E-Voting in Nigeria: A Survey of Voters' Perception of Security and Other Trust Factors

Conference Paper · November 2015

DOI: 10.1109/CYBER-Abuja.2015.7360511

3 authors, including:

Oluwafemi Osho
Federal University of Technology Minna
39 PUBLICATIONS **242** CITATIONS
SEE PROFILE

Victor Yisa
Federal University of Technology Minna
8 PUBLICATIONS **19** CITATIONS
SEE PROFILE

E-Voting in Nigeria: A Survey of Voters' Perception of Security and Other Trust Factors

Oluwafemi Osho*, Victor Legbo Yisa, Olawale Joshua Jebutu
Department of Cyber Security Science,
Federal University of Technology, Minna
*Corresponding Author: femi.osho@futminna.edu.ng

***Abstract*—In March and April, 2015, for the first time in the history of Nigeria, elections were conducted, using partial electronic voting means. Specifically, smart card readers were utilized for accreditation of prospective voters. While the 2015 election exercise was adjudged the best ever in the history of the country, it was not without challenges. One of these was the failure, in many instances, of the readers to authenticate eligible voters. This study was aimed at collating the perception by voters of security and four other factors capable of influencing their trust the use e-voting system. Using questionnaire, the data collated from 306 participants were analyzed. Majority of the participants were male (63.7%), students (40.8%), within the ages of 18 and 24 years (39.5%), and intermediate in their IT proficiency level (50.3%). The study reveals that the proposed factors enhance voters' trust. Demographic differences were also found to affect the perception of the proposed factors. If the country plans to deploy full-fledged e-voting mechanism for future elections, voter education, with emphasis on voters with low IT literacy and the elderly, must be given due attention.**

Keywords—election, e-voting, smart card reader, INEC, trust

I. INTRODUCTION

The advancement and application of information and communication technology in all facets of life have provided several potential benefits including improved efficiency, convenience, with reduced costs and productivity. Most countries and institutions all around the world are using ICT to improve services for its citizenry, a trend popularly known as e-governance [1]. An example of this is the application of ICT in the conduction of elections, a phenomenon known as electronic voting or e-voting.

Electronic voting is a general term which is connected here to allude to all parts of electoral voting that includes some component of casting or tallying of votes using electronic means [2][3]. Adoption of electronic voting during elections could solve problems, usually associated with manual voting, such as long queues, invalid votes, fraudulent votes, and help ensure transparency [4].

Many countries are at different stages of e-voting adoption. Countries like Australia, Canada, France, and Japan, have implemented legally binding e-voting and legally binding remote e-voting systems. While most countries are still holding pilots and trials, other countries, including Germany, Ireland, and Netherlands have stopped using e-voting for elections, due to the conclusion that further developments are needed in the fields [5].

Prior to 2015, elections in Nigeria had been conducted using traditional (manual) method of voting. Not surprisingly, each election had always been plagued by irregularities, rigging, and other forms of malpractices, malfeasances, and electoral fraud, which often lead to loss of lives and property [6], [7], [8], [9], [10]. Transparency, freeness, and fairness – which are all requirements of a voting system – have always been lacking. Mass ballot paper thumb printing, exemption of valid voters from the voters list, intimidation, errors due to miscomputation and forged results, snatching of ballot boxes, impersonation, and inflation of election results, to mention but few, were commonplace [11], [12]. The situation got so critical that some authors labeled elections in Nigeria as inseparable from violence [13], and synonymous with rigging [10]. Consequent upon these, [14] concluded that the manual method of conducting elections in Nigeria had been "bought over and corrupted;" thus highlighting the need for new ideas and methods of voting.

Attempts, in the past, to adopt the use of e-voting system by the Independent National Electoral Commission (INEC) in Nigeria were resisted, even by the legislature [6]. Sections 53(2) of the Electoral Act, 2006 [14], and 52 of the Electoral Act, 2010 [15], for instance, prohibited the use of an e-voting system. This resistance was borne out of the fact that past projects in the country had failed. And there was no guarantee that embarking on the use of e-voting system would fare better. In other words, the government could not be trusted in such critical area. Trust (or distrust) is easily transferable [16]. Having earned citizens' distrust in one area, it would be difficult for the government to be trusted in others.

However, over the years, the country has made significant progress in the adoption of technology. An instance is the adoption trend of mobile technology and internet, which have continually maintained an upward surge. From 2000 to 2013, the percentage of individuals using the internet rose from 0.06 to 38.00 [17], while the number of mobile subscribers have moved from 0.02 to 67.68 per 100 inhabitants, within a period of 12 years, from year 2000 [18]. Having experienced the benefits that information technology affords, the realization that more and more processes manually being handled could be automated has continued to grow stronger and wider. This

explains the yearnings and calls, from different sectors, for the adoption of e-voting system for the conduction of elections [12], [14], [15], [19], [20], [21]. And, considering the fact that even developing countries, like India and Brazil have successfully implemented e-voting for the conduction of their respective elections [12], [16], Nigeria cannot afford to continue with the traditional method.

In March and April, 2015, during the general elections, Nigerians witnessed the partial use of e-voting system to complement the manual method. By taking this stride, the country joined the league of low- and middle-income countries that have utilized biometric identification systems for voter identification. Up to 34 of these countries, including Ghana, Senegal, Cameroun, Zambia, Kenya, Malawi, Mali, Mauritania, Sierra Leone, and Rwanda had implemented, for one election or the other, this partial adoption of e-voting system [15]. Essentially, the decision to adopt the use of information and communication technology tools was the result of part of the recommendations of the Registration and Election Review Committee, a committee of experts on electoral issues inaugurated by INEC in 2011 [10].

During the 2015 general elections, e-voting mechanism was deployed to ease accreditation process. Smart card readers (SCRs), a low power consumption technological device running on the android operating system, were utilized for accreditation of voters, via authenticating and confirming voters' permanent voter's cards (PVCs) [10], [15], [22]. The permanent voter's card has a chip embedded into it to verify and authenticate prospective voters by comparing the biometrics earlier obtained and stored in the database during registration with that of the voter on the spot.

Before the elections, INEC test-ran the SCRs in 12 states of the Federation [23]. Unfortunately, most of the problems encountered during the test run were still experienced during the elections. For instance, some of the card readers broke down and were not able to perform its intended purpose. Others showed blank screens, while others had Subscriber Identification Module (SIM) issues [24]. Even where the card readers worked, and were able to correctly display voter's information from the PVC, verifying voters using their biometrics was very difficult [24], [25]. Yet, in spite of the shortcomings recorded, the use of the SCRs boosted voters' confidence in the electoral processes. Hence, it was not surprising that the number of elections petitions substantially dropped after the elections [15].

Electronic voting, over the years, has attracted vast amount of studies, spanning across many disciplines. However, most of these studies have concentrated on the technical aspect. These include e-voting design requirements [5], [26]; development [27], [28], [29], [30]; security [31], [32]; and implementation issues [33]. Quantitative studies have been mainly focused on investigating perceptions on requirements or factors that influence trust of, readiness to accept, and adoption of e-voting systems. Kimbi & Zlotnikova [16] investigated readiness factors, considering Tanzanian voters. Nu'man [34] developed a trust model to ascertain what trust requirements are applicable to voters in Jordan. Yao and Murphy [35] sampled potential voters in US, exploring their perceptions about e-voting requirements capable of influencing intention to use the systems.

Few studies have attempted exploring adoption models in the context of Nigeria. Studies by [12] and [36] focused on exploring factors that affect e-voting adoption from the perspective of managerial and operational staff of INEC – the nation's Election Management Body (EMB).

It has already been established that Nigerians are in support of the adoption of e-voting for elections in the country [21]. Yet, some pertinent questions need to be answered: Are all categories of voters similar in their opinion of e-voting system? Do voters prefer e-voting system to the traditional manual system? Which e-voting mechanism is most preferred by voters? What factors would enhance voters' trust in the adoption of e-voting system? This study seeks to identify some trust requirements capable of influencing, and investigate the level of influence of these requirements on, voters to trust the adoption of e-voting technology in Nigeria.

The rest of the study is organized as follows: section 2 discusses the theoretical foundations on which our model is based, and presents the research model. The methodology used in the study is described in section 3. Section 4 presents the results, while discussions on the results are presented in section 5.

II. THEORETICAL FOUNDATION

Our model of trust requirements is hinged on two research areas: information technology adoption and e-voting system (EVS) design.

A. Information Techn ology Adoption

Different theoretical models have been developed to explain user acceptance or adoption of technology, with varying capacity to explain the variance in the intention by individuals to use technology [37]. Some of these models include the Technology Adoption Model (TAM) [38], Technology-Organization-Environment (TOE) [39], Diffusions on Innovation (DOI) [40], and that proposed by [41]. Attempts have also been made to develop adoption model with specific focus on e-voting [12], [36].

One model, however, that encapsulates the conceptual and empirical frameworks of eight of these commonly used models, is the Unified Theory of Acceptance and Use of Technology (UTAUT), developed by [37]. This model has been demonstrated to be highly effective at explaining variance in user acceptance and usage behavior.

UTAUT is composed of four constructs: performance expectancy, effort expectancy, social influence, and facilitating conditions. Performance expectancy connotes the measure of perceived usefulness of a system towards achieving 'gains in job performance.' Effort expectancy refers to the measure of ease of use of the system. Social influence describes the perceived social approval to use the new system, while facilitating conditions are the measure of perceived availability

of the system's supporting organizational and technical infrastructure.

Extending this model to e-voting, three of the constructs, with the exception of social influence, can be applied to understand e-voting acceptance. These constructs capture specific requirements of e-voting systems. Performance expectancy directly relates with requirements such as security, privacy, and reliability. Effort expectancy is synonymous with ease of use of the e-voting system. Facilitating conditions, on the other hand, captures availability of the system.

B. E-Voting System Design

In reality, developing a perfect e-voting system is essentially an impossible task, given the current architecture of the internet and the PC [42], [43]. Notwithstanding, designing an EVS is a complex task. Zissis [5] explained that the complexity involved in this system is due to a host of multidisciplinary requirements that must be satisfied. Beyond technological considerations are legal, political, and societal influences [5].

Every EVS must satisfy some requirements. These have been categorized under legal, functional, operational, and security requirements. Some of these include [5], [35], [44]: availability, authenticity, freedom, eligibility, practicability, robustness, security, uniqueness, verifiability, fairness, democracy, privacy, ease of use, accuracy, integrity, and uncoercibility. These requirements affect the likelihood, and potentially the rate, of acceptance of any EVS. In other words, if an EVS would be accepted by users, there must be evidence that such system possesses most of the aforementioned characteristics.

A critical look at the requirements reveals that there are five major requirements, namely availability, security, privacy, ease of use, and reliability. Every other requirement is directly or indirectly related to one of these requirements. We define these primary requirements in respect of e-voting and list other related requirements:

- Availability: the property of a system to be accessible to authorized users whenever needed. This is closely linked with mobility and accessibility. With respect to e-voting, valid voters are provided with the means to cast their vote. Satisfying this requirement entails protecting the system against primarily network attacks capable of making the system unavailable to access. These attacks include distributed denial of service, traffic redirection, connection flooding, hardware-based attack [5], and jamming attack.

- Security: the property of an EVS to ensure voters and voting integrity. It encapsulates security of e-voting components: hardware, software, communications information [45] against different attacks. These attacks include insider (programmer), phishing, DNS, spoofing, denial of service, distributed denial of service, automated vote buying, and malware attacks [42], [26], [43], [46]. A secure e-voting system guarantees every vote is tamper-proof [29]. E-voting systems arguably require the highest possible level of security [34], exceeding that required for e-commerce [5], [43]. Security ensures other requirements like integrity, freedom, secrecy, equality, generality, fairness of elections [5], and authenticity.

- Privacy: this is a system's capability that ensures that a particular vote cannot be linked to a voter [29], [34], [35]; any traceability between a vote and its voter is basically removed [47]. An e-voting system that guarantees privacy ensures voters' votes are not revealed by the system. Based on this description, privacy is related with anonymity, confidentiality, uncoercibility, and secrecy.

- Ease of use: the property of an EVS that makes voters able to use it with little or no assistance. An e-voting system that is easy to use is especially beneficial to those with low computer literacy. One other requirement in the same category is practicability.

- Reliability: this is synonymous with dependability. It connotes a system's capacity to function as required. Such a system performs exactly as expected. A reliable system ensures that the voting outcome is the absolute consequence of the votes cast [26]. For instance, a reliable e-voting system must ensure no valid vote is rejected, and no invalid vote is accepted [34]. A reliable system is also capable of ensuring eligibility, robustness, accuracy, fairness, and democracy.

III. RESEARCH MODEL

Acceptance of new system always correlates with trust in such systems. The achievement of public trust has always been one of the cardinal objectives for implementing e-voting system [5]. This trust is enhanced when such system proves its dependability [34], and closely knit with this property of reliability is security.

The Council of Europe, in their guidelines on transparency of e-enabled elections [48] emphasized that "… trust should not be taken for granted and states need to do their utmost in order to ensure that it is preserved. All the more so because once trust and public confidence is diminished, it is exceedingly challenging to regain it."

Our trust model, represented in Figure 1, suggests that these five main requirements independently affect voters' trust. Based on this, we propose the following hypotheses:

H1: higher availability will influence voters' trust, and consequently participating, in the use of the electronic voting system.

H2: higher security of the system will influence voters' trust, and consequently participating, in the use of the electronic voting system.

H3: higher privacy of the system will influence voters' trust, and consequently participating, in the use of the electronic voting system.

H4: higher ease of use of the system will influence voters' trust, and consequently participating, in the use of the electronic voting system.

H5: higher reliability of the system will influence voters' trust, and consequently participating, in the use of the electronic voting system.

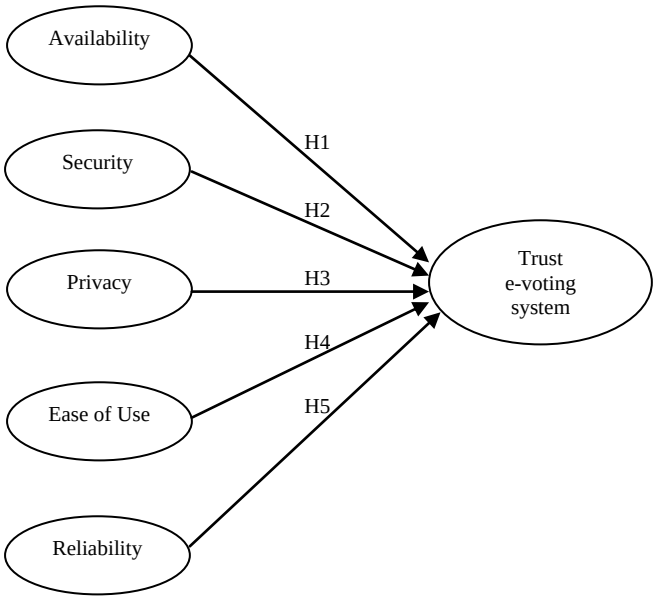

Fig. 1. Proposed model of trust factors

IV. Methodology

A. Participants

To collate data, a survey was conducted between October and November, 2014 in one of the northern states in Nigeria. A combination of purposive and stratified random sampling techniques was employed in the selection of participants. Based on the fact that the minimum age requirement to be eligible to vote is 18 years, we ensured only participants eligible to vote were considered. We then divided the above-18-years population into three groups: students, employed, and Non-employed. Participants from each group were sampled randomly.

The research instrument used was questionnaire. In total, 350 questionnaires were distributed. Out of these, 306 were valid, and consequently used in the analysis. The participants consist of 195(63.7%) males and 111(36.3%) females. Majority were students (40.8%), within the ages of 18 and 24 years (39.5%). Most (50.3%) classified their IT proficiency level as intermediate. The sample characteristics of the respondents are presented in Table 1.

B. Procedures and Data Analysis

The questionnaire (see Appendix F) used was composed of three sections. The first section contains definition of terms related to electronic voting used in the construction of the scale items. General questions pertaining to respondents' characteristics, and order of preference among the three main mechanisms of deploying electronic voting constituted the second section. The last section presents the measurement scales, each with 3 items. Level of agreement was indicated on a 5-point Likert scale, ranging from 1 = Strongly Disagree to 5 = Strongly Agree.

A pilot test was performed involving 28 respondents including IT faculty members and professionals, students, employed and unemployed personnel participated in a pilot test. Various comments were considered in revising the questionnaire, to improve its validity.

A candid assessment of the 10 IT faculty members and professionals who participated in the pilot test was sought. They were requested to rate the general layout, complexity, and relevance of the questions under each factor, using a scale of 1 to 5, where 1 stands for lowest score and 5 for the highest score. A minimum of 70% rated the general layout of the questionnaire, and each proposed factor, 4 and above. On the other hand, in terms of complexity, 70% scored the questionnaire 3 and below.

The internal consistency of the factors was measured with Cronbach's alpha coefficient. The overall internal consistency of the 15 items was 0.92, which indicate high reliability of the items. Each of the scales also indicated high reliability. The mean, standard deviation, and internal consistency of the 5 factors are presented in Table 2.

For the analysis of the data, SPSS 16.0 was used for descriptive analysis of the sample characteristics, and Amos 22 for confirmatory factor analysis of the constructs. For assessing model adequacy, Goodness-of-fit index (GFI), comparative fit index (CFI), both of which must be above 0.9 to have a good fit [35], [49]; the root mean square error of approximation (RMSEA), with value between 0.05 and 0.08 considered acceptable; and the normed chi-square (χ^2/df), where value less than 3 implies a good fit [50].

V. Result

A. Preferred E-Voting Mechanism

TABLE I. Sample Characteristics of Respondents

	Frequency	Percent
Sex		
Male	195	63.7
Female	111	36.3
Age		
18 – 24	121	39.5
25 – 34	96	31.4
35 – 44	62	20.3
45 – 54	22	7.2
55 – 64	4	1.3
Above 64	1	0.3
Occupation		
Student	125	40.8
Employed	95	31.0
Unemployed	86	28.1
IT Proficiency Level		
Novice	35	11.4
Intermediate	154	50.3

Advanced	90	29.4
Expert	19	6.2
Missing Values	8	2.6
Participated in Voting		
Yes	196	64.1
No	110	35.9
Preferred Voting System		
Manual Voting	75	24.5
E-Voting	225	73.5
Missing Values	6	2.0
Study Total	306	100.0

TABLE II. TABLE 2. MEAN, SD AND INTERNAL CONSISTENCY OF MODEL FACTORS

Factor	No. of Item	Mean	SD	Cronbach's alpha
Availability	3	4.41	0.83	0.70
Security	3	4.38	0.86	0.82
Privacy	3	4.29	0.82	0.77
Ease of Use	3	4.46	0.77	0.83
Reliability	3	4.50	0.79	0.81

When asked of the preferred voting method, 73.5% of participants reported they prefer electronic form of voting to the manual method. The study found out that in the category of participants who are novice in their level of IT proficiency, majority (72.7% v 27.3%) preferred manual voting. This contrasted sharply with other IT proficiency categories. In these categories, e-voting was preferred, with increasing percentage of majority from the intermediate to the expert category: intermediate (21.7% v 78.3%), advanced (16.9% v 83.1%), and expert (11.1% v 88.9%). The finding was highly significant ($\chi^2 = 45.54,\ p < 0.001$).

They were also requested to rank the 3 different electronic voting deployment platforms, in order of their preferences, from 1 = most preferred to 3 = least preferred. To identify if participants have different preferences for the e-voting mechanisms the Friedman test was used. The mean ranks of the mechanisms are presented in Table 3. Web-based e-voting system has the least mean rank. This implies it is the most preferred form of e-voting system. However, the finding was not significant ($\chi^2(1) = 3.66,\ p = 0.16$). It therefore cannot be concluded that voters do have different preferences for all the e-voting mechanisms.

TABLE III. TABLE 3. MEAN RANK OF E-VOTING MECHANISM

E-Voting Mechanism	Mean Rank
Polling booth/Kiosk voting system	2.09
Web-based EVS	1.94
Mobile-based EVS	1.97

B. Measurement Model results

The results of the measurement model and confirmatory factor analysis of security and other trust factors are presented in Table 4 and Figure 2 respectively. The obtained model fit indices were GFI = 0.90, CFI = 0.93, RMSEA = 0.08, $\chi^2/df = 2.87$, and $p < 0.001$. The factor loading of each latent variable was high, with range from 0.54 – 0.86. The same can be observed with the scales. Each factor loading was also high, with values between 0.76 and 0.92.

We performed some post hoc analyses to see if there are differences in perception based on the individual factors. We focused on perception by sex, age, occupation, IT proficiency level, and voting experience. In the perception by sex (see Appendix A), male participants had higher perception scores for three of the characteristics: security, privacy, and ease of use. Both sexes had similar perception for availability and reliability. Considering perception by age (Appendix B), in all the characteristics, except security, the perception scores by the age group 55 – 64 were lower than the rest of the groups. Based on occupation (Appendix C), the study reveals those who were unemployed rated all the characteristics lower, when compared to the scores by those in other occupation categories. One interesting finding is the perception by IT proficiency level (Appendix D). In all the characteristics, with increasing level of proficiency, there was increase in perception score. The same as discovered when the perceptions by voting experience was considered (Appendix E). Those who possessed voting experience scored all the characteristics higher.

VI. DISCUSSION

This study aimed to explore the perception of voters on security and four other trust factors, to influence participation in the use of e-voting system for elections in Nigeria. The construction of the factors was based primarily on e-voting system characteristics. The scale items indicated high internal consistency. Data used for testing the measurement model were collated using survey method. Majority of the participants were male, students, within the ages of 18 and 24 years, and intermediate in terms of IT proficiency. Majority of the participants had participated in one or more elections in the past.

The study found out that majority of voters would prefer the use of e-voting system, rather than continue with the manual method primarily in use. This is consistent with the finding of [21]. However, voters who deem themselves novice in their IT proficiency level prefer the country continue to utilize manual voting during elections. Kimbi and Zlotnikova [16] had identified low IT literacy as an impediment to acceptance of e-voting system. Much effort would no doubt be required to convince this category to accept the use of e-voting system. Equally to increase such voters' trust, the electronic voting system must be developed to guarantee maximum ease of use. This finding also highlights the need for government to develop necessary measures to bridge the digital divide.

Another finding is the lack of significant evidence to conclude that voters prefer one e-voting method to another. One explanation is that voters in Nigeria are generally not used to the use of electronic method of voting. An e-voting system was used, partially, for the first time in the last 2015 general elections. Until there is full adoption, voters will not be able ascertain which mechanism is most preferable.

TABLE IV. TABLE 4. MEASUREMENT MODEL RESULT

Factor	Item	Loading
Availability	Be deployable via mobile and web platforms, and/or a polling station	0.54
	Have facilities for all eligible citizens, including disabled and old citizens, to be able to vote.	0.71
	Be accessible right from the time voting starts and all through the period of voting.	0.77
Security	Ensure only eligible voters can access the e-voting system.	0.66
	Ensure a cast vote cannot be altered by unauthorized person or system.	0.86
	Be secure against session hijacking, malware, and other forms of attack.	0.83
Privacy	Ensure voters' identification data are secure against unauthorized disclosure and alteration.	0.76
	Ensure no vote can be traced to a particular voter.	0.63
	Ensure no attacker can successfully eavesdrop on a voter during voting process.	0.83
Ease of Use	Be easy to learn to use.	0.82
	Be simple to operate.	0.86
	Provide help facility readily available to voters in the event of problems with voting procedures.	0.71
Reliability	Ensure no voter can successfully cast more than one vote.	0.82
	Be able to acquire votes correctly, i.e., any vote cast is rightly recorded.	0.78
	Not reject valid votes nor accept invalid votes.	0.70

$\chi^2 = 244.05$, $df = 85$, GFI = 0.90 CFI = 0.93, RMSEA = 0.08, p < 0.001

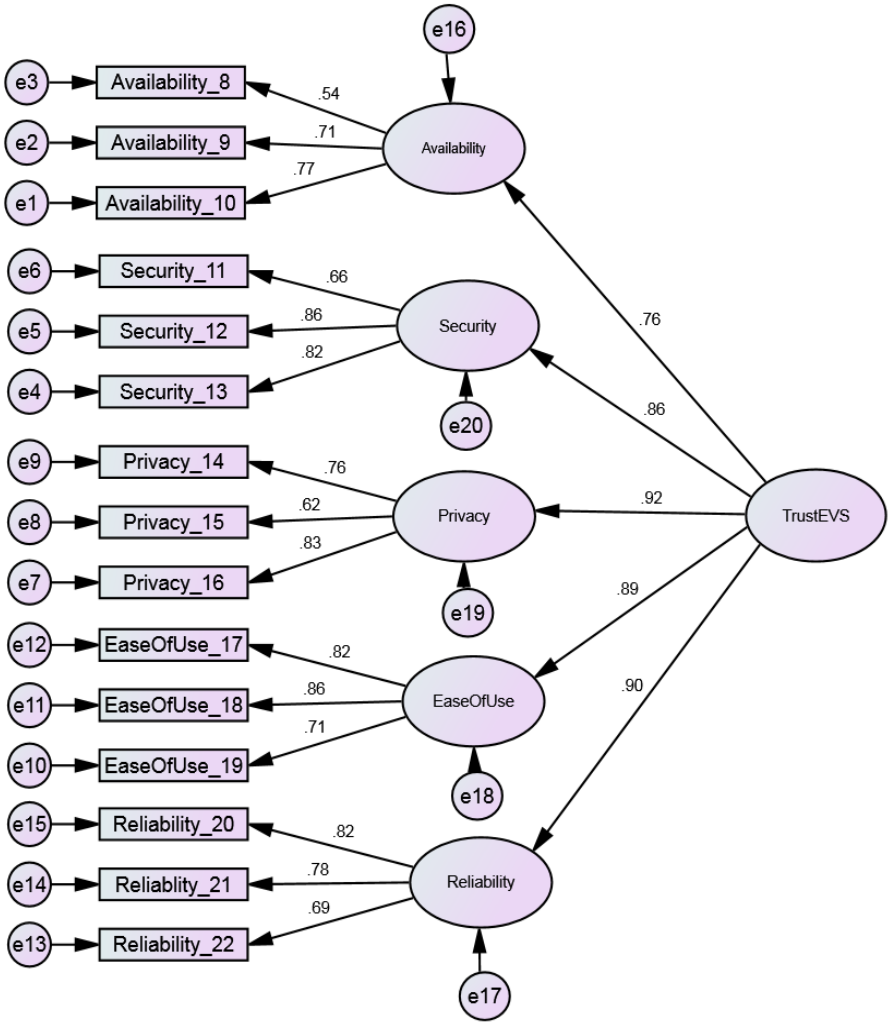

Fig. 2. Confirmatory factor analysis of security and other trust factors

As expected, all five factors – privacy, reliability, ease of use, security, and availability – are capable of enhancing voters' trust in the acceptance of e-voting system for elections. A similar result was recorded in [16], where majority of voters in Tanzania have concerns over security, reliability, and privacy of e-voting, though they prefer the system to the existing manual system. The authors cautioned that absence of security, reliability, and privacy would pose serious threats to acceptance of e-voting. Thus, an EVS that would earn voters' trust, and consequently determine their acceptance and participation, must satisfy all these requirements.

Surprisingly, security was rated only ahead of availability. Privacy was placed in the first position. When privacy is related with anonymity, confidentiality, uncoercibility, and secrecy, it becomes clearer while this is most paramount to Nigerian voters. The use of coercion, either physically or subtly, from informal observations, is not new in the country. For instance, during the last general elections, one of the authors witnessed prospective voters in a particular polling booth being promised monetary rewards once they voted for a particular candidate. While a voter cast vote, the agent of the candidate was close by to ensure such voter voted as instructed. It is obvious that any system that would guarantee the privacy of voters would be welcomed.

Closely tied to privacy was reliability. The smart card readers used during the 2015 general elections were not reliable. If one views this characteristic in connection with eligibility, accuracy, fairness, and democracy, it can be said unequivocally that if electronic form of voting would be used for future elections, the government must ensure these related characteristics are given due attention in the e-system design. During the elections, many eligible voters were not authenticated by the readers. The voters' registration sheets had to be completely resorted for accreditation of voters.

Ease of use is another important factor to influence trust in an e-voting system. Any system that is difficult to use, regardless of the amount of functionalities it possesses, would not be easily acceptable by users. Most voters would prefer to cast their votes with little or no help, even if they have to use an electronic system.

It has been cautioned that replacing manual, paper-based, voting with e-voting could exclude a sizeable number of voters from participating [51], most of which would likely be old voters and those with low computer literacy. Studies have ascertained the fact that age provides a bias towards e-voting, with young voters having most bias for the system [16], [35], [51]. Providing an easy to use e-voting system would inevitably contribute substantially to alleviating this potential challenge. Zissis [5] advised that to make e-voting as equivalent to manual voting, ease of use and accessibility must be guaranteed.

An e-voting system that aims to gain its users' trust must guarantee security, as deduced from the study. This covers security of voting data and channels. Voter and voting integrity are essential for any essential election. To ensure security of e-voting system, [16] warns that it must not be perceived only from a technical point of view. Issues relating to security are often local, specific to individual country. The government and EMB will do well to identify the local threats, and put necessary mechanisms in place to address them.

The least scored factor was availability. However, the rating is high enough to affect voters' trust. Voters definitely would appreciate a voting system that is easily accessible; and deployable via different platforms, including mobile platform. Mobile penetration is Nigeria has continued to maintain upward trend. This technology could be leveraged on for election purpose.

One other interesting findings in this study is the need for due attention to be paid to demographic differences. Those who had ever voted in Nigeria gave higher considerations to the proposed trust factors. Also, the level of rating was influenced by level of IT proficiency. Considering the fact that majority of voters with low computer literacy prefer manual to electronic voting system, simply explains why they rated all the trust factors less than voters in other IT proficiency category. The implication is that the government needs to massively improve existing methods employed for voter education.

Our study also agrees with [37] in the moderation of performance expectancy by age. Using the UTAUT, it was noted that the influence of performance expectancy is stronger for men. From our study, while both men and women rated reliability equally, the men were more disposed to security and privacy. The study also reveals that men also tend to value ease of use, as a trust factor, more than women. This contradicts the finding of [35].

VII. Conclusion

The Independent National Electoral Commission (INEC) has been urged to utilize electronic voting mechanism for future elections [19], [20]. One important summary of this study is that any e-voting system the Commission hopes to deploy must give due considerations to characteristics that a typical e-voting system must possess. Essentially, privacy, reliability, ease of use, security, and availability are critical to enhancing voters' trust in the system. Also, voter education, with emphasis on voters with low IT skills and adult voters, would be indispensible.

Having recorded some significant gains upon the partial adoption of e-voting during the 2015 general elections, it is evident that embracing e-voting fully can only improve election processes in Nigeria. The country must therefore take decisive steps towards full implementation of electronic voting. Evidently, the electoral reforms will be gradual. The starting point could be establishing necessary legislative framework. An example is Kenya, which, in a bid to reform her electoral processes, established a new electoral body. One of the mandates given to the Commission was "the use of appropriate technology and approaches in the performance of its functions" [52]. However, considering the consequences Nigerians have experienced in past elections as a result of the perversion of the manual methods, it is evident that the country

cannot afford to get it wrong, when she decides to fully implement electronic voting system.

While this study has exposed some important findings in respect of the adoption of electronic voting systems for future elections in Nigeria, there are limitations. The fact that data was collected within one state of the country imposes a constraint to generalizing the result of the study as being representative of the entire country. While it may be argued that experience by voters during elections, which potentially could affect their disposition to a new system of voting, are similar across the nation, further studies, covering preferably all the geopolitical zones of the country, are required before accurate generalization can be made.

Another limitation is the lack of consideration of the relationships among the different factors. Essentially, all the factors are inter-connected. An e-voting system that cannot guarantee security would invariably not ensure privacy. These inter-relationships could also be explored in further studies for the construction of the measure model.

References

[1] O M Olaniyi, D O Adewumi, E A Oluwatosin, O T Arulogun, and M A Bashorun, "Framework for Multilingual Mobile E-Voting Service Infrastructure for Democratic Governance," *African Journal of Computing and ICT Nigeria Computer*, vol. 4, no. 3, pp. 23 – 32, 2011.

[2] S. A. Adeshina & O. Adegboyega, "Design Imperatives for Evoting as a Socio-technical System," in Electronics, Computer and Computation (ICECCO), 2014 11th International Conference on, 2014, pp. 1-4.

[3] Tsun-Shao Chen. (2003, July) https://files.nyu.edu/tsc223/public/ElectronicVoting.pdf

[4] Murshadul M Hoque, "A Simplified Electronic Voting Machine System," international Journal of Advanced Science and Technology, vol. 62, pp. 97-102, 2014

[5] D. Zissis, "Methodologies and technologies for designing secure electronic voting information systems," Unpublished.

[6] C. Ayo, A. A. Adebiyi, & A. B. Sofoluwe, "E-Voting Implementation in Nigeria: The Success Factors," in Curbing Political Violence in Nigeria: The Role of Security Profession, R. I. Salawu, A. Akinade, & S. O. Adetona, Eds., 2008, pp. 50-60.

[7] J. Iteshi, "Audio-visual voting method, The only way to build genuine democracy in Nigeria," 2006, Retrieved from http://www.gamji.com/article6000/NEWS6205.htm

[8] L. Anyanya, "Assessment of 2011 elections in view of recommendations from the 2010 workshop," in Election Security in Nigeria: Matters Arising, L. Olurode, Eds. Abuja: Friedrich-Ebert-Stiftung, 2013, pp. 19-30.

[9] M. Igini, "Election security in theory and practice: Perspective of a resident electoral commissioner," in Election Security in Nigeria: Matters Arising, L. Olurode, Eds. Abuja: Friedrich-Ebert-Stiftung, 2013, pp. 43-62.

[10] k. Bolaji, "Toward institutionalizing credible elections in Nigeria: A review of reform measures by the Independent National Electoral Commission" in Improving Electoral Practices: Case Studies and Practical Approaches, Stockholm: Institute for Democracy and Electoral Assistance, 2015, pp. 49-82.

[11] F. N. Okafor, "Electoral Violence and The 2015 General Elections in Nigeria: The Implication Perspective," *Afro Asian Journal of Social Sciences*, vol. VI, no. 1, pp. 1-14, 2015.

[12] S. R. Ishaq, W. R. S. Osman, A. J. K. Shittu & R. G. Jimoh, "Adoption of e-voting system in Nigeria: A conceptual framework, " International Journal of Applied Information Systems, vol. 5, no. 5, 2013, pp. 8-14.

[13] L. Olurode & M. K. Hammanga, "Deployment of security personnel in elections: Challenges and lessons from the field," in Election Security in Nigeria: Matters Arising, L. Olurode, Eds. Abuja: Friedrich-Ebert-Stiftung, 2013, pp. 63-85.

[14] F. Okoye, "Nigeria: Civil Society Groups and Electronic Voting Systems, the Challenges," Vanguard, January 2010, Retrieved from http://www.vanguardngr.com/2010/01/civil-society-groups-and-electronic-voting-systems-the-challenges/

[15] C. Nwangwu, "Biometric Voting Technology and the 2015 General Elections in Nigeria," Conference on The 2015 General Elections in Nigeria: The Real Issues, July 2015. Retrieved from http://www.inecnigeria.org/wp-content/uploads/2015/07/Conference-Paper-by-Chikodiri-Nwangwu.pdf

[16] S. Kimbi & I. Zlotnikova, "Citizens' readiness for remote electronic voting in Tanzania," Advances in Computer Science: an International Journal, vol. 3, issue 2, no. 8, 2014, pp. 150-159.

[17] ITU, "Individuals Internet: 2000-2013," Retrieved from http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals_Internet_2000-2013.xls

[18] ITU, "Mobile_cellular_2000-2012," Retrieved from http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Mobile_cellular_2000-2012.xls

[19] S. Daniel, "2015: As Buhari's victory covers INEC flaws…," Vanguard, May 2015, Retrieved from http://www.vanguardngr.com/2015/05/2015asbuharisvictorycoversinecflaws/

[20] C. Okeke, "Implement electronic voting in 2019, CSO tell INEC," Leadership, June 2015, Retrieved from http://leadership.ng/news/440398/implementelectronicvotingin2019csostellinec

[21] C. Ayo, A. Adeniyi, & I. Fatudimu, " E- Democracy: A Requirement for a Successful E-Voting and E-Government Implementation in Nigeria," International Journal of Natural and Applied Sciences, 4(3), 2008, pp. 310-318.

[22] INEC. (2015) www.inecnigeria.org. [Online]. www.inecnigeria.org/wp./FactSheet-on-PVC-and-Card-Readers.docx

[23] A. Hassan. (2015, March) Premium Times. [Online]. http://www.premiumtimesng.com/news/headlines/178264-inec-says-card-reader-test-successful-admits-41-fingerprints-verification-failure.html

[24] Vanguard. (2015, march) Vanguard Nigeria. [Online]. http://www.vanguardngr.com/2015/03/after-initial-card-reader-failure-nigerians-persevere-vote-in-peaceful-elections/

[25] N. Ibeh. (2015, March) Premium Times. [Online]. http://www.premiumtimesng.com/news/top-news/179447-3-card-readers-fail-to-accredit-jonathan.html

[26] D. A. Gritzalis, "Principles and requirements for a secure e-voting system," Computers & Security, vol. 21, no. 6, 2002, pp. 539-556.

[27] M. Malkawi, M. Khasawneh, O. Al-Jarrah, & L. Barakat, "Modeling and simulation of a robust e-voting system," Communications of the IBIMA, vol. 8, 2009, pp. 198-206.

[28] R. Alaguvel & G. Gnanavel, "Offline and online e-voting system with embedded security for real time application," International Journal of Engineering Research, vol. 2, no. 2, 2013, pp. 76-82.

[29] G. Z. Qadah & R. Taha, "Electronic voting systems: Requirements, design, and implementation," Computer Standards & Interfaces, vol. 29, 2007, pp. 376-386.

[30] L. O. Osho, "Development of a hybrid e-voting system using cloud architecture," Unpublished.

[31] I. Ray, I. Ray & N. Narasimhamurthi, "An anonymous electronic voting protocol for voting over the internet," Proceedings of the Third International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems, WECWIS, 2001, pp. 188-190.

[32] A. Juels, D. Catalano & M. Jacobsson, "Coercion-Resistant Electronic Elections," Proceedings of the 2005 ACM workshop on Privacy in the electronic society. ACM, 2005, pp. 61-70.

[33] R. kofler, R. krimmer & A. Prosser, "Electronic voting: algorithmic and implementation issues," Proceedings of the 36th Hawaii International Conference on System Sciences, 2003, pp.1-7.

[34] A. Nu'man, "A framework for adopting e-voting in Jordan," Electronic Journal of e-Government, Vol. 2, Issue 2, 2012, pp.133-146.

[35] Y. Yao & L. Murphy, "Remote electronic voting systems: an exploration of voters' perceptions and intention to use," European Journal of Information Systems, Vol. 16, 2007, pp.106-120.

[36] S. R. Ishaq, R. G. Jimoh, W. R. S. Osman, & A. J. K. Shittu, "Adoption of e-voting systems: A case study of Independent National Electoral Commission (INEC), Nigeria: A Preliminary study," Knowledge Management International Conference (KMICe), Malaysia, pp. 304-308, July 2012.

[37] V. Venkatesh, M. G. Morris, G. B. Davis & F. D. Davis, "User acceptance of information technology: Toward a unified view," MIS Quarterly, vol. 27, no. 3, 2003, pp. 425-478.

[38] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," MIS Quarterly vol. 13, no. 3, 1989, pp.319–339.

[39] L. Tornatzky, & M. Fleischer, The Process of Technology Innovation, Lexington, MA: Lexington Books, 1990.

[40] E. M. Rodgers, Diffusion of Innovations, 4th ed. New York: Free Press, 1995.

[41] C. L. Iacovou, I. Benbasat, & A. S. Dexter," Electronic Data Interchange and small Organizations: Adoption and Impact of Technology," MIS Quarterly, 19(4), pp. 465- 485.

[42] D. Jefferson, A. Rubin& B. Simons, "A comment on the May 2007 DoD report on Voting Technologies for UOCAVA Citizens" Retrieved from https://www.verifiedvoting.org/wp-content/uploads/2014/10/serve_dod_comment_2007.pdf

[43] D. Jefferson, A. D. Rubin, B. Simons & D. Wagner, "A security analysis of the Secure Electronic Registration and Voting Experiment (SERVE)," 2004, Retrieved from http://requiem.googlecode.com/files/paper.pdf

[44] A. Al-Ameen & S. A. Talab, "E-voting System Vulnerabilities," in Information Science and Digital Content Technology (ICIDT), 2012 8th International Conference, 2012, pp. 67-73.

[45] E. Onyekpere, "Election security finance," in Election Security in Nigeria: Matters Arising, L. Olurode, Eds. Abuja: Friedrich-Ebert-Stiftung, 2013, pp. 87-101.

[46] S. S. Chaeikar, M. Jafari, H. Taherdoost & N. S. C. Kar, "Definitions and criteria of CIA security triangle in electronic voting system," International Journal of Advanced Computer Science and Information Technology, vol. 1, no. 1, 2012, pp. 14-24.

[47] K. Sampigethaya & R. Poovendran, "A framework and taxonomy for comparison of electronic voting schemes," Computers & Security, vol. 25, 2006, pp. 137-153.

[48] Council of Europe, "Guidelines on transparency of e-enabled elections," 2011, Retrieved from Retrieved from http://www.coe.int/t/DEMOCRACY/ELECTORAL-ASSISTANCE/themes/evoting/CoEenabledElections_en.pdf

[49] J. F. Hair, R. E. Anderson, R. L. Tatham & W. C. Black, Multivariate Data Analysis, 5th ed., New Jersey: Prentice-Hall, 1998.

[50] L. W. Vilca & M. Vallejos, "Construction of the Risk of Addition to Social Networks Scale (C^r.A.R.S)," Computers in Human Behavior, Vol. 48, 2015, pp.190-198.

[51] A. Oostveen & P. V. D. Besselaar, "Users' experiences with e-voting: A comparative case study," International Journal of Electronic Governance, vol. 2, no. 4, 2009, pp. 357-377.

[52] L. Mahiri-Zaja, "New security challenges of election management in Kenya," in Election Security in Nigeria: Matters Arising, L. Olurode, Eds. Abuja: Friedrich-Ebert-Stiftung, 2013, pp. 115-121.

Appendix A: Perception by Sex

Level	Availability	Security	Privacy	Ease of Use	Reliability
Male	4.41	4.39	4.30	4.49	4.50
Female	4.41	4.35	4.28	4.43	4.50

Appendix B: Perception by Age

Level	Availability	Security	Privacy	Ease of Use	Reliability
18 – 24	4.45	4.40	4.33	4.49	4.50
25 – 34	4.35	4.39	4.23	4.47	4.50
35 – 44	4.43	4.35	4.26	4.47	4.52
45 – 54	4.38	4.27	4.42	4.36	4.49
55 – 64	4.25	4.33	4.17	4.17	4.42

Appendix C: Perception by Occupation

Level	Availability	Security	Privacy	Ease of Use	Reliability
Student	4.45	4.44	4.33	4.50	4.51
Employed	4.47	4.39	4.33	4.51	4.58
Non-employed	4.27	4.27	4.18	4.36	4.38

Appendix D: Perception by IT Proficiency Level

Level	Availability	Security	Privacy	Ease of Use	Reliability

Novice	4.13	4.03	3.92	4.15	4.21
Intermediate	4.42	4.35	4.25	4.45	4.48
Advanced	4.46	4.50	4.44	4.56	4.57
Expert	4.60	4.70	4.49	4.70	4.63

Appendix E: Perception by Voting Experience

Voting Experience	Availability	Security	Privacy	Ease of Use	Reliability
Yes	4.44	4.40	4.36	4.47	4.53
No	4.36	4.33	4.17	4.46	4.44

Scale from 1 = Strongly Disagree to 5 = Strongly Agree

Appendix F: Questionnaire Item

E-Voting Adoption in Nigeria: A Survey of Voters' Perception of Security and Other Considerations

Dear Ma/Sir, the aim of this survey is to explore the degree of influence of security and other factors among voters to trust the adoption of e-voting technology in Nigeria. We therefore solicit your sincere response. Your utmost privacy is guaranteed. Thanking you for your usual cooperation.

Definitions

- **E-Voting**: (also known as electronic voting) system is an automated system of voting via electronic means. Often votes are cast and tallied electronically.
- **Session Hijacking (**mentioned in question 13**):** occurs when a hacker takes over an authenticated user's session.
- **Malware (**mentioned in question 13**):** a software or program created to cause a computer system to malfunction. Example of malware is a virus program.
- **Eavesdrop (**mentioned in question 16**):** unauthorized capturing of data packets during transmission between systems.

General Questions

1. Sex: **[ ]** Male **[ ]** Female.
2. Occupation: **[ ]** Student **[ ]** Employed **[ ]** Non-Employed.
3. Age: **[ ]** 18-24 **[ ]** 25-34 **[ ]** 35-44 **[ ]** 45-54 **[ ]** 55-64 **[ ]** Above 64.
4. Level of IT skills proficiency: **[ ]** Novice **[ ]** Intermediate **[ ]** Advanced **[ ]** Expert.

> **Novice:** requires frequent guidance in the use of computer, its applications and tools.
> **Intermediate:** requires occasional guidance in the use of computer, its applications and tools.
> **Advanced:** generally require little or no guidance.
> **Expert:** serves as key resource and advises others.

5. Have you ever participated in any voting (either at the local government, state, or national level) before? **[ ]** Yes **[ ]** No.
6. For an election, which system of voting would you prefer? **[ ]** Manual (traditional) voting **[ ]** e-voting.
7. Assuming the following three e-voting mechanisms were all available in an election, rank them according to your preference. Write '1' for your most preferred, '2' for the next preferred, and '3' for the least preferred.
   - **[ ]** Polling booth/Kiosk e-voting system
   - **[ ]** Web-based (Computer-based) e-voting system
   - **[ ]** Mobile-based e-voting system

For the following statements please indicate (by ticking) your agreement using the scale:

5 = Strongly agree 4 = Agree 3 = Neutral 2 = Disagree 1 = Strongly Disagree

		5	4	3	2	1
Availability – An e-voting system should:						
8.	Be deployable via mobile and web platforms, and/or a polling station					
9.	Have facilities for all eligible citizens, including disabled and old citizens, to be able to vote.					
10.	Be accessible right from the time voting starts and all through the period of voting.					
Security – An e-voting system should:						
11.	Ensure only eligible voters can access the e-voting system.					
12.	Ensure a cast vote cannot be altered by unauthorized person or system.					
13.	Be secure against session hijacking, malware, and other forms of attack.					
Privacy – An e-voting system should:						
14.	Ensure voters' identification data are secure against unauthorized disclosure and alteration.					
15.	Ensure no vote can be traced to a particular voter.					
16.	Ensure no attacker can successfully eavesdrop on a voter during voting process.					
Ease of Use – An e-voting system should:						
17.	Be easy to learn to use.					

18.	Be simple to operate.					
19.	Provide help facility readily available to voters in the event of problems with voting procedures.					
Reliability – An e-voting system should:						
20.	Ensure no voter can successfully cast more than one vote.					
21.	Be able to acquire votes correctly, i.e., any vote cast is rightly recorded.					
22.	Not reject valid votes nor accept invalid votes.					