Trust Models in Information Systems Security – A Survey

[1]Faye, W., [2]Ibitowa, F.O. & [3]Longe, O.B.
[1&3]School of IT & Computing, American University of Nigeria, Yola, Nigeria
[3]Department of Computer Science, The Polytechnic, Ibadan, Nigeria
E-mails: winner.faye@aun.edu.ng; ibitowafolashade@yahoo.com; olumide.longe@aun.edu.ng

ABSTRACT

As we move towards a data-centric world with shifting threats and perimeters that threatens the realization of network security goals such as availability, integrity, confidentiality, authentication, authorization, privacy, non-repudiation of services and other hard security issues, it has become expedient to shift paradigm in the way trust is established and authenticated. Trust is a subjective human belief. It is one the most essential means to improve security and enable interoperability in existing heterogeneous information ecosystem architecture. Trust models are used widely in information systems with the purpose of measuring the trustworthiness of a set of entities based on their behaviours. Today's enterprises are open and competitive and relies on distributed infrastructure across various geo-spatial location and various cyber-physical locations in order to offer seamless and effective services to clients. With attendant increasing digitization and decentralization of information technology (IT) and information and control systems (ICS) especially in nuclear installations and associated facilities distributed computing frameworks are becoming more vulnerable to attacks from malicious agents, masquerading as trusted agents, thereby increasing the chances of risks and security compromises. This necessitates a better understanding of trust models used in computing, as trust and reputation management system are tools to mitigate security threats and vulnerabilities. This paper presents a precise and condensed survey of selected trust models used in information systems. The attributes of trust needed for enterprise information systems and networks are identified with the aim of identifying trust characteristics in each model.

Keywords: Trust Models, Information System, Security, Distributed Systems.

iSTEAMS Multidisciplinary Conference Proceedings Reference Format

Faye, W., Ibitowa, F.O. & Longe, O.B. (2019): Trust Models in Information Systems Security – A Survey. Proceedings of the 22nd iSTEAMS Multidisciplinary SPRING Conference. Aurora Conference centre, Osogbo, Nigeria. 17th – 19th December, 2019. Pp 223-241
www.isteams.net/spring2019. DOI - https://doi.org/ 10.22624/AIMS/iSTEAMS-2019/V22N1P21

1. INTRODUCTION

The term trust is coined out from the sociological, psychological and environmental environments. The term trust isn't distinctive. It tends to vary on the context where and the reason for its use. It has drawn most attention of researched whose specialty is on system security. There is no agreed on definition for the term trust, however, its help in aiding in the decision-making processes has gained wide acceptance (Fernandez-gago, Moyano, & Lopez, 2017). Trust is the ground and underpinning of secure communication (Shibin et al., 2017), Various fields like the electronic commerce, social media, mobile technology, web services, wireless technology and many more have used the trust construct to gain a competitive advantage against others who are into similar business. For example online retail forecast in 2012 noticed around the world the increasing number of online user and has tripled until date, reasons because more after intensive study on the continuous intention of user it was noticed that this numbers jumped up because more emphasis was put into creating sufficient trust and perceived sense of security on their various platform(Meskaran, Ismail, & Shanmugam, 2013).

1.1 Trust Models

Different kinds of model have been proposed by different authors to aid fasten up information security. Model such as Tr-OrBAC Model is a model proposed by (Irfane, 2015) for a collaborative system is meant for access control into the collaborative system. A collaborative system can be view as a different organization coming together to accomplish a task. STrust Model is a model proposed by (Sherchan & Paris, 2011) is a framework of build around the social network to facilitate trust amongst users of the platform. SORT Model is a self-organizing trust model built to ensure trust amongst paired system. Some other conceptual model has been built around scenario cases with regards to trust has been proposed. This clearly shows how important it is for the term *"Trust"* to be in place to ensure users acceptance and a competitive advantage to others who has similar technology in place. Prior research on this trust model has shown of a trend of an improved model of trust over the years and have tried to improve on previous model existing so as to ensure the security of information.

2. EXISTING RESEARCH ON TRUST MODELS

We present here very recent researches on trust models by authorship, title, focus, theory/method, the research Method and gaps identified. Kim, Tao, Shin, & Kim (2010) in their article titled "An empirical study of customers' perceptions of security and trust in e-payment systems Change" focused on the concept of trust as believed to improve security, hence the paper investigated issues with electronic payment and how customer perceive trust and security and how it motivates the usage of Electronic payment . The TAM Model was used and a Quantitative approach was adopted for evaluation. The findings of this study showed technical and security factors rise the intention of customers. Consumers' perceived security and trust positively as it related to consumers' perceived use of electronic payment. The TAM model is not sufficient enough to test how customer perceive the payment system as it measures just 40% of the customer's perception.

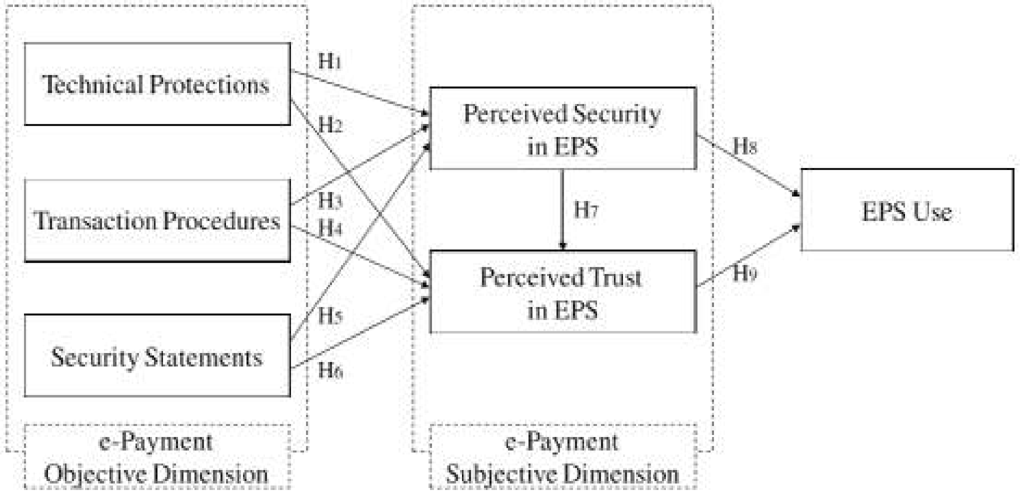

Figure 1. The model of perceived security and perceived trust in EPS use.
Source : Kim, Tao, Shin, & Kim, (2010)

Sherchan & Paris (2011) proposed STrust: A Trust Model for Social Networks Building trust on Social Platform. A model was proposed to ensure people share their opinion without been judges and finally then report In lack of trust on the social platform and the way it has improved after the model has been implemented. It was a conceptual paper. The findings of these study showed the behaviors of users on the social platform and how to identify malicious persons. It is with this regards that a recommendation for future work was given to develop an approach for bootstrapping the web community in order that the causative cycle between social trust and social capital is resolved.

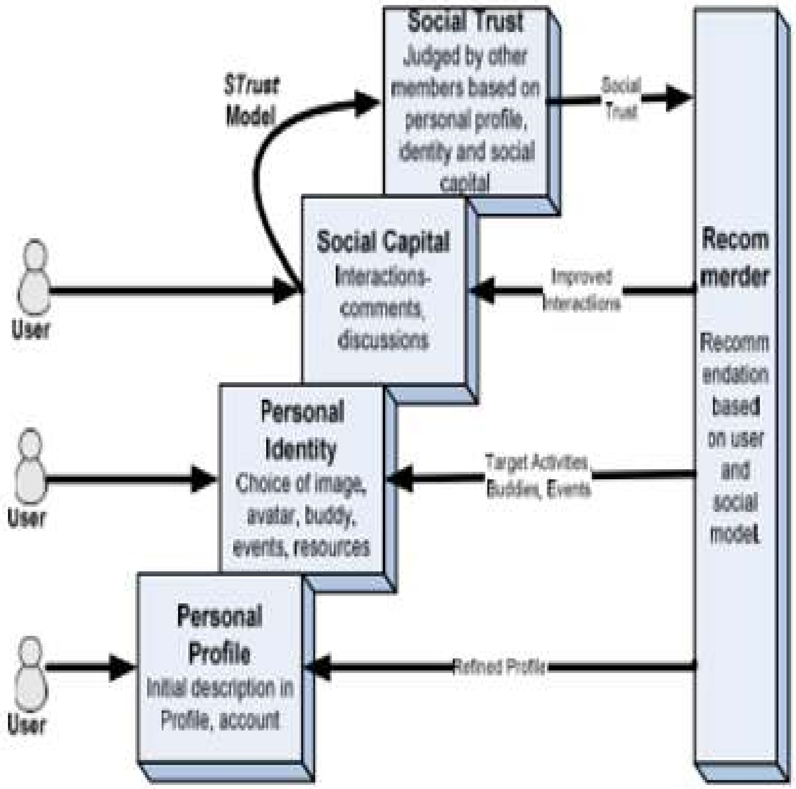
STrust Model
Social Trust
Judged by other members based on personal profile, dentity and social capital
Social Trust
Recom merder
Recomm endation based on user and social model.
User
Social Capital
Interactions- comments, discussions
Improved Interactions
User
Personal Identity
Choice of image, avatar, buddy, events, resources
Target Activities, Buddies, Events
User
Personal Profile
Initial description in Profile, account
Refined Profile

Figure 2. Framework for building trust communities in social network
Source : Sherchan & Paris, (2011)

Pushpalatha & Rao (2012) experimented with regression-based trust model for mobile ad-hoc networks. Their work focused on the implementation of regressions based trust model over routing protocol in mobile and ad hoc networks which will help to monitor how malicious node is limiting the optimization of network performance in ad hoc environment. The throughput got from the routing protocol on mobile and ad hoc network was 65%. This model can be improved on so as to increase the percentage of the throughput

$$\tau = \sum_{j=1}^{n} w_j T(j)$$

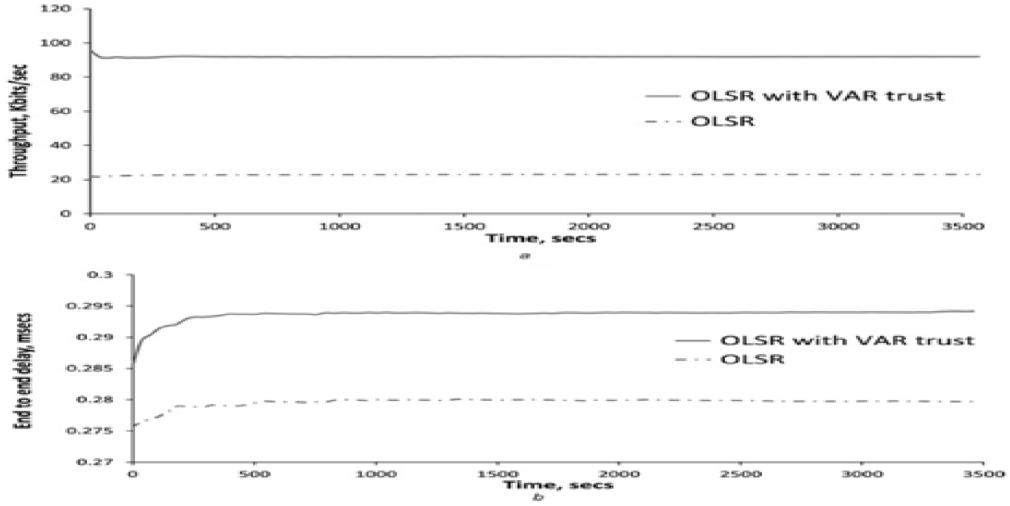

Figure 3. Performance of OLSR with trust amidst 20% no forwarding node
Source : Pushpalatha & Rao, (2012)

Can & Bhargava (2013) proposed the SORT: A Self-ORganizing Trust Model for Peer-to-Peer Systems. This model was proposed to build trust among peer to peer system, because of the series of attacks that have occurred due to lack of verification of a counterpart system. This model is used to create trust and to help eliminate malicious peer. Individual behavior was taken and is often check against their current behaviors to see if the pattern negate the baseline pattern of their behaviors. The model was able to figure out a malicious peer within a peer-to-peer system. It was reported that having trust in a peer doesn't eliminate the threat, The concept of insider attack was not taken into consideration. The situation where the peer is an attacker itself

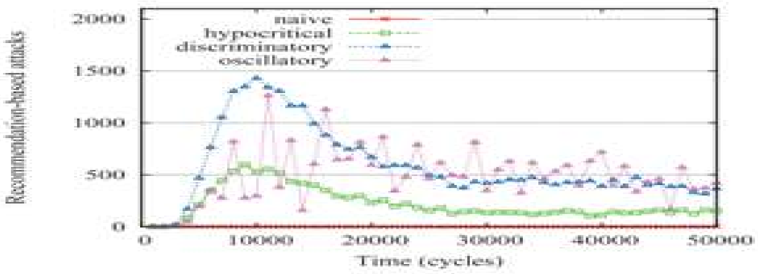

Figure 4. SORT with 10% malicious
Source : Can & Bhargava, (2013)

Meskaran et al. (2013) examined online purchase intentions and the effects of trust and security perception. They opined that the rapid growth of electronic commerce has exposed customers to the wide web. In other to ascertain the intention of the customer to continuously use the platform, theories were combined with trust and security to assess How customer perceive shopping online. The Theory of Planned Behavior (TPB), Theory of Reasoned Action (TRA) and the Technology Acceptance Model (TAM) were used as underpinning antecedents of trust and security. Their model is believed to boost user's intention to use the system of purchase but No survey was carried out to test the model which leave the model questionable and in a loop.

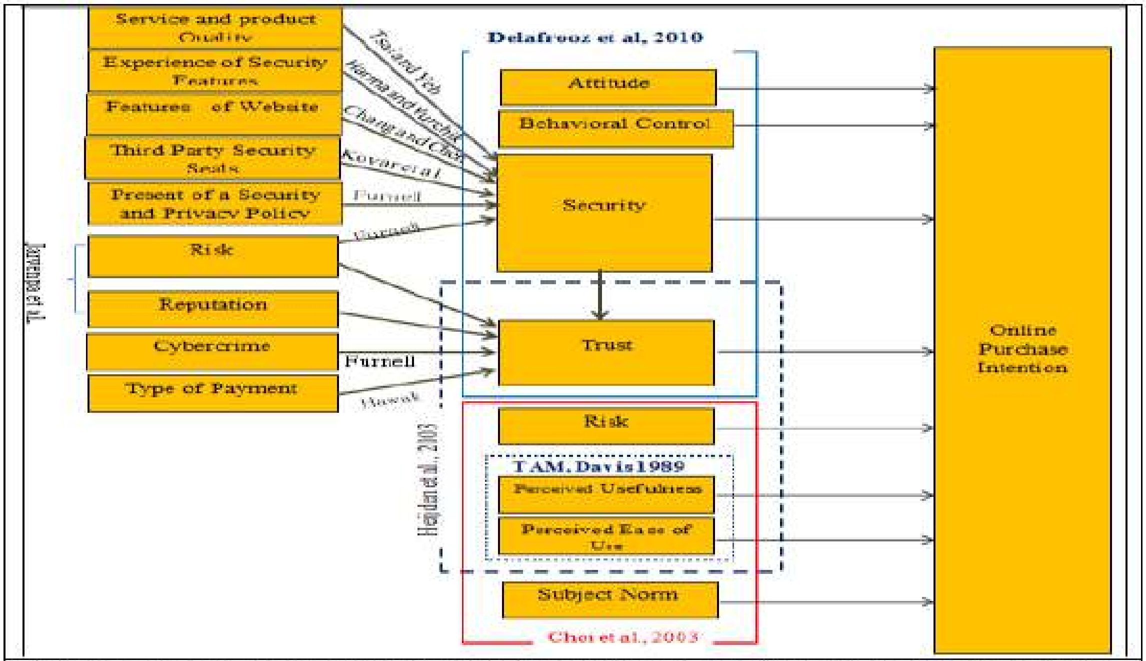

Figure 5. Comprehensive model based on The Theory of Planned Behaviour (TPB), Theory of Reasoned Action (TRA) and the Technology Acceptance Model (TAM
Source : Meskaran et al., (2013)

Abdel, Bentahar, Otrok, & Mourad, (2015) carried out a survey on trust and reputation models for Web services using single, composite, and communities. They established that web services is a wide environment and there is no security mechanism that is applicable in such wide environment, this has prompted the need to create trust and reputation on the web and its operations and how it is perceived by decision makers and open environment. Classification based on trust and reputation was proposed to checkmate the issues of trust and how it raised trust on a website and it did. However, active malicious website and services still exist within the composite and community-based architecture with the sole aim of decreasing the reputation of a website were noticed

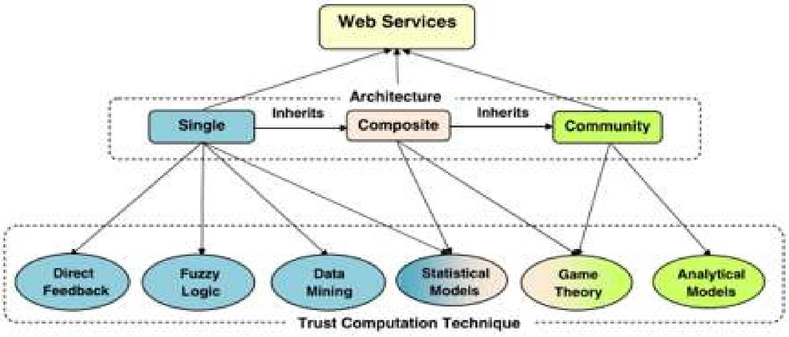

Figure 6. The trust computation technique
Source : Abdel, Bentahar, Otrok, & Mourad, (2015)

Irfane (2015) proposed the Tr-OrBAC: A Trust model for Collaborative Systems within Critical Infrastructures. The author engaged an organizations as an entity which comprises of various segments, hence he regrouped different organization structure into a collaborative system with an optimal sense of security among the separate segment of the organization This complex system proposed comes with its own security issues as it is more challenging to develop more complex security model to protect this collaborative system

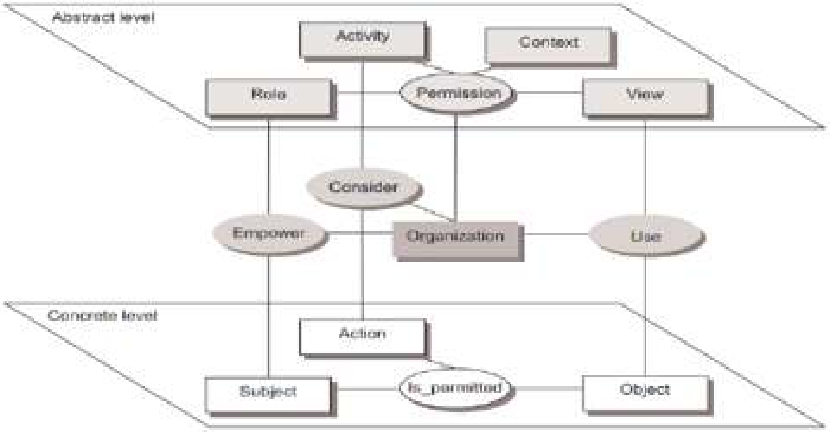

Figure 7. OrBAC model
Source : Irfane, (2015)

Yan, Zhang, & Vasilakos (2016) introduced a security and trust framework for virtualized networks and software-defined networking. They based their development on the fact that the higher the generation of wireless technology goes, security and trust in the context of virtualized networking and software-defined networking has to be looked into to ensure its adequacy to cater for these systems. Their model was in the forecast for higher XG network which needs to be tested.

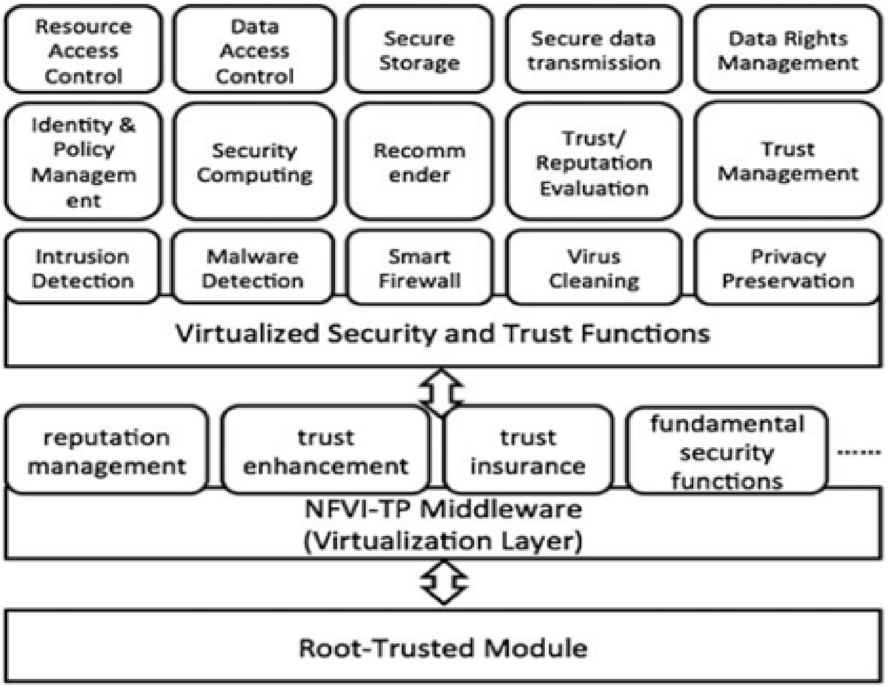

Figure 8. The model of perceived security and perceived trust in EPS use.
Source : Yan, Zhang, & Vasilakos, (2016)

Sun, Sun, Liu, & Gui (2017) carried out a research on initial trust model of mobile banking users (ITMMBU). They argued that despite the effort put in the creation of different applications based on trust models, many applications have not been utilized. Their work therefore examined Mobile banking and its cognitive risk and how to improve its acceptance based on their proposed multidimensional trust model. They engage quantitative method for their analysis but the conclusion of their analysis cannot be generalized because it was done at a particular location, a change of target population can lead to a different set of conclusion

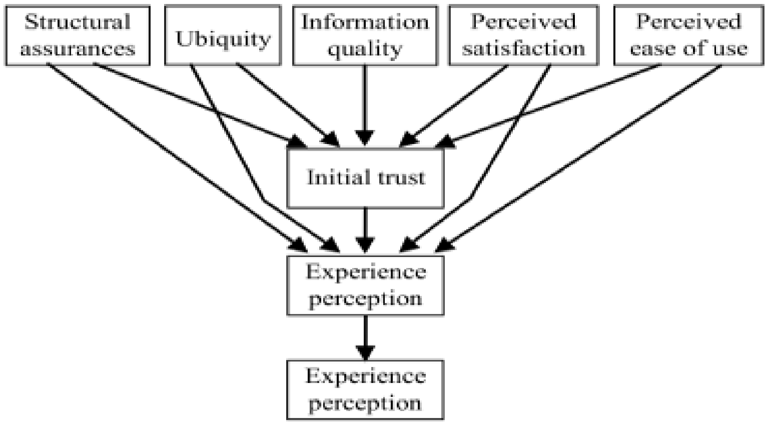

Figure 9. The model of perceived security and perceived trust in EPS use.
Source : Sun, Sun, Liu, & Gui, (2017)

Fernandez-gago et al. (2017) Modelled trust dynamics for Internet of Things. Their argument was that the internet has advances so much that it connects non-living things. There is therefore a need to aid trust among things that operate on the IoT platforms. Theirs was a conceptual model that has not been implemented. The framework proposed is questionable until proven otherwise

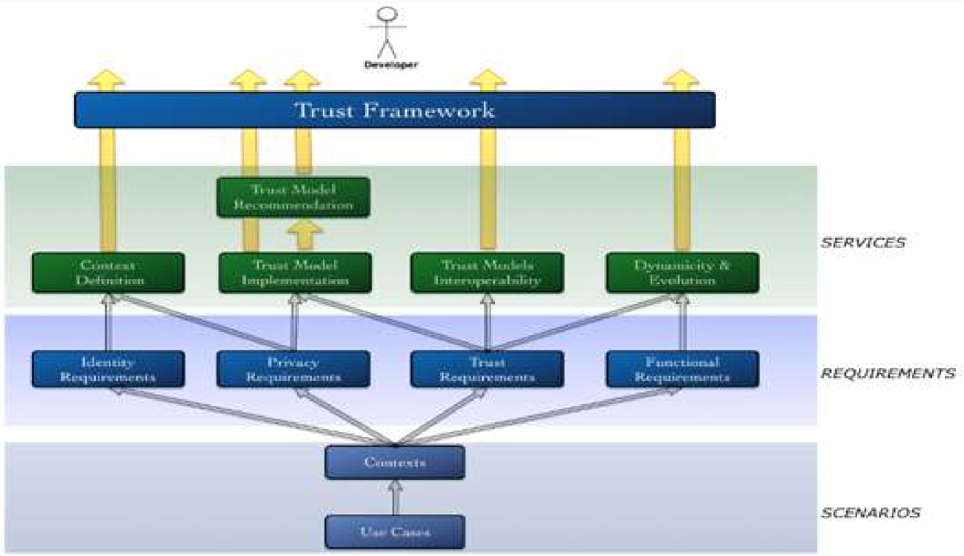

Figure 10. The model of perceived security and perceived trust in EPS use.
Source : Fernandez-gago et al., (2017)

3. CONCLUSION

Trust has become a major variable in building a resilient security system. Issues regarding trust in a system have prompt researchers into ensuring adequate model is built to ensure interacting system communicate without fear of malicious individual. Trust has facilitated more user's intension into using a system, having trust in a system doesn't stop attempt to break into the system. However, as attempt to break into the system increases these model have to be improved to counter these attack. As seen over the years different model have been develop to ensure maximum usage of the system. Continuous evaluation of these models will make the cyber space safer as more and more infrastructure gets connected to the World Wide Web to offer services and products.

In our discourse, we presented state of the art research on selected trust models used in information systems security. The attributes of trust needed for enterprise information systems and networks are identified with the aim of identifying trust characteristics in each model. Future work will seek to conduct research that fills the gaps identified in some of the selected models.

REFERENCES

1. Abdel, O., Bentahar, J., Otrok, H., & Mourad, A. 2015. A survey on trust and reputation models for Web services : Single , composite , and communities. Decision Support Systems, 74, 121–134. https://doi.org/10.1016/j.dss.2015.04.009
2. Can, A. B., & Bhargava, B. 2013. SORT : A Self-ORganizing Trust Model for Peer-to-Peer Systems. IEEE Transactions on Dependable and Secure Computing, 10(1), 14–27.
3. Fernandez-gago, C., Moyano, F., & Lopez, J. 2017. Modelling Trust Dynamics in the Internet of Things. Information Sciences. https://doi.org/10.1016/j.ins.2017.02.039
4. Irfane, M. Al. (2015). Systems within Critical Infrastructures. IEEE 5th World Congress on Information and Communication Technologies (WICT), 123–128.
5. Kim, C., Tao, W., Shin, N., & Kim, K. 2010. Electronic Commerce Research and Applications An empirical study of customers ' perceptions of security and trust in e-payment systems. Electronic Commerce Research and Applications, 9(1), 84–95. https://doi.org/10.1016/j.elerap.2009.04.014
6. Meskaran, F., Ismail, Z., & Shanmugam, B. 2013. Online Purchase Intention : Effects of Trust and Security Perception. Australian Journal of Basic and Applied Sciences, 7(6), 307–315.
7. Pushpalatha, R. V. M., & Rao, T. R. 2012. Regression-based trust model for mobile ad hoc networks. IET Information Security, 6(3), 131–140. https://doi.org/10.1049/iet-ifs.2011.0234
8. Sherchan, W., & Paris, C. 2011. STrust : A Trust Model for Social Networks. International Joint Conference of IEEE TrustCom. https://doi.org/10.1109/TrustCom.2011.112
9. Shibin, Z., Zhihai, X. I. E., Yifen, Y. I. N., Yan, C., Zhiwei, S., Lili, Y. A. N., & Haichun, W. 2017. Study on Quantum Trust Model Based on Node Trust Evaluation. Chinese Journal of Electronics, 26(3). https://doi.org/10.1049/cje.2016.11.007
10. Sun, B., Sun, C., Liu, C., & Gui, C. 2017. Research on Initial Trust Model of Mobile Banking Users. Journal of Risk Analysis and Crisis Response, 7(1), 13–20.
11. Yan, Z., Zhang, P., & Vasilakos, A. V. 2016. A security and trust framework for virtualized networks and software-defined networking. Security and Communication Networks, (March 2015), 3059–3069. https://doi.org/10.1002/sec