International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.03, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

SECURITY AND PRIVACY OF INTERNET APPLICATIONS: A DETERMINING FACTOR FOR USER LEVEL OF TRUST

Abubakar Mohammed[1], Suleiman Audu Abdullahi[2], Sani Alkali Umar[3]

[1]*Department of Information Technology, MAUTECH Yola, Nigeria*
[2]*Department of Information Technology, NIET NIMS University Rajasthan, Jaipur India*
[3]*Department of Computer Science, NIMS University Rajasthan, Jaipur India*

ABSTRACT

Today technology has brought so many changes across the globe that affects lives of human being. Among these changes include the internet applications which aides many activities ranging from commercial and other humanitarian services. Users always carrying their activities on internet platforms through their smart devices. Security and privacy of internet applications have make it possible for users to bear trusts on these applications. This paper explores the security and privacy mechanisms of internet applications that determine the user level of trust. It makes use of UML modelling technique by providing architectural model depicting the security and privacy tools of internet applications interactivity.

Keywords: Internet, Internet Applications, Security, Privacy, IoT

I. INTRODUCTION

Technology has brought so many changes in human endeavours, it brings ease of activities to society that affects almost all disciplines. With the rapid development of Internet and communications technologies, lives are gradually becoming an imaginary space of virtual world. People can chat, work, shop, keeps pets and plants in the virtual world provided by the network. However, human beings live in a real world, human activities cannot be fully implemented through the services in the imaginary space. It is the limitation of imaginary space that restricts the development of Internet to provide better services. To remove these constraints, a new technology is required to integrate imaginary space and real-world on a same platform which is called as Internet of Things (IoTs).

Based on a large number of low-cost sensors and wireless communication, the sensor network technology puts forward new demands to the Internet technology. It will bring huge changes to the future society, change our way of life and business models. IoTs allow people and things to be connected anytime and anyplace with

anything and anyone using any path or network and any service [1]. They are Material objects connected to material objects in the Internet.

Internet applications are usually programs that runs over the internet using HTTP or HTTPS. They are often run inside a web browser. Some part of the applications also may be client-based, where a small part of the program is downloaded and install in client desktop or device, but processing is done over the internet on an external server. Today there are several internet applications running on different platforms ranges from financial transactions, recruitment and placements, weather forecasting and many more.

Security and privacy are sometimes linked together and served as components of emerging technologies. Apart from benefits of internet and other web applications, security and privacy issues concerned most of the users of these applications. This in-turn determine the user level of trust on these applications.

Therefore, this research aimed at exploring security and privacy mechanisms of internet applications that determine the user level of trust. This can be achieved by the following objectives:

i. To provide security and privacy measures used in internet applications.
ii. To provide architectural model for internet applications interactivity.

II. LITERATURE REVIEW

I. Internet and Internet of Things

The Internet of Things (IoT) has form a dynamic global network infrastructure with self configuration capabilities that is based on standard and interoperable communication protocols. It represents the interconnection of numerous things consisting of smart devices and services. Currently, more than billion devices are connected to Internet which include PCs, embedded sensors, and mobile phones. This present Internet of smart devices is moving towards the Internet of Things, and is expected to comprise 16 billion interconnected devices by the year 2020 [2].

IoT Properties In contrast to traditional Information Technology (IT) systems such as enterprise applications, cloud computing, and big data with combination of a number of properties makes the IoT unique in terms of the challenges that need to be coped with. These properties were identified and analysed by several researchers. The identified distinguishing properties are four consisting of uncontrolled environment, the heterogeneity, the need for scalability, as well as the constrained resources utilized in the IoT [2]. These are discussed below:

a) Uncontrolled environment: Many things will be part of a highly uncontrolled environment; certain things travel to untrustworthy surroundings possibly without supervision. Sub-properties of the uncontrolled environment include mobility, physical accessibility, and the lack of trust.
Mobility deals with stable network connectivity; however constant presence cannot be expected in such an environment. Physical accessibility: In the IoT, sensors can be publicly accessible, e.g., traffic control cameras, and environmental sensors. Trust: A priori trusted relationships are unlikely for the

large number of devices interacting with each other and users. Thus, automated mechanisms to measure and manage trust of things, services, and users are crucial for the IoT.

b) Heterogeneity: IoT is expected to be a highly heterogeneous ecosystem as it will have to integrate a multitude of things from various manufacturers. Therefore, version compatibility, and interoperability have to be considered.

c) Scalability: The vast number of interconnected things in the IoT demands highly scalable protocols. This also has an influence on security mechanisms. For instance, centralized approaches with hierarchical Public Key Infrastructures (PKIs), as well as some distributed approaches with pairwise symmetric key exchange schemes cannot scale with the IoT.

d) Constrained resources: Things in the IoT will have constraints that need to be considered for security mechanisms. This may include energy limitations such as battery powered devices as well as low computation power like micro sensors. Thus, heavy computational cryptographic algorithms cannot be applied to all things.

II. User's Satisfaction, Trust and Perceived Quality

Customer satisfaction plays an important role in any organization's success. It becomes more important especially when customer's gaining alone does not associate to long term success [3]. Customer satisfaction is the main objective for strategic marketing planning since it fetches about many favorable outcomes to businesses. Today a lot of businesses are run on the platform of internet applications. If users are not having confidence on the security and privacy of their transactions details, they become unsatisfied with such platforms and that lead the business to lose.

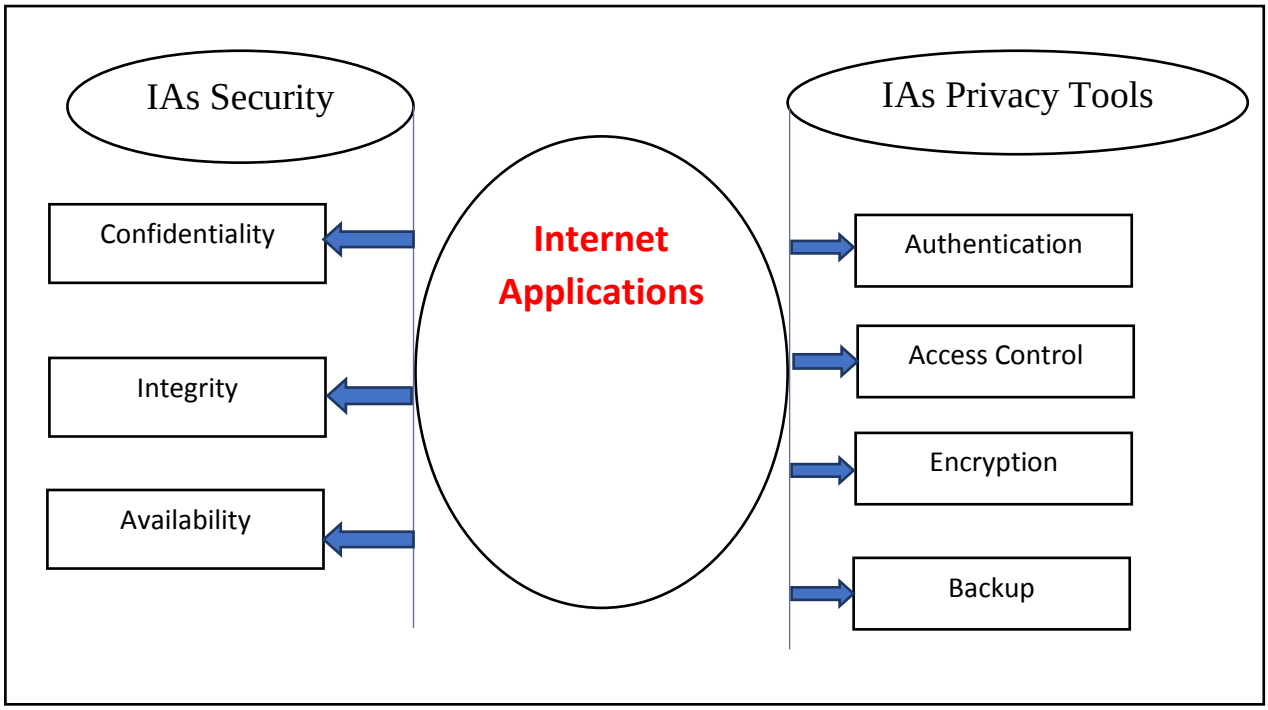
Trust is another issue to be considered, it deals with customer's belief that the online sellers are possible to behave kindly, capably, and ethically. Therefore, customers are possible to be indeterminate of internet applications if they do not feel certainty with web and internet applications they usually visit [4]. Customers are unlikely to transact over the website which lacks privacy or trust, because of fear of seller cunning. Moreover, customer's trust plays a primary role in keeping long-term relationships between customers and online or internet application operators [5].

Service quality is one of the key issues in internet applications. It simply determines how well a conveyed service level will match the user's expectations of the service quality. The extents of service quality in internet applications are sometimes been compromised especially on the area of e-commerce due to ease of use, website design, and assurance. Lately, service quality in e-commerce has meaningfully become the major drive to enhance customer satisfaction and has strong influence on building up loyal customers. If the websites are hard to use, customers will disregard that site and leave the page [6].

III. METHODOLOGY

The paper provides architectural model for internet applications interactivity using unified modelling language (UML) technique. It is designed using Microsoft Visio. The model is presented using figures as the outcome of the research.

IV. ARCHITECTURAL MODEL AND DISCUSSION



The above model provides architectural design of security and privacy of internet applications interactivity. The architecture is divided into two parts known as internet applications security (IAs Security) and internet applications privacy tools (IAs Privacy Tools). The IAs security provide the goals of achieving security within any internet applications, while the IAs privacy tools provide means of protecting data or achieving privacy within internet applications. The individual components are discussed below:

i. ***Confidentiality****:* often there is some private information that you want to keep secret from the attacker. Maybe it is a password, bank transaction details or any vital information that you don't want anyone else to be able to read. It could be anything. Sometimes it may be preventing adversaries from learning system secrets or policies.

ii. ***Integrity****:* If the system stores some information, you might want to prevent the attacker from tampering with or modifying that information.

iii. ***Availability****:* If the system performs some function, it should be operational when you need it. Consequently, you may need to prevent the attackers from taking the system out of service at an inconvenient time.

iv. **Authentication**: Is the identification of user's identity. It verifies that the individual is the person he or she claims to be. Methods of identification and authentication include usernames and passwords or biometric.

v. **Access control**: Is a security measure that defines who can access a system, when they can access it, and what actions they can take while accessing the system. In addition, the system should maintain an audit trail that records in a file both successful and unsuccessful access attempts. An unsuccessful access attempt could result from a user mistyping his or her password, or it could result from a hacker trying thousands of passwords. Organizations should investigate unsuccessful access attempts immediately to ensure they are not intentional breaches of security.

vi. **Encryption**: Is a process of converting readable data into unreadable characters to prevent unauthorized access (i.e. is the process of encoding or shielding of information or data to be revealed only by authorized users). You treat encrypted data just like any other data. That is, you can store it or send it in an e-mail message. To read the data, the recipient must decrypt, or decipher, it into a readable form and must have the knowledge of decrypting it.

vii. **Backup:** Is a duplicate of a file, program, or disk that can be used if the original is lost, damaged, or destroyed. Thus, to back up a file means to make a copy of it. In the case of system failure or the discovery of corrupted files, you restore the files by copying the backed-up files to their original location on the computer.

V. CONCLUSION

People are the actors that interacts with internet applications. Therefore, security and privacy of these internet applications should be the first thing to be considered. This will increase the level of users' trust on the applications. This paper provides architectural model that presents security goals of internet application users as well as tools to be used in maintaining privacy of the information and data sharing within the applications.

REFERENCES

[1] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context Aware Computing for The Internet of Things: A Survey" IEEE Communications Surveys & Tutorials, 2013, pp. 1-41

[2] E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier, and P. Kikiras. On the Security and Privacy of Internet of Things Architectures and Systems. Retrieved from https://www.tk.informatik.tu-darmstadt.de/fileadmin/user_upload/Group_TK/filesDownload/Published_Papers/SIoTpaper.pdf on 2nd April 2018.

[3] J. Flint, C. Blocker, and P. Boutin, "Customer value anticipation, customer satisfaction, and loyalty: An empirical examination," Industrial Marketing Management, vol. 40, pp. 219-230, 2011.

[4] Collier, J. E., and Bienstock, C. C. (2006). Measuring service quality in e-retailing, Journal of service research, 8 (3), 260-275

[5] Chiu, C. M., Cheng, H. L., and Fang, Y. H. (2009). Determinants of customer repurchase intention in online shopping, Journal of Marketing, 33 (4), 761-784 [

[6] Pearson, J.M., Pearson, A. and Green, D. (2007). Determining the importance of key criteria in web usability, Management Research News, 30(11), 28-816