6. Data Confidentiality: This is a very important feature to be taken seriously in E-Service security as there is a need to make sure that unauthorized people to have access to data [11].
7. User Anonymity: In this feature, information that will lead to the identification of the user should not be disclosed [11].

6. Findings And Analysis

In this section, the researchers of this paper present findings and analysis based on the content analysis of the reviewed literature together with results from the on-going online survey. The early research findings were based on reviewing related research works on E-Service and Security in developing countries [1]; [8]; [11]; [12]; [14]; [17]; [18] and [19].

One interesting finding is that the participants in the on-going survey are much aware of the security issues in E-Government services and with these lapses, some are reluctantly declining to do online transactions for the fair of identity theft/fraud. Their claims were further substantiated in the paper by [1] who raised the security issues associated with E-payments in Nigeria that have made the adoption of E-Service to be very low while the high level of corruption in the country have also contributed the low implementation of E-Government projects in Nigeria [1].

6.1. E-Service Security: Taking Proactive Measures

Using computers and E-Services afford us the opportunities to be connected to the modern world, doing online shopping, and connection to friends and family through social networking, emails are made possible with efforts of these services [9]. Most times, users have carried away with robust services they benefits from using the internet and security is being overlooked [9].

Unsafe user's practices could be exploited by the attackers and your computers could be infected with malware and other malicious software. When this happens, attackers could access your computers without your knowledge to carry out various crimes such as identity theft and using your personal data for dubious actions [9].

There are many other options available in taking proactive measures together with E-Service security preventive tools apart from Intrusion Detection System (IDS) as discussed by [17]. This approach uses the autonomous agents and it offers fault tolerance. Agent is free to have an own model of behaviour and when the deviation is detected from the expected behaviour, or any violation of a specification, other agents will be notified [17]. This approach has an edge over many others even in any compromised case involving one agent, the others agents could still continue to function [17].

Other proactive measures are therefore analysed below through the use of security prevention/detection tools, namely:

1. The use of Secured Software: The Enterprise Technology Challenge organised by the Co-Creation Hub, and sponsored by Oracle, was designed to mobilize Nigerian software developers and designers to build innovative, locally appealing and relevant web and mobile apps that enable & support small & growing businesses in Nigeria. Participants during the event had the opportunity to learn how to reduce risk and complexity in their businesses by using the most comprehensive, secure Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) cloud offerings on the market.

2. Intrusion Detection System (IDS): The IDS according to [17] make use of a hybrid approach constructed using a pattern machine engine together with a neutral functioning which aims at improving the detection efficiency. Intrusion Detection System (IDS) approach connects the information from the network level and monitoring data from the grid system in order to identify the attacks which were unable to be detected at the local level [17]. Intrusion Detection System (IDS) is an important and useful tool in detecting "denial of service (DoS) or distributed denial of service (DDoS) attacks", their performances will be reduced [17]. Snort is the most popular Intrusion Detection System (IDS) according to [18] and it has the capability to detect every attack experienced by the system administrators.

3. New Authentication Mechanism: As earlier mentioned in E-Service security requirements, there is a need to have more trustworthy "emerging mechanism" such as biometric authentication to check identity or other fraud associated with E-Services [11].

4. Automated Transaction Risk Scoring: This approach according to [19] uses specific logic and setting which can help to identify false transactions from the normal ones. Multiple data factors are used in this approach to calculate the fraud risk and a numerical score is assigned to each transaction made [19].

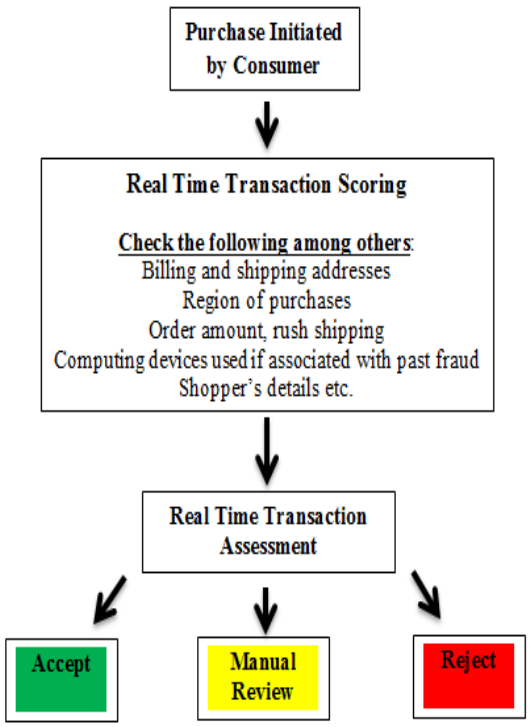

Figure 1. Automated Transaction Risk Scoring System (Ward, 2010)

5. Enhanced Hardware: Apart from the use of cryptographic keys and other secret information as recommended by [11], the use of enhanced hardware such as co-processor will be beneficial in order to maintain the required security for E-Service.

6. Encryption: To have a secured E-Service system, the use of encryption is encouraged. The data can be translated into secret code and for a user to read the secret codes, they must have access to the password or secret key in order to decrypt the data [11]. This is most efficient and effective way to have data being secured [11].

7. Secured Network Usage: It is user's responsibility to make sure that he or she connect to a secured network while mindful that once a computer is connected to the internet, many other computers are connected at the same time connected too which means the chances for the attacker to attack your computer is very high. It is very important for a user to secure router as modem does not have security settings [9].

8. Installation of Antivirus and Antispyware Software: Using updated antivirus and antispyware software could help to detect malware in the computer system and it is very helpful if we keep updating the software, though, many of the software do update automatically [9].

9. Unnecessary Software Removal: It is important for a user not to use any software installed on the system if the user has no idea about it. Attackers always exploit software vulnerabilities and removing unknown software from the system will protect the system from a possible attack [9].

10. Default Features Modification: Unnecessary default features modification helps to protect systems from a possible attack, it is very crucial to review all the features that came with the system enabled by default by disabling those you do not intend to use [9].

7.Statistical Analysis On Internet Security And Trust As A Major Barrier Facing E-Service Technology In Developing Countries

Following the literature review of related papers in E-Service security, the on-going survey for the purpose of this study revealed that participants in the on-going survey are much aware of the security issues in E-Government services and with these lapses, some are reluctantly declining to do online transactions for the fair of identity theft. Below are the results from the survey which is available at (https://www.surveymonkey.com/r/29HHMKQ).

1. Opinions on Solutions to Improved E-Service Adoption: Keywords presented by wordle below in Fig. 2 on the participant's opinions for the improved E-Service adoption in developing countries from the survey shows that over 50% indicated that adequate internet security should be provided if the E-Service adoption rate must improve. E-Service security according to [11] and as earlier discussed involve the determination of ensuring a secured e-service transaction over the internet while both data integrity and confidentiality maintained.

Figure 2. Opinions on Solutions to E-Service Improved Adoption

2. Adoption and the Use of E-Service: The survey results further indicated that over 90% of the participants were interested in using and adopting E-Service such as E-Payment in developing countries. A typical example is Nigeria when the Central Bank of Nigeria (CBN) introduced the cashless economy policies in 1912 where the manual banking systems in the country migrated to automation [1]. Though, few customers still engage in manual transactions few attract further charges as a means to encourage automated services and the policy has been so far successful [1].

The most obvious finding to emerge from the analysis is that less than 10% participants claimed they will not be using or adopting E-Service and it is interesting to know that the major reason behind their decisions is issues of Internet security and Trust as presented by wordle in Figure 4 below.

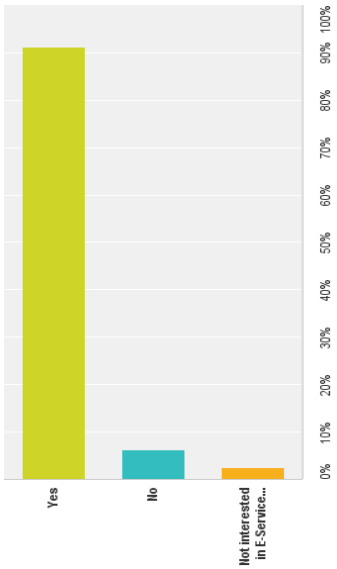

Figure 3. Adoption and the use of E-Services

3. Internet Security Issues: This has been a major barrier to the use and adoption of the E-Service. The survey results as displayed in Fig. 3 above indicated that almost 10% participants that will not be using or adopting E-Service in developing countries based their submission on the issues of Internet Security and Trust as presented by wordle in Figure 4 below.

Figure 4. Internet Security Issues

The security issues associated with E-payments in the country have made the adoption of E-Service to be very low [12] while the high corruption in the country has contributed the low implementation of E-Government projects in Nigeria [1]. There is no doubt that using or adopting a new system and technology might come with some challenges. In the case of developing countries, the fact that a technology which has been effectively adopted by a particular country or culture does not necessarily means it will work the same way in another culture, even though they may look similar but there is a need to step up with laudable and achievable solutions to help fight the E-Service security issues in developing countries as E-Government services are helping to boost government revenue, very fast and secured transactions, reduce corruption through the use of modern technology and transparent operations.

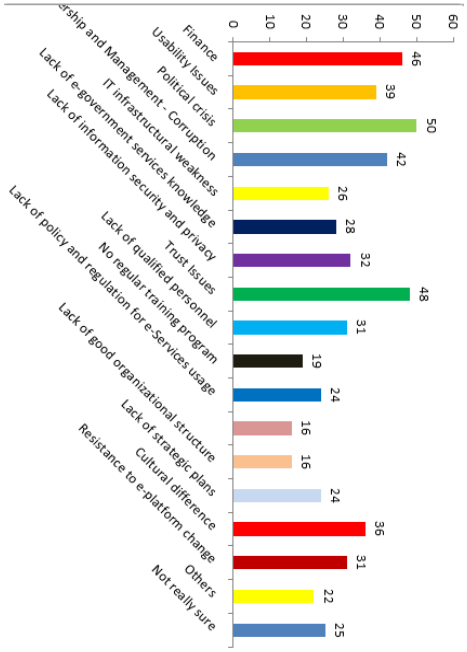

Figure 5. Barriers facing E-Service Adoption

As indicated in Figure 5 above and from that data available in my earlier survey on the Barriers Facing E-Service Technology in Developing Countries: A Structured Literature Review with Nigeria as a Case Study which was published in the LICE-2015 conference proceedings, trust issues have been a major problem together with internet security in E-Service adoption in developing countries. Though, there are various security measures that a user could do to have a secured transaction online but awareness is still very low and many system users need to acquire more knowledge on how to have a secured internet usage [16].

The security of the e-Service portals will be of the great benefit not only to the users but the government and private organisations who venture into the provision of E-Service to the populace. Furthermore, privacy principles must be respected and accepted by

the e-Services providers in order for the required benefits in implementing the projects to be achieved. More statistics analysis presented in both Table 1 and Table 2 below.

Table 1. Chi-Square Test on the barriers facing E-Service Technology

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	7.242[a]	7	.404
Likelihood Ratio	9.199	7	.238
Linear-by-Linear Association	2.130	1	.144
N of Valid Cases	30		

a. 16 cells (100.0%) have expected count less than the minimum expected count is .47.

Table 2. One-Sample Statistics T-Test on the barriers facing E-Service Technology

	N	Mean	Std. Deviation	Std. Error Mean
Main barriers facing E-Service Technology	30	4.33	2.454	.448

From the above analysis, the use of chi-square is very important in this study as categorical variables are involved from a single population. This will determine if there is a significant association between the variables as demonstrated in Table 1 on the barriers facing e-service technology. T-test statistical analysis, on the other hand, is useful when we need to compare performance in two conditions. T-test will help to decide if the difference between the conditions is real or merely fluctuations from one-time testing to another. In Table 2, one sample T-test allows us to test whether a sample mean differs significantly from hypothesized value.

4. Model For E-Service Technology In Developing Countries Capturing Security Threats and Proactive Measures

In other to justify the research argument and based on the results obtained from the survey which prominently identified Security Issues as major barrier facing e-service technology in developing countries, and the proactive measures to reduce and eradicate these security issues as obtained in related literature reviewed, a model has emerged as shown in Fig. 5 and this captures the E-Service technology Security issues and the proactive measures to reduce and eradicate these threats if fully implemented.

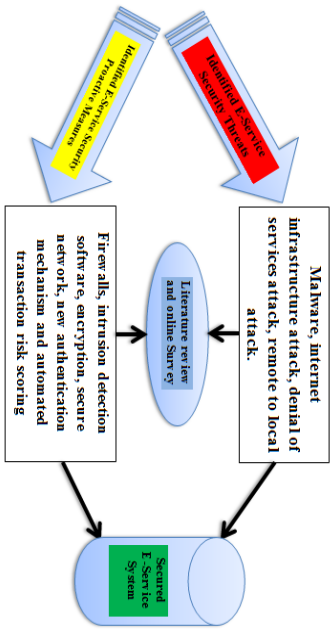

Figure 6. Proposed E-Service Security Model

5. Conclusion

We have been able to examine literature on what proactive measures need to be taken against E-Service security in developing countries and the use of online survey which gave us deep understanding on the users position towards E-Service security. A model has emerged as shown in Fig. 6 above and this captures the E-Service technology Security issues and the proactive measures to reduce and eradicate these threats if fully implemented. The use of the model is more prominent in the research methods/methodologies in various literatures reviewed.

The research is significant as the government need to invest money and commitment in the provision of a more secured E-Service to citizens, and it is rather unfortunate the situation at the moment. Though, e-Governance is still young in many developing countries such as Nigeria, successful E-Service implementation and adoption will provide increased revenue and the boost economy. There is a need for government to make a positive change in the way services are being delivered to citizen and others stakeholders. Changes should be made to legislation and laws in order to provide an enabling platform for E-Service Technology to flourish in the country. Issues like awareness and availability of services and trust all need further development in order to allow e-Government services to be delivered and used by citizens.

It is advisable to protect E-Service systems by adoption latest and current information best practices and unexpected activities from the internet attackers could further be prevented if strong security policies, procedures and practices could be put in place. A well-structured training and awareness program on

cyber security issues must be given to the employees handling various E-Services systems for both government and private companies as there is a need for them to take issues of E-Service security as part of their daily job while displacing high standard of ethics.

Further work is required to establish more advanced security measures apart from the ones earlier discussed to protect E-Services user's data from getting to the hand of unauthorized people. There is also a need to further validate the model developed in this paper and this is a limitation at the moment. More research is also needed to identify and implement cost-effective, usable E-Service Technology systems in developing countries.

6. Acknowledgement

Special thanks to the School of Computing and Faculty of Technology, the University of Portsmouth for granting the funds to attend the recently concluded IEEE i-Society international conference 2015 in London, United Kingdom.

7. Reference

[1] Ayoola T. J (1913) The effect of Cashless Policy of Government on Corruption in Nigeria, The International Review of Management and Business Research, Vol 2, Iss. 3.

[2] Bhuiyan, M.S.H (1911) "Public Sector eService Development in Bangladesh: Status, Prospects and Challenges" Electronic Journal of e-Government Volume 9 Issue 1, (pp11 - 29).

[3] Creswell J.W (1909) Research Design: Qualitative, Quantitative and Mixed |Methods Approaches. (Third Edition) SAGE Publication.

[4] CRISTEA, Valentin; LEORDEANU, Catalin; POP, Florin; DOBRE, Ciprian (1912) Proceedings of the Romanian Academy, Series A, The Publishing House of the Romanian Academy, Volume 13, Number 2, pp. 149–116.

[5] Hasan, M. Mahmudul (1911) E-Government Service Research Development: A Literature Review, International Journal of E-Services and Mobile Applications, 7(1), 18-49.

[6] Haque, S., and Pathrannarakul, P. (1913) The Role of Technology in Enhancing Transparency and Accountability in Public Sector Organizations of Pakistan. International Journal of Economics Business and Management Studies, 2(1), 19-24.

[7] Hector, D and Puyosa, P (1912) e-Government: Security Threats, IEEE eGovernment STC.

[8] Heeks Richard, and Savita Bailur (1907) "Analyzing e-government research: Perspectives, philosophies, theories, methods, and practice." Government information quarterly 24.2, pp 243-265.

[9] Kent, Jennifer and Steiner, Katie (1912) Ten Ways to Improve the Security of a New Computer, United States Computer Emergency Readiness Team.

[10] Khadaroo, I., Wong, M. S., & Abdullah, A. (1913) Barriers in local e–government partnership: evidence from Malaysia. An International Journal of Electronic Government, 10(1), 19-33.

[11] Manish Mehta, Sachin Singh and Yugyung Lee (1900) Security in E-Services and Applications, Wiley Inprint Inc.

[12] Mundy, D and Musa, B (1910) "Towards a Framework for e-Government Development in Nigeria" Electronic Journal of e-Government, Volume 8, Issue 2, PP148-161.

[13] Nkem Ekene Osuigwe and Amanze Unagha (1911) Public Libraries and E-Government in Nigeria, The Information Manager Vol. 11 (1&2).

[14] Patel, Nipul and Conners, Susan E (1908) Outsourcing: Data Security and Privacy Issues in India, Issues in Information systems, Vol. IX, No. 2.

[15] Ruyter Ko De, Martin Wetzels and Mirella Kleijnen (1901) "Customer adoption of e-service: an experimental study" International Journal of Service Management, Volume 12, No. 2, pages 184-197.

[16] Schwester, R. (1909) Examining the barriers to e-Government Adoption. Electronic Journal of e-Government, Vol 7(1).

[17] SPAFFORD, Eugene H. and ZAMBONI, Diego (1900) Intrusion detection using autonomous agents, Computer. Network, 34, pp. 547–570.

[18] Sulaiman, R., & Sharma, D. (1911) Enhancing security in e-health services using agent. In *Electrical Engineering and Informatics (ICEEI), 1911 International Conference on* (pp. 1-6). IEEE.

[19] Ward, Theresa (1910) Strategies for Reducing the Risk of eCommerce Fraud, A First Data Corporation White Paper.

[20] Webster, J. and Watson, R.T (2002) Analyzing the past to prepare for the future: Writing a literature review. MIS Quarterly 26, xiii–xxiii.

