SECURITY AND PRIVACY MANAGEMENT TECHNIQUES IN THE IOTS

BELLO, ABDULAZEEZ OMEIZA; AND AMANNAH, CONSTANCE IZUCHUKWU
Ignatius Ajuru University of Education, Rumuolumeni, P.M.B. 5047, Port Harcourt, Nigiria.

Abstract
The Internet of Things is an evolving technology for physical objects. Privacy concerns any individual's right of control. On the other hand, security refers to the way personal data from somebody is safeguarded. Despite the importance of security and privacy management in the IoTs, there are still rising issues confronting the IoTs thus the need to device stronger techniques in addressing these issues. The aim of this paper is to review the security and privacy threats in the IoTs and the prevention techniques. The objectives is to compare the reviewed techniques and recommend a more viable techniques for managing privacy and security in the IoTs. SLR methodology is used to review the techniques based on their ideas, merits, demerits and prospect. Intelligence gathering techniques opined that intelligence should be adopted by companies to boost their security domestically but however there was difficulties in gathering information for big data using the existing mining algorithm. Social-media techniques is capable of using user's twitters account profile to protect user's data but it was only limited to information gathering. Soft-biometric techniques is a strong techniques for measuring objects performance and authentication but the error rate of the techniques is high. BITAG Guideline's security and privacy techniques employed high level policies/guidelines in checkmating security and privacy issues but however detailed list of the guidelines are not specified and threats are left untouched. The authors thus recommended that fuzzy-based security and privacy techniques and new hybrid algorithm techniques should be hybridized for a viable security and privacy in the IoTs.

Keywords: Internet of Things (IoTs), Security, Privacy, Intelligence gathering.

Introduction

The Internet of Things (IoTs) is a type technology that allow users to relate with various physical objects connected to it. Through IoTs, objects can acknowledge each other and gain intelligence experience in making effective decision based on their ability to communicate information about themselves. (Chibroma, 2017). Despite its common usage, the word "Internet of Things" remains vague since it refers to a broad range of technologies such as Radio-Frequency Identification and Wireless Sensor Networks (WSN). As demonstrated by IoT applications such as smart homes, smart phones and smart roads, the Internet of Things' role in our daily lives is rapidly growing and developing. Infinite services and solutions are becoming more prevalent as a result of this breakthrough known as IoTs. However, offering such solutions in a consistent and safe manner is difficult, since IoTs systems inherit much of the

current Internet's problems and, most likely, exacerbate them as a result of direct contact with physical items.

The objects have access to data composed by other objects connected to it and they can as well be incorporated to nearby objects. The Internet of Things (IoTs) is the interconnection of physical objects such as cars, home appliances, and other products such as sensors and software that are linked to it. The IoTs is based on the concept of efficiently managing vast volumes of data from physical objects over the internet.

The concepts of security and privacy are inextricably linked. The right of an individual to control his or her own life is referred to as "privacy." Security, on the other hand, refers to protection from unauthorized data access. In order to limit who can access the information, we put security controls in place. Privacy is also important as: privacy gives us the power to select and share our thoughts and feelings. Privacy safeguards our information, which is not publicly shared (Chen et al, 2019).

Statement of the Problem

Due to so many heterogeneous objects connected to IoTs and the amount of big data linked to it, security becomes a serious threats to IoTs. These objects and nodes are very prone to intrusion and attacks because adequate measures are not put in place to protect and safeguard them. The moment any of the layers is breached, a hacker can easily take control of a device and use it for a malicious purpose and can as well attack any linked devices. Most of the applications in the IoTs are not well secured, they lacked malware and virus protection thus they are easily prone to online attacks thus the need for a viable privacy and security techniques to protect the IoTs.

Aim and Objectives

The aim of this paper is to review privacy and security management techniques in the IoTs. This paper intends to:

i) review current security techniques in the IoTs
ii) review current privacy techniques in the IoTs
iii) compared the reviewed security techniques in the IoTs
iv) compared the reviewed privacy techniques in the IoTs
v) recommend the effective and more viable security and privacy techniques in the IoTs.

Related Literature

The general idea about Internet of Things (IoTs) is to effectively manage big data of physical objects on the internet. The Internet of Things (IoT) is a cutting-edge method of connecting to the Internet. Objects in the Internet of Things identify themselves and acquire information by taking relevant decision based on the information on their domain. Application areas for IoTs encompass smart health, smart homes, smart environment, etc. (Adeshina, 2016)

Intelligence gathering is the collection of data for knowledge gain of others. These information could be gathered by government intelligence agencies, military intelligence department or commercial intelligence organization. This is a process which is utilized for analyzing the processes of information data of private and public firms, and its relevance in the blocking of fraud, crime and breeching of

information that is legally democratic. The word intelligence can be defined as information that is scrutinized and processed in order for the benefit of individuals who enact decisions. Yet, intelligence is also utilized by companies for boosting their security domestically. However, due to the current growth of technology, it is very difficult for software developers and data analyst to gather information of Big Data using the existing data mining algorithms such as K-means, K-Nearest Neighbor, Apriori, Page-rank and AdaBoost. This is as a result of poor query plans and non-user-friendly interfaces that are supported by these existing data mining algorithms (Donkur, 2018)

The Broadband Internet Technical Advisory Group (BITAG) (2016) presented a high-level collection of Internet of Things privacy and security guidelines for data, object and communication. BITAG, on the other hand, does not include a detailed list of procedures nor does it define the countermeasures needed to enforce those procedures In addition, IoTs-related attacks and threats are unaffected.

Quercia et al. (2011) proposed a report on our Twitter accounts, ourselves: using Twitter to predict personality. They demonstrated a method for reliably predicting a user's personality based on three publicly available profiles counts (such as followers, following and listed counts). They showed that by using these three variables about an active twitter user, they could accurately predict the personality traits of five users. They used data from myPersonality, a Facebook application, to correlate personality scores with users of Twitter. They were able to predict the user's five personality traits on a scale using the dataset. This model, on the other hand, was solely based on intelligence.

Tome et.al. (2014) proposed Soft biometrics and application in person recognition at a distance. The authors Performance metrics such as false rejection rate, false acceptance rate, error rate and authentication rate has been checked. Because of preprocessing lack, the error rate is more. The improvement in accuracy should be there for less number of errors with the utilization of accurate methods of pre-processing.

Fuzzy-based Security and Privacy System for P2P Overlays, which uses JXTA Protocol for Nodes Communications, was presented by Kouhei et al. (2011). For the evaluation of peer reliability, the authors used fuzzy logic with two parameters: Reputation and Actual Behavior Criterion. Other past papers in their study were also used to identify the most trustworthy peer. However, they were unable to use this strategy to create a protection solution for P2P grids.

According to Dubbois (2014), young people take more precautions in protecting privacy than older people and the current paradox is focused on the idea that "social life is more of online connections and social networking sites do not provide users with the resources that would effectively allow them to maintain their privacy in a manner that is suitable for them." According to a recent Pew Research Center study (Rainie et al. 2013), 86% of internet users have employed tactics of removing or hiding their footprints online. Clearing cookies, email encryption, real name encapsulation and virtual private network to conceal IP addresses were among the methods used.

Pooranian et al. (2011) suggested a new hybrid algorithm for scheduling of task in grid computing to minimize missing tasks. Their focus is based on resource discovery models in computational grids that value the make period of independent workloads in heterogeneous VOs which employed privacy models and security techniques by combining hybrid computing techniques such as genetic algorithm and Particle Swarm Optimization. They did not, however, consider network privacy confidence and only regarded make span.

Data Security in intelligence gathering components involves people, process and technology. Data security is assumed to be technological when there is an application of sophisticated security hardware, firewall, encryption methodology, software and regular penetration test. These technological advances in data security can also be boosted with regulatory requirements, security certification process, standards, policies and checklists (Etorobong, 2014).

Issues of data security among humans is very subjective, and should be taken seriously. There is an abysmal practice and demonstration of data security among humans today, and it is very appalling. Most at times, humans are the sole contributors of data leakages especially on email platform. Zakaria et al (2013) in his research once described humans as the weakest link in the security chain. Humans need to change their behaviors on data security in order to protect information assets. For successful data leakage prevention and detection, there is need for a proper orientation on the concept of data leakage, its causes and prevention.

Research Methodology

A systematic literature Review (SLR) was used to carry out a critical analysis, evaluation and provide accurate result in reviewing security and privacy management techniques in the IoTs. The SLR will help to detect, review and harmonize all the subject-related research.

The article selection process for evaluation of these techniques is carried out in three phases, namely;

i) keywords-based Search, titles, summary, reference analysis and quality of publication. Google search engine is used to find most of the relevant materials found in books, thesis, journals and conference papers.
ii) in phase two, some criteria are used to ensure strong quality articles and publications.
iii) in phase three, we ensured all the selected text for review are all related to security and privacy management techniques in IoTs.

Discussion

There is a rapid increase in the number of objects connected to the IoTs daily and these objects are posing more security threats to the IoTs. Attacks on these objects can be severe, some of the objects can be abused and even attacked and thus there is a need to ensure a protected connection among the various computing nodes and gadgets in order to have a secured authentication of its members. Privacy and Security management techniques play an important roles in establishing strong and viable connections among IoTs layers, nodes, devices, applications and other infrastructures.

There are many techniques for managing security and privacy in the IoTs but the study reviewed and organized some of these techniques in a systematic manner based on their viability. The merit and demerit of the reviewed security and trust management techniques are summarized below.

Table 1: Summary of the Merits and Demerits of the Security and Privacy Management Techniques

Authors	**Security and Privacy Techniques**	**Merits**	**Demerits**
Donkur (2018)	Security and privacy management via intelligence gathering	The authors' ideology was to opine that the word intelligence can be defined as information that is scrutinized and processed in order for the benefit of	However, due to the current growth of technology, it is very difficult for software developers and data analyst to gather information of Big Data

		individuals who enact decisions. Yet, intelligence is also utilized by companies for boosting their security domestically.	using the existing data mining algorithms such as support vector machine, K-Nearest Neighbor (KNN), Apriori, AdaBoost, Page-rank.
Quercia et al (2011)	Twitter account, user's details and personality prediction.	The authors used three counts publicly available on user's profile (including following, followers, and listed counts) to present a way for predicting twitter user's personality effectively and accurately. The authors demonstrated that by using the above three user's counts to accurately predict user's personality trait.	However this model was built only on intelligence gathering
Tome et.al. (2014)	Soft biometrics and application in person recognition at a distance	For performance measures such as verification rate, False rejection rate, false acceptance rate and error rate checked.	Because of preprocessing lack, increase in error rate. The improvement in accuracy should be there for less number of errors with the utilization of accurate methods of pre-processing
Kouhei et al (2011)	Utilized privacy and security p2p overlays using fuzzy techniques. The nodes communication is by JXTA protocols	The authors employed Fuzzy techniques using two metrics such as real behavioral criterion and reputation criterion for evaluation of peer reliability. Experiences forms other past papers in their survey were also used to detect the most reliable peer.	However the authors could not develop a security solution in P2P grids using this technique.
BITAG (2016)	A high-level security & privacy model	The authors proposed an advanced privacy and security templates/guidelines for the data, object and communication.	However, a complete list of the templates/guidelines is not outlined by BITAG nor a countermeasures is specified for the templates implementation. Also, threats were not properly touched.
Dubois (2014)	Clearing cookies, email encryption ,	The authors argue that young people take more precautions in	This technique is not robust and very limited

	real name encapsulation and private networks to conceal IP address techniques	protecting privacy than older people and the current paradox is focused on the idea that "social life is more of online connections and social networking sites do not provide users with the resources that would effectively allow them to maintain their privacy in a manner that is suitable for them	
Pooranian et al. (2011)	The authors suggested a new hybrid algorithm for scheduling of task in grid computing to minimize missing tasks	The authors focus is based on resource discovery models in computational grids that value the make period of independent workloads in heterogeneous VOs which employed privacy models and security techniques by combining hybrid computing techniques such as genetic algorithm and Particle Swarm Optimization	The authors did not, however, consider network privacy confidence and only regarded make span.

Table 2: Summary of the Prospects of the Security and Privacy Management Techniques

Authors	**Security and Privacy Techniques**	**Prospects**
Donkur (2018)	Security and privacy management via intelligence gathering	If implemented with more advanced algorithms, the technique will be a major privacy and security solution in the future.
Quercia et al (2011)	Twitter account, user's details and personality prediction.	With an increasing number of counts for predictions, there is a chance of better accuracy in future.
Tome et.al. (2014)	Soft biometrics and application in person recognition at a distance	With a rapid growth of biometric technologies, a more sophisticated biometric devices will reduce error rate of this technique for enhanced security and privacy
Kouhei et al (2011)	Utilized privacy and security p2p overlays using fuzzy techniques. The nodes communication is by JXTA protocols	There is great future in this technique if more research is carried out on it and combination with other strong techniques will help in solving most privacy and security problems.
BITAG (2016)	A high-level security & privacy model	The technique will be a great pre-security and privacy measures in the future if further research

		is done to outline the security guidelines list and countermeasures
Dubois (2014)	Clearing cookies, email encryption , real name encapsulation and private networks to conceal IP address techniques	The technique has a great potential for social-media solutions if properly implemented.
Pooranian et al. (2011)	The authors suggested a new hybrid algorithm for scheduling of task in grid computing to minimize missing tasks	The techniques has a great prospect in solving most security issues especially if hybridized with a technique that has stronger network privacy interface.

Conclusion

The study shows that as the number of nodes and objects connected to the IoTs increases so too the more danger and threats it poses to the IoTs domain. The study reviewed using the SLR several literature related to privacy and security management techniques in the IoTs and the techniques reported in fvour of their concepts, merits, demerits, and prospects in addressing security and privacy issues in IoTs. In general, all the techniques contributed in one way or the other for the management of security and privacy in the IoTs but to strike a balance between efficiency and performance, the study recommended that fuzzy-based security and privacy techniques and new hybrid algorithm techniques should be hybridized for a viable security and privacy in the IoTs.

References

Adeshina, D. (2016). IoT & Machine Learning Algorithms: A Review. *International Journal of Computer Science & Information Technologies*, 7(3), 1174 – 1179, Article e3445677717. ResearchGate. https://www.researchgate.net/figure/Machine-Learning-algorithms-in-Internet-of-Things-IoT-smart-transportation-applications_tbl1_332333099

Biodun, O. (2014). Alexandra's Theory on Security and Privacy Management. *International Journal of Computer Applications (IJCA)*, 5(6), 20 – 27.

BITAG (2016). Internet of Things (IoT) Security and Privacy Recommendations. https://www.bitag.org/report-internet-of-things-security-privacy-recommendations.php

Chen, A., Jangun O., & David, F. (2019). Principles of trust for embedded systems, Software Engineering Institute. http://www.sci.cmu.edu.

Chibroma, B. (2017). A Large-Scale IoT-based Study on Source Code reviewer Recommendation. https://arxiv.org/pdf/1806.07619.pdf

Donkur, A. (2018). Proposed Embedded Security framework Internet of things (iot), Vehicular technology, information theory & aerospace & electric systems technology using intelligence gathering. 2nd IEEE International conference, 2018, India.

Dobbins, D. L. (2015). Analysis of Security Concerns and Privacy Risks of Children's Smart Toys." PhD diss., Washington University St. Louis, St. Louis, MO. [Google Scholar]

Etorobong, M. (2014). IoT-based Security for Reliability & Maintainability, 2014 ACM/IEEE, International Conference on Technical Debt. https://doi.org/10.1145/3194164.3194814

Ibikunle, G. (2014). Historical Survey of Modern Embedded Systems. *ACM Journal of Computing*, 7(10), 21 – 27.

Kouhei, U., Spaho, E., Ogata, Y., Barolli, L., Xhafa, F. & Iwashige, J. (2011). A Fuzzy-based Trustworthiness System for JXTA-Overlay P2P Platform. *Intelligent Networking and Collaborative Systems* (INCoS'11), 944 – 949. https://www.researchgate.net/publication/220783193_A_fuzzybased_trustworthiness_system_for_JXTA-Overlay_P2P_platform

Viega, J., & Mcgraw A. (2017). Design & Implementation of a Principled

Embedded System. *International Journal of Computer application (IJCA)*, *16*(7), 1– 10.

Mendez, D., Papapanagiotou, I., & Yang, B. (2017). Internet of Things: Survey on Security and Privacy. Arxiv. https://arxiv.org/abs/1707.01879

Rainie, L., Sara, K., Ruogu, K., Mary, M., Maeve, D., Stephanie, B., & Laura, D. (2013). Anonymity, Privacy, and Security Online. Pew Research Center. https://www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online/

Quercia, D., Kosinski, V., X Stillwell, V. and X Crowcroft, V. (2011). Our Twitter Profiles, Our Selves:Predicting Personality With Twitter. In *Social-Com/PASSAT*, 180–185.