Potential Risk and Benefit of Smart buildings: Home Automation Using COTS Systems

Ibrahim Muhammad Hassan[1], Suleiman Bashir Abubakar[2], Jamilu Y. Abudullahi[3] Adamu Isah[4]

[1] Senior Lecturer, Department of Computer Science, Hussaini Adamu Federal Polytechnic, Kazaure Jigawa State. Nigeria.
Ibrahimhass003@gmail.com
[2]Lecturer II, Department of Computer Science, Jigawa State Institute of Information Technology, Kazaure Jigawa State. Nigeria.
sbbabura@gmail.com
[3]Lecturer I, Department of Computer Science, Jigawa State Institute of Information Technology, Kazaure Jigawa State. Nigeria.
jyabdullahi@gmail.com
[4]Senior Lecturer, Department of Computer Science, Hussaini Adamu Federal Polytechnic, Kazaure Jigawa State. Nigeria.
Isad77@gmail.com

***Abstract**: To fully exploit the concept of home automation using Commercial Off-The-Shelf (COTS) products, customers look into integrated systems that have been pushed towards a common everything approach, that's one size fits all solution: The COTS product is easy to purchase, install/ deployed and maintain. It is COTS products that perpetuated the idea of one solution to meet all needs. This paper describes home automation in relation to COTS, followed by security concerns through the risk exposure, and also further discussed the risk exposure and management. Lastly, emphasizes legal, ethical, and social issues related to the topic, etc.

Index Terms— Commercial Off-The-Shelf, Home Automation, Risk, likelihood, Conseqiences, Automation, risk

1 Introduction

Over the past decades, system integration in home automation had been geared towards achieving a "common everything approach". The bulk of customers tends to search for one-size fits all solutions, a package that is easy to purchase, configure, install and maintain. The answer to the above problem is home automation Commercial Off-The-Shelf (COTS) products. Example of these products shown in figure 1.1 includes Fanless embedded system Tank-600, 10.1'RISC-based IoT panel PC IOBA-10f. These COTS products preserve the concept of the solution to meet all needs and provision of one-line item purchase that assures customers to meet all the features they want (2). However, COTS describes a system package solution embraced to satisfy the desire of a purchasing organization with no reason to authorize bespoke or custom-made solution either in software or hardware. Also, COTS represent some formal terms of commercial items used in home automation. It comprises different services such as installation services, training services, and cloud services. All these services are obtained from the marketplace, to be purchased and used under license for products(3).

The adopted technology in home automation using COTS system is becoming much easier than ever before, by offering a chance for people to transform their homes in to "Smart Homes". The automation of homes using COTS system is much easier and better than the manual configuration of the system, which is tedious, time-consuming and prone to error. In the marketplace, a lower-power wireless technology can be purchased to provide an avenue for devices to be surface-mounted which also eliminate the need for home re-wiring(4). The idea of home automation through COTS products reduces the installing cost and the known do it yourself. The smart home encompasses more than just hardware installation, but also application software is configured in relation to the physical context of the individual devices including their locations in and around the home. This paper aims to assess the application and understanding risk analysis and management in using home automation system and also to consider the legal, ethical, social, environmental and professional issues related to the topic. This paper is organized as follows, first set the scene by introducing home automation with respect to COTS. Then methodology and related work. Ths is followed by security concern through risk exposure and discussion of risk assessment and management in-home automation. Consideration of legal, ethical, social, environmental issue and conclusion.

(1

.

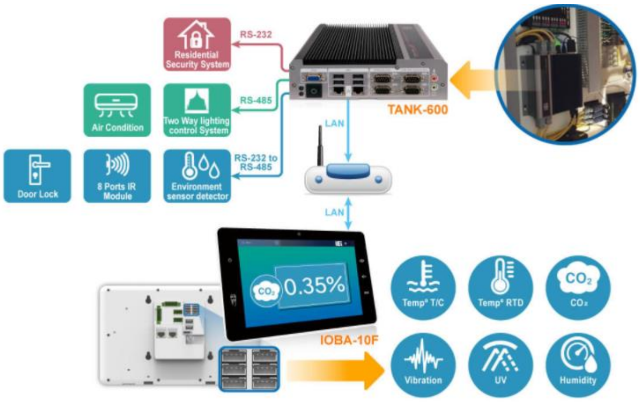


Figure 1. 2: Depicting TANK-400 &

METHODOLOGY

Source of information and search strategy

The following scientific databases IEEE Xplore Digital library, ACM, and Google Scholar were searched using the following keywords "Home automation", "COTS systems" restriction of the year of publication were not imposed. Reference list of retrieved articles was examined for additional literature.

RELATED WORK

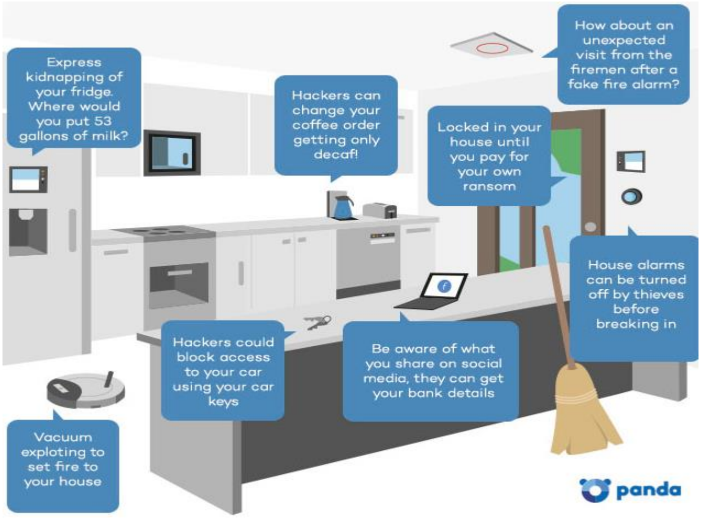
COTS in home automation refers to any software or hardware that are commercially made available either for sale, license, or lease to the public, due to the lower cost, rapid availability, and low risks. However, home automation products that are made available in the market are considered as an alternative to in-house, government-funded developments (5). Home automation makes life simpler, smarter, and easier to manage. Home automation offers audiovisual features that can be controlled by mobile devices; this includes all lighting in each room and heating. The central control has security features that set alarm when intruder access gates, CCTV, doors etc., (6).

COTS software for home automation refers to the software known as "one size fits all" approach guided by the general best practices, below are the reason that derived customers to turn to COTS Solution:

- Convenience: COTS is a ready-made software that have much appeal for home automation of all size fits all as it's readily available. When a customer needs a straight forward solution for the automation should have a new COTS application implemented in matter of an hour or day. A complex system can be deployed so easily and quick
- Predictable cost: Compared to the previous alternatives, COTS products have more predictable cost that have few options of customization at the annual licence implementation typically for the long term cost support such as Update, patches are also handed by the user not always the vendor.

4. SECURITY CONCERN:

4.1 Risk Assessment and Management


Express kidnapping of your fridge. Where would you put 53 gallons of milk?
Hackers can change your coffee order getting only decaf!
Locked in your house until you pay for your own ransom
How about an unexpected visit from the firemen after a fake fire alarm?
House alarms can be turned off by thieves before breaking in
Hackers could block access to your car using your car keys
Be aware of what you share on social media, they can get your bank details
Vacuum exploting to set fire to your house
panda

(7)

Figure 4 1: Shows different risk at smart home that a hacker can exploit.

Home automation is void without adequate security system which can lead to various security risks. Poor security system in homes can expose homeowners vulnerable to serious threats such remote spying, theft, replay attack and unauthorized access etc. as vulnerabilities in figure 4.1. Presently, security research concentrates more on individual devices and the way how they interact with one another, for example, motion sensors and automatic light. in some systems when there is an intrusion in the home stereo or other entertainment appliances will play recorded dog barking which the trigger the light to be on (8).

According to HP 2015 report, ten out of ten home automation tested were found not immune to the risk of unauthorized access. Moreover, the countermeasure uses to minimise the security risk in homes is by using a strong password and never use the DEFAULT Password/PIN because they can be found available on the internet or attached to the products after purchase. Furthermore, proper attention should be a focus on security towards using WIFI, smart hub ZigBee, due to its vulnerability. A strong password can be used to manage that and also by purchasing a current modern router that provides more than one access point to the user, it is important to have a separate access point for home automation to decouple from it from the rest of the network (9). Another measure is that homeowners should not allow any unauthorized person to tamper with the devices e.g. routers, Smart devices, HVAC etc. Tempering can be lead to the system compromise. CCTV is also vulnerable to attack, but it is recommended that only homeowners will have access to camera capture footage. Most of the time data travel to the third party's server. It is important to state that no foolproof method to guarantee security but should make it not easier for the attackers to take our homes. (Hp report, 2015).

In general, smart homes are full of risks, which gives access to the attacker to compromise the systems. Even though the issue of COTS product emerges, companies that produce a commercial product with predefined secure layers could be difficult to bypass. The cyber-security company uses mathematical formulas to protect against advanced security threats in smart home devices. Therefore, it's necessary to reduce the impact of the risks to family, home, and devices via the following points.

- ✓ Turn on your device encryption
- ✓ Make sure your OS is regularly updated
- ✓ Lock your phone with strong password
- ✓ In case of smartphone, no apps should be downloaded unless from secure store

In smart homes, the attacker exploits an application that the user downloads from smart things apps store that allows the homeowner to remotely lock/unlock doors etc. Attacker sends a message from his browser to a home control system or smartphone apps to retrieve pin code or multiple pin code to sustain access to the home system.

Risk ascertain the value of useful information in home automation system such as assets, vulnerabilities, threats that could be in the system the controls in homes determine the potential consequences.

The table 1.1 below describes the building blocks of risk assessment through identification of threat, vulnerabilities, affected assets, consequences, and Controls.

1. 1: Summary of Risk Analysis and Management

Threats	Vulnerability	Assets / Target type	Consequences	Control Measure
Replay attack	The transmission that exists between the remote control /(phone) and connected devices at home and homeowner phone	Smart home devices / PCs, Phones, Network	Traffic interception, Identity Theft	Adopting proper encryption and secure protocol from trusted module platform,
Downloading apps from untrustworthy smart stores our sources	Lack formal procedure for authorization of publicly available information	Smartphones /PCs	Phishing is used to gain access to emails & other home devices/ or social engineering	Activation of firewall, antivirus
Remote spying	Insecure network architecture or sending the password in clear.	All smart home network devices	Home can be compromised easily.	Good network design with adequate security
Theft of home device, other properties or document. (electronic or Physical copy)	Unprotected devices, lack of care at smartphone disposal anywhere, lead to uncontrolled copying	Smart home devices, smartphone, other home appliances, server's CCTV Documents, PCs	Homeowner will get compromised which leads to loss of essential services	Backups, antivirus, and physical security, Antiviruses for eDocument
Tempering software or hardware/ destruction of home device	Uncontrolled applications downloading, lack backup copy or careless use of physical access to the home and rooms.	Devices, smartphone, network etc.	Result in interruption of many services, and become susceptible to attack	Doors, locks, trusted downloads, human security. Smart device to send alert to owner phones
Dependency on outside experts	Inability to address the problem yourself	Home devices, network	Privacy intrusion	Enforce security encryption
Loss of confidence from the company product	Loophole in the in already purchased products	Smart applications/devices	Cracking you network, Hacking your devices	Review the problem with the company i.e. smart things product
Lack of digital privacy, risk for digital violation	Non-digital right control (DRC)	Smartphones, PCs	Service providers	Provide cryptography in DRC to be imposed on smartphones TPM
Breach of	Inadequate		Out of service,	Regular maintenance

information maintainability	maintenance, installation of storage media in smart home		failure of devices	service and proper checks
Denial of Actions	Poor network architecture, lack proof or sending or receiving message	Phones Pcs other smart devices	Attacker disable and corrupt the network, system or the serviced run at smart home	Strong use of a password. Antivirus, antispyware, provide good network architecture.

(10)

4.2 Assesment of incident likelihood

The likelihood refers to the probability of risk potential occurrence which is measured in quantitative values such as High, Medium and Low in-home automation to identify the likelihood of table 1.1 the following has to be considered, the identification of threats, assets, vulnerabilities, and consequences to assets using the following scale:

Low risk	0-2
Medium risk	3-5
High risk	6-8

Table 1. 2: Assesment of incident likelihood

	Likelihood occurrence of threats	Low			Medium			High		
	Ease of exploitation	L	M	H	L	M	H	L	M	H
Assets Values	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9
	6	6	7	8	7	8	9	8	9	10
	7	7	8	9	8	9	10	9	10	11
	8	8	9	10	9	10	11	10	11	12
	9	9	10	11	10	11	12	11	12	13

In the table above when asset value is 5, the threat will become "High" the vulnerability will be "low" and the risk measure will become "7". Also, when assuming the asset value is 2, for the modification, the threat will become "low" then the easy of exploitation will become "High" the risk measure will be "4".

4.3 Level of Risk Determination

In this case incidence with their corresponding consequences are associated with assets and likelihood will either be qualitative or Quantitative but here the scale according to (11) is 0-5.

Table 1. 3: Depicting Level of risk determination

Threat	**Likelihood of Exploitation**	**Ease of Exploitation**	**Asset value**	**Risk Level (Scale)**
Replay attack	Medium	Low	3	5
Tempering software or hardware/ destruction of home device	low	Low	2	3
Downloading apps from untrustworthy smart stores our	Low	Medium	3	3

sources				
Theft of home device, other properties or document. (electronic or Physical copy)	Medium	Low	4	6
Loss of confidence from the company product	Medium	Medium	3	4
Lack of digital privacy, risk for digital violation	High	High	5	7
Breach of information maintainability	Medium	High	3	5
Denial of service	High	High	5	7
Dependency on outside experts	Low	Medium	4	5
Remote spying	Medium	Medium	3	7

Figure 4.2: showing probability and impact key

4.4 Probability and Impact Matrix

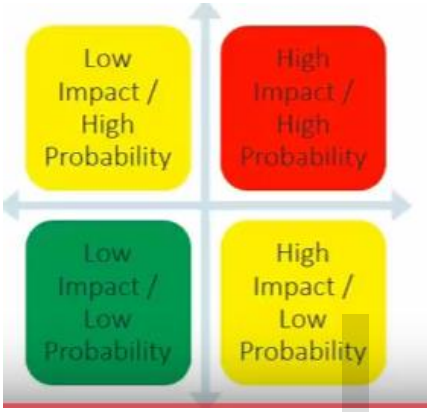

Low Impact / High Probability
High Impact / High Probability
Low Impact / Low Probability
High Impact / Low Probability

Figure 4.3: showing probability and impact key

As shown figure 4.2, the risk is divided into 4 categories; high impact/ high probability is Red this risk would have a serious impact, actions have to take. Similarly, low impact/ low probability even incident happened it will not affect the smart home objectives its label as green. Those are the two extremes. In yellow action might be taken when the need arises.

Below table 1.4 depends on the risk rating on the scale of (5) Very low, Low, Medium, High, and Very High

Table 1. 4: Probability and impact matrix

	Very Low	low	Medium	High	Very High
Very High	Medium	Medium	High	High	High
High	low	Medium	Medium	High	High
Medium	low	Medium	Medium	Medium	High
Low	low	low	Medium	Medium	Medium
Very Low	low	low	low	low	Medium

5. Consideration of Legal, Social Ethical, Environmental, and Professional issues

Legal issues:

Home automation provides unprecedented understanding in a manner that smart homes are used by their occupants. The recent interconnection technologies enable homes to capture detail ong the COTS products smart n sensors, cameras were used to create datasets e.g. individual in or around the home.

Security Camera and Data protection & impact on privacy of others

Data Protection Act (DPA) 1998 support strict standard usage of closed-circuit television (CCTV) that monitors the moment of a stranger around the home by controlling his data, therefore it is difficult to operate with the exclusion of home purpose. Section 36 of DPA states for any stranger information, which includes individual video footage, caught just for the home purpose is not covered by the restriction (12).

The restriction imposed by DPA when installing home Camera. Most of the CCTV cameras captured footage from behind boundary of property it is often unavoidable. Therefore it is vital to consider the following:

- Indicate a symbol that CCTV is in operation here.
- To Keep footage only for a reason which has been taken
- Secure the footage as long as you need it.
- Never released the footage to the third party.

Furthermore, if CCTV is installed to prevent crime you can safeguards the footage so long its need, to enable the owner to detect and prosecute the criminal and sent the information to police or relevant authorities.

Human Right Act 1998

Article 8 of HRA 1998 stated that an individual must have legal right to respect their privacy, families, and homes, therefore, in using the camera to monitor neighbour activates it is clear indication of a breach in their HRA 1998 and can prosecute the homeowner based on that act. (13).

Data Protection Legislation

Presently DPA 1998 will be replaced in May 2018 by the New EU-Wide General Data Protection Regulation (GDPR) and UK Government abides by the regulations to be set up as planned, despite Brexit vote. GDPR has similar concept and principles with DPA 1998 but with the addition of new obligations. Both the two imposed an obligation in collection and usage of personal data of the stranger families to ensure that the footage did not prejudice them based on the collected data (14). In using COTS products, one must acquire a license for the products or can face prosecution when found with counterfeiting the products.

Social issues:

Cyber-criminals such as hacker, crackers exploit the smart home convenience, internet connections to compromise the smart devices such PCs, central control, sensors surveillance camera and homeowners' smartphones to commit a range of criminal activities. For example, an attacker can exploit applications downloaded from different COTS company's products from the store. Which permits the user to control smart home devices remotely from a smartphone, tablet etc. The hacker sent some program from his browser to the application stores to obtained PIN or password of homeowners device that will allow him to gain access to locks, Wi-Fi etc. The hacker will have equal access to the homeowner; then DoS can be imposed to avoid the user from gain access to smart home devices.

The attacker can take advantage of some pre-defined configure cameras to gain access through applications by using the default password. It is then suggested that homeowners should change their default password immediately.

Environmental Issues

Smart homes with smart thermostat enable the homeowner with the power to the carbon footprint in different ways, to control the temperature of the home in and around via smartphone, or remotely. For example, if a homeowner goes on a vacation and quickly remembers that thermostat was not adjusted, it can be done instantly from a mobile phone, or when a door was left open the smart thermostat can automatically turn off air-condition or heating system depending on the situation. However, the device can be set up to regulate heater or air conditioning system when the homeowner is at work, and about to be home the device will activate itself before owner's arrival. The device learned the home temperature preference to make it easier to maximized energy efficiency(15).

According to United States Protection Agency (USPA); This automated thermostat reduces the electricity usage by 10% -30 % (16). If an automated household with four occupants emits 543 kilograms of carbon dioxide per year and compared with an average smart home with the same number of the occupant that emits 473 Kilograms of CO_2. However, the difference is 70kg of CO_2 which precisely is not a small amount in our environment. CO_2 emission caused global warming. (16).

Ethical issues

Smart homes violate two major association for computing machinery (ACM) ethical codes 1.4: to be fair without taking any action to discriminate and 1.7: respect others privacy (Anderson, 2013). Firstly, according to the codes, it is unfair to build a smart home because the technology will not be available to everyone, secondly, the risk involved in the smart home which leads to another violation so, modern technology should follow ethical codes.

Code 1.4 says middle and lower class cannot afford to set up smart building due to the price of COTS products to be procured. However, it is also unfair to older people due to the limited understanding of recent technology as compared to the younger generations when it comes to operations.

CCTV security cameras monitor resident at all time in all rooms, therefore, smart homes violate the ethics code 1.7; respect privacy of others. According to (Hill, 2013), an incident that happened where white hat found identifiable information for a smart homeowner online including physical address and contact, and then gain access to their smart home control. Later the cracker notifies the owner about the porosity of his network but they all denied until their room light was turned off.

Now the fear in home security camera is for the owner to be monitored by the outsider instead, where his personal information will be compromised. This monitoring produces a large amount of data of the resident should be avoided (Asplund, Laberg & thygesen, 2005).

Conclusion

Smart homes are interconnected with devices which may cause undesirable consequences to the homeowner privacy with regards to family, sensitive information and misuse of smartphones. This risk sometimes affects devices like CCTV, personal belongings which are not planned for, which are dynamically attached to smart home automation. The sensitive part of the smart home is concerned information registry such as homeowner's energy consumption, the daily routine of his family, life situation can be taken by criminal activities for example burglary, theft of information as detail shown in table 1.1. Legal, ethical, environmental etc. play major role in home automation and described in 5.0

References

1. Corp. II. Home Automation | IEI 2017 [cited 2017 2nd December 2017]. Available from: https://www.ieiworld.com/smart-building/en/home-automation.php.
2. Gill K, Yang S-H, Yao F, Lu X. A zigbee-based home automation system. IEEE Transactions on consumer Electronics. 2009;55(2):422-30.
3. Stefanczak C. Custom automation vs. commercial-off-the-shelf, or both? | Control Engineering 2013. Available from: https://www.controleng.com/single-article/custom-automation-vs-commercial-off-the-shelf-or-both/4a2dd4b1266652312ccaa5a6b835c6d0.html.
4. Stefanczak CA. Custom automation vs. commercial-off-the-shelf, or both? Control Engineering. 2013;60(9):45-6.
5. Gansler JS, Lucyshyn W. Commercial-off-the-shelf (cots): Doing it right. MARYLAND UNIV COLLEGE PARK CENTER FOR PUBLIC POLICY AND PRIVATE ENTERPRISE, 2008.
6. Saad al-sumaiti A, Ahmed MH, Salama MMA. Smart Home Activities: A Literature Review. Electric Power Components and Systems. 2014;42(3-4):294-305.
7. Is the Internet of Things (IoT) as safe as it should be for our homes? 2016.
8. Velte A. Build your own smart home. 2003.

9. Storm D. Of 10 IoT-connected home security systems tested, 100% are full of security FAIL | Computerworld. 2015.

10. Bibliographic Info :: BSOL British Standards Online. BSI; 30 June 2011.

11. International Organization for S. Information Technology; Security Techniques; Information Security Management Guidelines for Telecommunications Organizations Based on ISO: Technologies de L'ìnformation: Techniques de Sécurité: Lignes Directrices Pour Les Organismes de Télécommunications Sur la Base de L'ISO/CEI 27002: International Organization for Standardization; 2009.

12. @ifacility. Rules and Regulations of Home CCTV installation | iFacility 01749 600600. 2017.

13. ifacility. Rules and Regulations of Home CCTV installation | iFacility 01749 600600: @ifacility; 2017 [updated 2017-03-15]. Available from: https://www.ifacility.co.uk/regulations-home-cctv/.

14. EGi - Legal Article - Smart buildings and data laws: an unfamiliar regulatory landscape 2017. Available from: https://www.egi.co.uk/legal/smart-buildings-and-data-laws-an-unfamiliar-regulatory-landscape/.

15. Chianis A. What is a Smart Home and How Does it Support Green Living? : @safewise; 2013 [updated 2013-08-08]. Available from: https://www.safewise.com/blog/what-is-a-smart-home-and-how-does-it-support-green-living/.

16. Louis J-N, Caló A, Leiviskä K, Pongrácz E. Environmental impacts and benefits of smart home automation: Life cycle assessment of home energy management system. IFAC-PapersOnLine. 2015;48(1):880-5.