A Review of Cyber Security Issues in Hospitality Industry

Neda Shabani and Arslan Munir

Kansas State University, Manhattan, KS 66506, USA
nshabani@ksu.edu, amunir@ksu.edu

Abstract. The purpose of this study is to emphasize the importance of cyber security in hospitality industry. This study further identifies and analyzes several common network threats and recommends useful security practices and techniques to prevent cyber attacks in hotels. This study is a rich source of information for Information Technology (IT) directors and Chief Information Officers (CIO) to advance their policies and procedures for security of electronic information in hotels using the most recent and updated information available in the area of hospitality industry. The methodology of this study is a unique combination of qualitative method and review method for an in-depth understanding of real-life issues within the industry and the most recent technical and practical solutions that hotels use to handle and solve these issues. The findings of this study show that the techniques currently utilized by hotels to prevent cyber attacks are mostly rudimentary and outdated. Furthermore, study indicates that most of the hotel staff lacks the knowledge and expertise to handle potential threats and thus hospitality industry becomes even more vulnerable to cyber threats and attacks. Finally, the paper discusses some implications and recommendations to hotel's policy makers to help secure the hotels' and guests' information from security attacks.

Keywords: Cyber Security, Hospitality Industry, Information Security

1 Introduction

Technology in hospitality industry is driven by the increasing transaction volumes, complex reporting requirement, e-marketing [14], and international communication needs. Information technology (IT) can improve almost all areas of hospitality industry, such as guest services, reservations, food and beverage management, sales, food service catering, maintenance, security, and hospitality accounting. More recently, Internet of things (IoT) is shaping the future of hospitality management industry by opening up new avenues for immediate, personalized, and localized services. For example, in-room IoT units like thermostats, motion sensors, and ambient light sensors can be utilized to control the temperature and lighting in hotel rooms based on room occupancy to minimize

energy costs. Moreover, edge/fog computing can be utilized to provide location-based services for the hospitality industry [10]. Although technology incorporation in hospitality industry over recent years has transformed the way services are provided and received and has helped in improving guest experiences, it has also given rise to various challenges among which ensuring the cyber security of these incorporated technologies in the hospitality industry is of paramount significance [8] [11].

The use of technology in hospitality industry often requires gathering of guest information and thus can lead to data breach and information loss. To prevent against losses, organizations monitor their computer networks for a multitude of security threats, such as computer-assisted fraud, espionage, sabotage, vandalism, hacking, system failures, fire, and flood, etc. Since hospitality industry is a consumer-centric business where consumer loyalty and trust directly translates to revenue, hence to retain the public trust and to prevent copycat hackers to hack into an organization's computer systems, most of the hospitality organizations try not to reveal the data breaches and cyber attacks against their computer systems [4]. Thus, this paper mainly focuses on the review of cyber security threats and risks faced by the hospitality industry, state-of-the-art tools and techniques that can be employed by the hospitality industry to defend against cyber attacks, and implications and recommendations for the hospitality industry to help secure the hotels' and guests' information from security attacks.

1.1 Research Purpose and Research Questions

The purpose of this study is to emphasize the significance of cyber security in hospitality industry by identifying and analyzing several common network threats and recommending useful security practices and techniques related to electronic information and network systems to prevent cyber attacks in hotels. The following research questions were created to be answered based on the unique methodology leveraged by this study:

1. What methods, tools and techniques are currently used in hotels regarding computer network and information protection?
2. What are the current threats to computer network security in hotels?
3. What are the ways of handling security attacks in the hotel's computer networks?
4. What is the importance of network security in hotels?
5. Which methods hotels leverage to secure their websites for data and financial transactions?
6. What criteria hotels consider in making a strong password for their computer networks and logins (computers and websites)?

The remainder of this paper is organized as follows. Section 2 provides an in-depth review of cyber security issues in hospitality industry. Section 3 outlines the methodology employed by this study to answer the research questions posed by this study. Findings and results of this study are presented in Section 4. Section 5 concludes this study and provides recommendations for hospitality industry to help secure hotels' and customers' data from potential security attacks.

2 Background and Literature Review

This section discusses background and literature review related to cyber security in hospitality industry. In particular, this section discusses common hardware/software used in hospitality industry, information security tools and techniques, cyber threats, risks, and challenges in hospitality industry, and cyber attack prevention methods in hospitality industry. Figure 1 depicts an overview of cyber security threats in hospitality industry and potential cyber attack prevention methods that are discussed in this paper.

2.1 Hardware/Software Used in Hospitality Industry

IT is the science and technology of using computers and other electronics to save and transmit information. Organizations that use IT need to tackle and administer electronic information safely and securely. The organization's administrative managers are responsible for the protection of the organization's assets and information [4]. Like other organizations, IT systems in hotels comprise of both software and hardware. The basic software in a hotel includes the property management system (PMS), point-of-sale system (POS), call accounting system (CAS), and hotel accounting system. The basic hardware in a hotel include front desk computers, POS terminals, back office computers, cameras, printers, routers, switches, network cables, sensors and other IoT devices. The front and back office computers, POS terminals, and printers are connected to routers and switches with network cables that enable communication between these devices. The hotel's local area network (LAN) typically consists of devices within the hotel's premises. The hotel LAN is connected to other networks and the Internet through routers. The firewalls protect the hotel network from outside attacks. The hospitality industry uses the POS and PMS to manage reservations while avoiding duplex reservations for the same date and time [5].

2.2 Information Security Tools and Techniques

Organizations using IT are vulnerable to various security threats and attacks. The most common threats include viruses, inside attackers for network access, laptop theft, spoofing, unauthorized insider access, unauthorized outside attack, and denial of service attacks. Information security aims at maximizing the revenue of organizations and investments by minimizing the damage that could be caused by security attacks [13]. Most of the information security systems aim at providing three main security services: confidentiality, integrity and availability. Information security systems strive to protect valuable assets from disclosure or damage. This protection can be attained through both technological and non-technological methods, such as physical security of assets, user identification and authentication, biometrics, and firewalls [4]. We define some of the information security terminology, tools and techniques in the following:

1. Digital Identifiers (IDs) are the electronic counterparts of driver's licenses, passports, and membership cards. Digital IDs often include a username

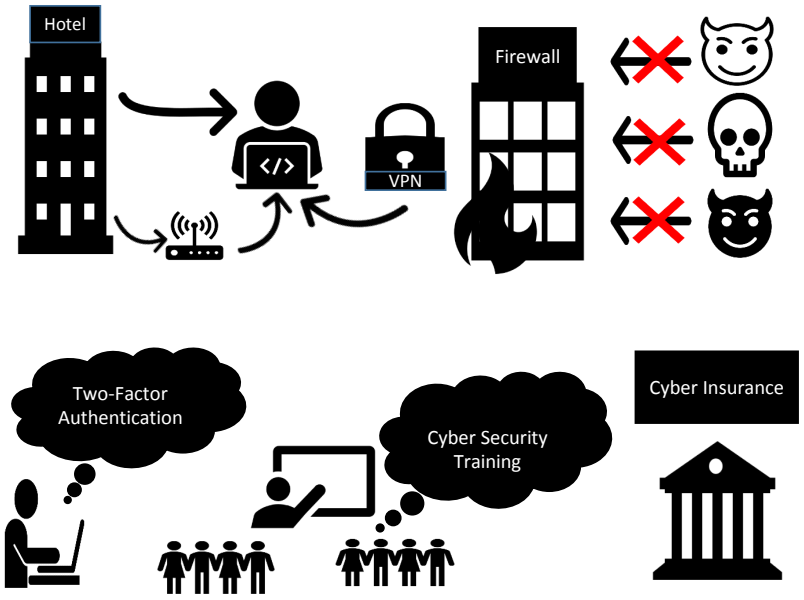

Fig. 1. Overview of cyber security threats for hospitality industry and potential cyber attack prevention methods.

and a password. In asymmetric cryptography (a type of information security system), a user/system possess a public key and a private key, which can serve as IDs. Digital *certificates* are used in asymmetric cryptography to authenticate public keys and IDs. A certificate binds the ID of a user/system to its public key by providing a digital signature over the public key and the ID of the user/system [12].

2. Intrusion Detection System is a system that analyzes the events happening in a computer system or a network to detect intrusions or attacks. An intrusion can be defined as an effort to circumvent security services employed by the system, such as confidentiality, integrity, and availability. Many times intrusions from malicious actors are aimed at carrying out a denial of service attack that makes the computer systems of an organization unavailable. Intrusions can be caused by various means: (i) attackers connecting to the systems from the Internet or the outside networks; (ii) authorized users of the systems who try to obtain additional privileges for which they are not authorized; and (iii) authorized users who misuse and abuse the privileges given to them.

3. Physical Security refers to keeping the networking and computing equipment of an organization in a secure physical environment [4].

4. Firewall can be a hardware, a software or a combination of hardware and software equipment to monitor the traffic between devices and/or two or more computer networks. A hardware firewall is a physical device that is attached to

a network while software firewall is a software that is installed on devices (e.g., computers, tablets, phones, etc.) in a network to monitor the network traffic flow. The firewall can also block particular malicious packets trying to enter or leave a computer network.

5. Encryption is the process of hiding the information by making the information transformed in a way that is impossible or very hard to understand. Encryption mainly provides confidentiality security service. The aim of encryption is to keep the information secret from all but the authorized parties.

6. Biometrics is a technology of authenticating a user based on physical or behavioral characteristics, such as finger prints, voice recognition, gait, and retina or iris identification. Biometric technology is an effective method of identity verification. The biometric systems measure the physical characteristics of an individual, and compare them with the recorded characteristics to verify the user's identity [1].

7. Access Control are techniques of restricting usage of system resources to authorized users/processes. Access control typically comprises of authentication and authorization.

8. Vulnerability Assessment Scan is a software that examines the system for potential vulnerabilities and inform the system administrator of those vulnerabilities so that system can be safeguarded against those weaknesses [4].

2.3 Cyber Threats, Risks, and Challenges in Hospitality Industry

Cyber crimes have always been there since the introduction of computers, however, the nature of attacks and crimes varies as the technology evolves. Hacking, technology theft, and frauds are the most common security attacks whereas other security attacks are also possible [4]. Most of the hacking attacks are aimed at obtaining confidential information (e.g., financial information of banking accounts, user accounts information) without authorization. Technology theft occurs when an attacker consciously connects to a computer with intentions to steal technological information. Theft of trade secrets happen when a person or a business uses confidential trade information for (another) business without authorization. Fraud transpires when an attacker consciously connects to a computer with intentions of fraud or masquerades a legitimate user of the computer system.

The appraised cost of cyber crimes is approximately $6 trillion per year on average through 2021 [6]. Consequently, organizations are increasing their cyber security budgets to mitigate potential data breaches. The average cost of a data breach for an organization is in millions, however, this cost only accounts for the direct cost of the data breach which is quantifiable. The true cost of data breach for a business is much higher than this when outlook for a business and collateral effects in the aftermath of a breach are considered.

Although hospitality industry aspires to provide trust and comfort to guests, achieving this is not easy anymore due to lots of potential threats that are aimed at destroying the reputation of hotels as well as destroying the customer trust by

acquiring and abusing guests' personal and financial information. Hoteliers must know that these threats are always out there, and they need to take responsibility for any data loss as they can prevent this data loss and breach from happening by adopting effective preventing measures.

Data breaches in the world of business are consistent and remind the organizations the significance of incorporating cyber security tools and techniques in their businesses to help prevent such incidents. Besides implementing cyber security tools and techniques, it is imperative for hotel users and staff to have fundamental knowledge about cyber security and practices. One of the most significant factors that can prevent data from being breached or loss is to be careful and conscious about what sources of information to trust and have some knowledge about secure websites and emails versus not secure websites and emails. For example, opening an unsecure website or clicking on the link within an unsecure email can cause a big disaster for a hotel if the staff are not knowledgeable enough in this regard. In addition, hackers and attackers are not only able to abuse the computer system of the hotels by using different type of phishing email, viruses, etc., but also, they are able to attack and take advantage of Wi-Fi in the hotels [3]. Most of the hotels nowadays offer free Wi-Fi to their guests and the guests can have access to the same network all over the hotel such as lobby, convention center, dining room and other places within the hotel. If the hotel Wi-Fi is not secure, which is the case for most of the contemporary hotels, hackers can monitor the guests' traffic on the Wi-Fi and use that to steal the guests' private information. Furthermore, by taking advantage of hotels' Wi-Fi, hackers can offer malicious "updates" for famous software such as Adobe Reader or Flash Player so that the users would not hesitate to update their software and then those updates contain malware that criminals use to get all the usernames, passwords, or other important information from users' computers or smartphones. Interestingly, in most of the cases, the software programs that are used by hackers and cyber criminals, are not new programs and can be even decade old programs. However, due to negligence and ignorance of many hotels and lack of system updates, even these old software programs can be utilized by the hackers to acquire confidential information from the hotels [7].

Attackers can be from both inside and outside an organization. Especially in hospitality and tourism industry where turnover rate is very high, the possibility of inside attackers is higher in comparison to other industries. Consequently, some organizations, such as Burger King Corporation, take measurements to prevent inside attackers, and provide infrastructure to ensure only a single sign-on by an employee. In this case, only one record needs to be expunged from the system in case of an employee's termination or resignation so that the former employee will not have any access to the system [4].

There are so many ways that attackers can get into guests' information, however, one of the most common ways that attackers use specifically in hospitality industry to breach data is "Fake Booking", in which the attacker build and design a website with the exact look and features of the main hotel's website and use the same name to pretend that it is the hotel's legitimate website. Conse-

quently, many potential guests visit that phishing website and probably some of them book their room through that fake website, thus revealing all their personal and financial information to the attacker.

2.4 Cyber Attack Prevention Methods in Hospitality Industry

It is to be noted that none of the security software, antiviruses, and other tools can 100 percent guarantee to prevent hotels and any other business from cyber attacks, however, hotels must implement the most effective and updated tools and techniques to secure their information as much as possible. In general, hotels can divide the process of securing their information into three phases: prepare and protect, defend and detect, respond and recover.

One of the tools to prevent data breach attacks that hotels can take advantage of is web application firewall (WAF). WAF is different from regular firewall (discussed in Section 2.2) in that a WAF is able to filter the content of specific web applications and thus help preventing attacks originating from web application security flaws, such as SQL injections, buffer overflow, and security misconfigurations. WAF solutions are also useful to detect and prevent data theft because in case of attackers targeting credit card database, the WAF solutions can detect and block the database.

Another way to secure data in hotels is by employing digital certificates (Section 2.2). Digital certificates bind a message to the owner/generator of the message and help provide non-repudiation security service. In hospitality industry, digital certificates can help prevent frauds from customers or hotel/restaurant owners as false claims from either can be legally challenged and the truth be established by using digital certificates. The use of digital certificates by hotels for their websites ensure the authenticity of their websites to the customers.

Cyber security insurance can provide hotels another way to secure themselves and customers' information as well as cover their losses in the case of data breach. According to Butler [2], cyber security insurance must be a consideration for any hotel owners. Hotel owners must know that data breaches and cyber claims are not included in general liabilities policy, which makes it even more important for hotel owners to think about and acquire cyber insurance to cover any claims in case of a cyber attack. Cyber security insurers will cover both first and third party in the case of cyber attack and data loses. The third party can be both customers and government or any regulatory agencies.

3 Methodology

This paper takes advantage of two research methodologies to emphasize the importance of cyber security in hospitality industry. One of the methodologies is an in-depth review of all academic and professional articles available in the area of hospitality cyber security. The authors have summarized in Section 2 the most important findings and issues related to cyber security and threats for hospitality industry in this paper. The other methodology was qualitative in nature and

the authors interviewed thirty hospitality professionals, academicians and hotel guests. Among thirty interviewees, three of them were hospitality professors who teach "Hotel IT", seven of them were hotel managers from different size hotels, ten of them were hotel staff (front desk clerks) and ten of them were hotel guests. Each interview took an average of ten minutes (about five minutes with guests and fifteen minutes with staff and managers). The questions that were asked from managers and professors were very similar to the research questions of this paper and the questions that were asked from hotel staff and guests were mostly basic questions about computer, email and website security.

4 Findings and Results

The findings and results of this study after interview with the front desk employees, guests, managers and professors indicate that many hotels use rudimentary tools/software such as antiviruses to prevent data breach and data loss. It was shocking to learn that many medium- to small-size hotels do not have an IT manager or dedicated computer security professional. Even some of those hotels do not have any contract with any IT company for handling cyber security issues. When computer-related problems are faced by these hotels, they call random IT professionals from different companies to fix their computers' problems which can be a big security risk to the hotel as that random IT person can be a potential threat to the hotel computer system and network.

Two of the managers interviewed for this study confessed that they have experienced data breach in last five years and one of them mentioned that the attacker was likely a former employee who had some personal problem with the IT manager, and he wanted to take revenge in this way. Unfortunately, due to sensitivity of the topic, both managers refused to explain the extent of data breach. Furthermore, except a couple of hotel staff members, majority of the hotels' staff mentioned that they have not received any suspicious or unsecure email in which the sender asked them to click on some random link to get their information. Indeed, most of the hotel staff and most of the hotels' guest that were interviewed did not have much knowledge about cyber security. During the interview with one of the guests, the guest mentioned that she had an experience of getting her data breached through a hotel network system. The guest indicated that she was a loyalty-program member of that specific hotel and observed some abnormal transactions in her credit card and later on the data breach of the hotel went viral. One of the other hotels' guest talked about his experience of "Fake Booking". He said that he booked a hotel room online from a known hotel brand and when he went to the hotel, the front desk staff was not able to find his reservation. He then showed his printed reservation confirmation upon which the hotel staff recognized that the website name was misspelled and the website was not the legitimate hotel website. While asking about hotels' Wi-Fi, unfortunately most of the guests mentioned that they use the hotels' Wi-Fi, which is often unsecure and is very vulnerable to security attacks. Hence, the sensitive information entered by guests, such as bank account details or

user name and passwords for different accounts, over the hotels' unsecure Wi-Fi network is susceptible to theft by hackers. The authors suggest the guests to use a virtual private network (VPN) when using hotels' Wi-Fi and entering their personal information on websites they visit during their stay.

During interview with managers and staff, the focus of conversation was on training as managers informed that there is no formal training in place for staff regarding cyber security and data privacy. One of the managers complained about the high turnover rate in hospitality industry and he mentioned that due to this turnover issue, it might not be cost-effective to train the staff about these "marginal" issues. It was shocking to hear that word from a manager who should know best about the loss his hotel may experience due to data breach, and which can be many times more than the cost of training staff regarding data security and privacy. During our discussion with professors, professors pointed out theoretical aspects of cyber security as they did not have practical experience in the area, however, they provided useful suggestions that hoteliers can use to provide better security and privacy. We have covered some of these suggestions in this paper.

Overall, findings have shown that lack of knowledge and carelessness is the most observable issue of the hospitality industry staff (managers and front desk clerks) and majority of guests. Another finding was lack of training for employees and lack of usage of strong tools and techniques to secure hotel computer systems and network. Lack of IT experts in hotels was another finding of this paper which has a direct relationship with vulnerability of hotels for data breaches. Finally, failing to update the hotel software on regular basis, not changing the passwords periodically, and not creating strong passwords were some of the other important findings of this paper that indicated the vulnerability of hotels to security attacks.

5 Conclusion, Implications, and Recommendations

This study aims at emphasizing the importance of cyber security for hospitality industry. The study discusses the tools and techniques that can help prevent cyber attacks in hospitality industry. Findings and results from this study reveal some of the main causes that create security vulnerabilities for the hospitality industry, however, due to sensitivity and confidentiality of the topic, certainly the authors are not able to figure out many other factors during the interviews that may affect information security of hotels.

After reviewing many academic and professional resources, we summarize that there are five major risks and challenges that hotels have faced so far. As noted by Hiller [9], these five challenges are:

1. Identity theft leading to credit card fraud has caused many data breaches and information stealing from hotel's network systems.
2. Silent invasions are cyber-crime attacks that employ powerful tactics such as social engineering (e.g., phishing) and recently advanced persistence threats (APTs) that bypass the defenses that are in place by hotels.

3. Unfortunately majority of the hotels have either no security audit or longer security audit cycles that put the investors and the guests at high risk for security attacks.
4. Physical crimes like terrorism that put the hotels at risk.
5. Loss of competitive advantage and negative outlook that is experienced by hotels after cyber security attacks.

In general, cyber attacks can occur in any of the following three forms:

1. The intruder may obtain unauthorized access to the network.
2. The intruder may destroy, otherwise corrupt or alter the data.
3. The intruder may acquire fake permission for system user and then implement some malicious procedures to fail, hang, or reboot the system.

There are many implications and recommendations available for users in hospitality industry to take advantage of, however, in this paper, we present a few important ones.

Checking a website domain and secure socket layer (SSL) certification of websites plays a significant role in Internet era and users must be very careful in entering their personal and financial information on websites. We suggest a few tips and advices for hotel customers while traveling and especially during the hotel stay. We suggest customers to: (i) not use online banking on public computers and public Wi-Fi, (ii) not access email inbox when traveling and connected to an unsecure Wi-Fi, (iii) prevent computer or smartphone from automatic connection to unknown Wi-Fi networks, (iv) use remote desktop applications instead of saving sensitive information on the laptop or smartphone when traveling, and (v) utilize a VPN network for browsing and entering personal information on websites when connected to an unsecure Wi-Fi network.

Research has shown that hotels which have loyalty programs are more vulnerable to security attacks because attackers know that these hotels have access to more consumer data as compared to those hotels that do not have this program. Thus, the information of guests and customers of hospitality industry who are the member of these loyalty programs is more vulnerable. Managers of those hotels can take a few measures to protect the information and data of loyal customers:

1. Giving the customers information about the possibility of being hacked by cyber attackers and advise/notify them to regularly change their passwords. Further, managers can inform the customers to avoid using the same password for several websites. Also customers can be informed to check and monitor their account activity more often. Managers can also reward customers for being security cautious.
2. Sending the customers an automatic email and notification in case of password change or login to their account so that in case if they have not logged in to their account or change the password, they can immediately be aware of potential abuse and report it.

3. Empowering the system to employ two-factor authentication so that for logging into accounts, in addition to providing user name and passwords, guests would also be required to submit the security code that they will receive on the same email address or phone number that they provided while singing up for the account. Hence, in case of attempted masquerade attacks, a cyber attacker will not be able to access the account if they are not in possession of the email account or the phone (number) that the account was registered with as the attacker will not be able to acquire the passcode sent by the authentication system.

There exist a variety of tools and techniques available to scan the vulnerability of the computer system and network. The hotels can utilize these tools and techniques depending on the affordability to protect data and personal information of guests. Furthermore, it is advised that each hotel should have a contract with an IT company or a dedicated IT manager whom the hotel trusts so that the hotel computer systems and networks are security audited on a regular basis. Additionally, hotels should dictate internal regulations and policies for the hotel's employees regarding cyber security and computer network usage. The hotels should also have a cyber security training program in place for those employees whose job is computer related and are tasked with handling emails and social media. Furthermore, hotels must have a secure and certified website that leverages extended validation or at least domain validation, so that the guests be able to book the rooms or amenities provided by the hotel online without having concern of being hacked or abused. Finally, the hotels should acquire a cyber insurance so that the insurance covers the loss and liabilities in case the hotel experiences a data breach or cyber attack.

References

1. Bilgihan, A., Karadag, E., Cobanoglu, C., Okumus, F.: Research Note: Biometric Technology Applications and Trends in Hotels. FIU Hospitality Review 31(2), 1–18 (2013)
2. Butler, J.: Not Just Heads In Beds – Cybersecurity for Hotel Owners. https://www.hospitalitynet.org/opinion/4073687.html (2016), Last visited on December 26, 2019
3. Clark, C.: The Serious Cyber Security Threat That Could Hurt Hotels. http://www.pcma.org/news/news-landing/2015/04/13/the-serious-cyber-security-threat-that-could-hurt-hotels#.VqhHLGCZaJV (2015), Last visited on February 26, 2016
4. Cobanoglu, C., Demicco, F.J.: To Be Secure or Not to Be: Isn't This the Question? A Critical Look at Hotel's Network Security. International Journal of Hospitality & Tourism Administration 8(1), 43–59 (2007)
5. Collins, G.R., Cobanoglu, C., Bilgihan, A., Berezina, K.: Hospitality Information Technology: Learning How to Use It. Kendall Hunt Publishing (2017)
6. Eubanks, N.: The True Cost Of Cybercrime For Businesses. https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#764083449476 (July 2017), Last visited on December 26, 2019

7. Greenberg, A.: Cybercrime Checks Into Hotels. https://www.forbes.com/2010/02/01/cybersecurity-breaches-trustwave-technology-security-hotels.html#4f1684853c8c (2010), Last visited on December 26, 2019
8. Hahn, D.A., Munir, A., Mohanty, S.P.: Security and Privacy Issues in Contemporary Consumer Electronics. IEEE Consumer Electronics Magazine 8(1), 95–99 (January 2019)
9. Hiller, S.: Top 5 Risks and Security Challenges for Hotels in 2015. https://insights.ehotelier.com/insights/2015/01/22/top-5-risks-and-security-challenges-for-hotels-in-2015/ (January 2015), Last visited on December 26, 2019
10. Kansakar, P., Munir, A., Shabani, N.: A Fog-Assisted Architecture to Support an Evolving Hospitality Industry in Smart Cities. In: Proc. of the 16th International Conference on Frontiers of Information Technology (FIT). IEEE, Islamabad, Pakistan (December 2018)
11. Kansakar, P., Munir, A., Shabani, N.: Technology in Hospitality Industry: Prospects and Challenges. IEEE Consumer Electronics Magazine 8(3), 60–65 (May 2019)
12. Paar, C., Pelzl, J.: Understanding Cryptography. Springer (2010)
13. Rusch, J.J.: Computer and Internet Fraud: A Risk Identification Overview. Elsevier Computer Fraud & Security 2003(6), 6–9 (June 2003)
14. Shabani, N., Munir, A., Hassan, A.: Revolutionizing e-Marketing via Augmented Reality: A Case Study in Tourism and Hospitality Industry. IEEE Potentials 38(1), 43–47 (January 2019)