClnt, “Smarter security intelligence,” http://public.dhe.ibm.com/common/ssi/ecm/en/ims14435usen/IMS14435USEN.PDF.
[7] L. B. A. Rabai, M. Jouinia, A. B. Aissa, and A. Milli, “A cyber security model in cloud computing environments,” Journal of King Saud University-Computer and Information Sciences, vol. 25, no. 10, pp. 63–75, 2013.
[8] X. Li, C. Chandra, and J.-Y. Shiau, “Developing taxonomy and model for security centric supply chain management,” International Journal of Manufacturing Technology and Management, vol. 17, no. 1-2, pp. 184–212, 2009.

[9] C. Fallenstein, J. Joseph, D. Lim, and J. C. D’Orsay, “On-demand business: network challenges in a global pervasive ecosystem,” in Mobile, Wireless, and Sensor Networks: Technology, Applications, and Future Directions, R. Shorey, A. Ananda, M. C. Chan, and W. T. Ooi, Eds., John Wiley & Sons, Hoboken, NJ, USA, 2006.

[10] M. Pauly, Cloud Computing End-To-End: Why Preparations is Everything, 3rd edition, 2014, http://www.wtw-systemsus.com/umnn/uti/508254_2/blobBinary/Backgrounder_DS-ps.pdf.

[11] IBM-Forum2014, IBM Technology Day Transforming your Business with IBM Cloud, Analytics and Security, March 19, 2014, Riyadh, Saudi Arabia, 2014.

[12] M. A. T. Alsudairy and T. G. K. Vasista, “CRASP—a strategic methodology perspective for sustainable value chain management,” in Proceedings of the 23rd IBIMA Conference, Valencia, Spain, May 2014.

[13] M. Donovang-Kuhlisch, “Security and privacy within an intelligent sensor grid,” in Proceedings of 11th International Commands and Control Research and Technology Symposium, Cambridge, Mass, USA, September 2006.

[14] A. Andrade, Strong mobile authentication in single sign-on systems [M.S. thesis], Department of Computer Science and Engineering, Aalto University, Espoo, Finland, 2011.

[15] IBM-SecSol, “IBM Security Technology Outlook: An outlook on emerging security technology trends. A white paper,” http://www.guruonline.tv/services/viewfile.aspx?type=1000&DocumentId=154623.

[16] PwC Advisory Oracle practice, “How to drive innovation and business growth,” http://www.pwc.com/en_US/us/supply-chain-management/assets/pwc-oracle-innovation-white-paper.pdf.

[17] J. Alaven and E. Autio, “Chapter IX-mobile business services: a strategic perspective,” in Mobile Commerce Technology, Theory and Applications, B. E. Mennecke and T. J. Strader, Eds., IRM Press, 2003.

[18] A. Kim and J. S. Moskowitz, Incentivized Cloud Computing: A Principal Agent Solution to the Cloud Computing Dilemma, NRL/MR/5540-10-9292, Naval Research Laboratory, United States Navy, 2010.

[19] J.-H. Wu and S.-C. Wang, “What drives mobile commerce? An empirical evaluation of the revised technology acceptance model,” Information and Management, vol. 42, no. 5, pp. 719–729, 2005.

[20] L. A. Mohr and M. J. Bitner, “The role of employee effort in satisfaction with service transactions,” Journal of Business Research, vol. 32, no. 3, pp. 239–252, 1995.

[21] M. A. T. Al Sudairy, “Enterprise infonomics model for strategic for strategic sustainable business development,” in Proceedings of the 23rd IBIMA Conference, Valencia, Spain, May 2014.

[22] J. Al-Muhtadi, R. Hill, and S. Al-Rwais, “Access control, using threshold cryptography for ubiquitous computing environments,” Journal of King Saud University-Computer and Information Sciences, vol. 23, no. 2, pp. 71–78, 2011.

[23] Electronic Tutorials, Sensors and Transducers, 2014, http://www.electronics-tutorials.ws/io/io_1.html.

[24] Engineer’s Handbook, “Sensors,” 2004, http://www.engineer-shandbook.com/Components/sensors.htm.

[25] W. Apolinarski, M. Handte, and P. J. Marron, “A secure context distribution framework for peer-based pervasive systems,” in Proceedings of the 8th IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 505–510, Mannheim, Germany, April 2010.

[26] NSA-CSS, “Suite B Cryptography/Cryptographic Interoperability,” 2014, http://www.nsa.gov/ia/programs/suiteb.cryptography/.

[27] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhury, “Chapter 17: wireless sensor network security: a survey,” in Security in Distributed, Grid and Pervasive Computing, Y. Xiao, Ed., Auerbach/CRC Press, Boca Raton, Fl, USA, 2006.

[28] I. F. Akyildiz and I. H. Kasimoglu, “Wireless sensor and actor networks: research challenges,” Ad Hoc Networks, vol. 2, no. 4, pp. 351–367, 2004.

[29] M. Baldauf, S. Dustdar, and F. Rosenberg, “A survey on context-aware systems,” International Journal of Ad Hoc and Ubiquitous Computing, vol. 2, no. 4, pp. 263–277, 2007.

[30] HP-WANS, “Enterprise Wireless WAN Security,” 2014, http://h20331.www2.hp.com/hpsub/downloads/WWAN-Security.pdf.

[31] C. J. Mitchell, Ed., Security for Mobility, The Institution of Engineering and Technology, London, UK, 2004.

[32] SANSI-3GM, Security along the Path through GPRS towards 3G Telephone Network Data Services, 2014, http://www.sans.org/reading-room/whitepapers/wireless/security-path-gprs-3g-mobile-telephone-network-data-services-165.

[33] 4GAmericas, HSPA: High Speed Packet, June 2014, http://www.4gamericas.org/index.cfm?fuseaction=page&sectionid=247.

[34] M. Aiash, G. Mapp, A. Lasbae, and R. Phan, “Providing Security in 4G Systems: Unveiling the Challenges,” 2010, http://eprints.mdx.ac.uk/6483/1/Secure_Barcelona_2010.pdf.

[35] N. Seddigh, B. Nandy, R. Makkar, and J. F. Beaumont, “Security advances and challenges in 4G wireless networks,” in Proceedings of the 8th International Conference on Privacy, Security and Trust, pp. 62–71, Ottawa, Canada, August 2010.

[36] S. Faisal, Performance analysis of 4G networks [M.S. thesis], Electrical Engineering. Blekinge Institute of Technology, Karlskrona, Sweden, 2010.

[37] S. Schwiderski-Grosche and H. Knospe, “Secure mobile commerce,” Electronics and Communication Engineering Journal, vol. 14, no. 5, pp. 228–238, 2002.

[38] S. B. H. Said, "A comparative study on security implementation in EPS/LTE and WLAN/802.11," in Wireless Networks and Security, S. Khan and A. S. K. Pathan, Eds., Signals and Communication Technology, pp. 457–489, Springer, Berlin, Germany, 2013.

[39] N. Padua-Perez and W. Pugh, Servlets and JSP, Department of Computer Science University of Maryland, College Park, Md, USA, 2014, https://www.cs.umd.edu/class/spring2006/cmsc132/Slides/lec33.pdf.

[40] I. C. Y. Ma and J. Irvine, “Characteristics of WAP Traffic,” Wireless Networks, vol. 10, no. 1, pp. 71–81, 2004.

[41] H. Evans and P. Ashworth, Getting Started with WAP and WML, Sybex Inc., Alameda, Calif, USA, 2001.

[42] X. Yan, “Mobile data communications in China,” Communications of the ACM, vol. 46, no. 12, pp. 80–85, 2003.

[43] J. Govil and J. Govil, “4G mobile communication systems: turns, trends and transition,” in Proceedings of the 2nd International Conference on Convergent Information Technology (ICCIT ’07), pp. 13–18, Gyeongju, Republic of Korea, November 2007.
[44] D. He, J. Wang, and Y. Zheng, “User authentication scheme based on self-certified public-key for next generation wireless network,” in *Proceedings of the IEEE International Symposium on Biometrics and Security Technologies*, pp. 1–8, April 2008.

[45] J. M. Chichira, “Mobile Computing with Security,” 2012, https://www.ibm.com/developerworks/community/blogs/96960515-2ea1-4391-8170-b0515d08e4da/entry/mobile_computing_with_security?lang=en.

[46] D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, 2012.

[47] F. M. Madani and I. Bimar, “Proposing a wireless PKI mobile optimized for M-commerce applications,” in *Proceedings of 3rd Information Security & Cryptology Conference with International Participation*, pp. 25–27, Ankara, Turkey, December 2008.

[48] Diversinet, *Diversinet Mobile PKI*, 2003, http://csrc.nist.gov/archive/pki-tw/g/2003/presentations/twg-03-18.pdf.

[49] R. Westervelt, “Knowledge-based authentication poses privacy issues,” 2014, http://searchsecurity.techtarget.com/magazine-Content/Knowledge-based-authentication-poses-privacy-issues.

[50] S. Y. Esayas, “A walk in to the cloud and cloudy it remains: the challenges and prospects of “processing” and “transferring” personal data,” *Computer Law & Security Review*, vol. 28, no. 6, pp. 662–678, 2012.

[51] M. A. T. Alsudairy and T. G. K. Vasista, “Cloud computing and privacy regulations: an exploratory study in issues and implications,” *Advanced Computing*, vol. 3, no. 2, pp. 159–162, 2012.

[52] N. I. King and V. T. Raja, “Protecting the privacy and security of sensitive customer data in the cloud,” *Computer Law & Security Review*, vol. 28, no. 3, pp. 308–319, 2012.

[53] EUR 21192, *The Future of Mobile Communications in the EU: Assessing the Potential of 4G*, 2014, http://ftp.jrc.es/EURdoc/21192-ExeSumm.pdf.

[54] Interpol, “World must better prepare itself for emerging cybercrime threats: interpol chief tells prestigious meeting in India,” http://www.interpol.int/en%3A2%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%20/News-and-media/News/2012/PR028.

[55] R. Grimes, “How to thwart employee cybercrime,” *InfoWorld Magazine*, 2010.

[56] A. Waqar, A. Raza, H. Abbas, and M. Khurram Khan, “A framework for preservation of cloud users data privacy using dynamic reconstruction of metadata,” *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 235–248, 2013.

[57] L. A. Olsson, C. L. Nehaniv, and D. Polani, “From unknown sensors and actuators to actions grounded in sensorimotor perceptions,” *Connection Science*, vol. 18, no. 2, pp. 121–144, 2006.

[58] H. Guo, L. H. Ngoh, Y. Wu et al., “Embedded info-security solutions for vehicular networks,” in *Proceedings of the 3rd International Conference on Communications and Networking in China (ChinaCom ’08)*, pp. 29–33, Hangzhou, China, August 2008.
Submit your manuscripts at http://www.hindawi.com